Beyond Logistics: Challenges to International Cybercrime Enforcement

Lissa Kryska, YLS ‘22 & Jackson Institute MA ‘22

In 2017, a joint effort involving the United States FBI and DEA, the Dutch National Police, Europol, and law enforcement in Thailand, Canada, Lithuania, the United Kingdom, and France brought down two large dark-web markets, Alphabay and Hansa. Before the coordinated takedown of Alphabay, at the time the largest dark-web market, Dutch police took control of Hansa, a smaller competitor. Police then allowed Hansa to continue running for a short period, during which they gathered information on existing users and on the new users who turned to the site after Alphabay’s demise. The subsequent shutdown of Hansa and the public revelation that it had been under police control for some time was intended to shake users’ faith in the entire dark net system, while the information collection generated leads for hundreds of investigations in tens of countries.

This successful operation shows the potential for effective cybercrime enforcement across national borders. However, as this article will detail, some of the most challenging aspects of international cybercrime enforcement were absent in this case. Cybercrime enforcement across national borders compounds the usual international issues of jurisdiction and cooperation with newer concerns about attribution, privacy and free speech, and state competition. Significant obstacles to effective international cybercrime enforcement include the potential for abuse of enforcement by authoritarian countries; differing conceptions of privacy and free speech even among democratic rule-of-law countries; unclear boundaries between state and non-state actions, with no incentive to define them; and the difficulty of maintaining/establishing the trust required for private-public partnerships as the number of parties on each side multiplies.

Norm- and Rights-Based Obstacles to International Cooperation

International efforts to address cybercrime from a law enforcement perspective are complicated by the different norms and laws across different jurisdictions. On the one hand, the more countries participate in a global effort, the more territory is covered, and the more thorough and effective policing can be. On the other hand, democratic countries risk empowering authoritarian leaders by assisting them in carrying out their agendas. For example, Interpol has been increasingly criticized in recent years over concerns that it is used by authoritarian countries to punish dissidents and advance other political agendas.

In the Alphabay-Hansa case, the leading enforcement countries were the United States and the Netherlands, with Europol serving a coordinating role. As both states were democratic countries considered to have strong rule of law, there was not the same concern about the mass data collection that took place as there may have been otherwise. Had the investigation required coordination with the Philippines, for instance, rather than the Netherlands, the massive collection of data about users of the online drug market would have had different implications, given the widespread accusations of extrajudicial killing of drug users and dealers under the Duterte administration.

The eventual fate of Alphabay’s head administrator points to another potential fracture in transnational efforts. A Canadian citizen, the suspect was arrested and imprisoned in Thailand,
where he “apparently took his own life” while in custody. Even when their cooperative enforcement efforts do not directly further authoritarian aims, some countries may be reluctant to coordinate closely with states that have poor prison conditions, uncertain prisoner protections, and weak rule of law.

While both Alphabay and Hansa served as markets for a number of illegal goods, including arms, stolen data, and malware, the majority of the traffic seems to have involved drugs. Global approaches to the drug trade differ in strategy, but the illicit nature of most narcotics is consistent throughout the world, and even countries that have decriminalized certain drug offenses do not consider drug use to be a core right. Other cybercrime enforcement will have to address more controversial topics.

Even among countries generally considered to have strong rule of law, cybercrime enforcement can be divisive because of vast differences in free speech and privacy standards. Speech that is protected in the United States is criminalized in some parts of Europe as hate speech, and European countries have demanded greater privacy and transparency from major technology companies. International cybercrime enforcement efforts will not only highlight differences between authoritarian and democratic countries, but between democratic countries as well, as one country’s “cybercrime” might be another’s protected right.

Specifically, actions to address political influence operations, fake news, large bot networks, and the takedown of extremist websites and platforms will be more difficult. Even among closely aligned countries, like the United States and Germany, activity that could be considered criminal in Germany (hate speech, membership in certain political parties) may be considered a protected right under the United States’ much broader interpretation of free speech. Coordination in cases involving these issues will be much more contentious. When expanding the number of actors to include private companies, academics, and more, there will be an even larger number of norms and sets of ethics to reconcile.

State Involvement and the Problem of Attribution

Another challenge which arises in the cybercrime context is the involvement of state actors. This problem was largely absent from the Alphabay-Hansa takedown, which involved large, open marketplaces populated by a number of individuals and groups, none of whom were reported to have state backing. (While North Korea has been known to engage in government-backed black-market transactions to raise funds, most countries do not actively support these types of criminal groups as a matter of policy.) The nature of the sites as drug markets made cooperation in this case easier. Many other cybercriminal acts, however, are suspected to have backing from, or at least a connection to, a nation state (see, for example, the Center for Strategic and International Studies’ list of recent cyber incidents).

The links between countries and the cybercriminals they host are often complex. Cybercrime carried out against an adversary country may be tolerated, encouraged, or even directed and funded by a national government. The lines between intelligence operations, cyber “warfare” officially conducted by states, and cybercrime are not well established. The countries with the most power, who could potentially have the ability to marshal a global consensus and
create enforcement mechanisms, have the least incentive to do so, as they would be neutering their own competitive advantage.

A large concern in cybercrime generally, which becomes even more important at the level of international law enforcement, is the question of attribution. Because of complex webs of servers and sites, the remote nature of the crimes, and constantly developing technology, disagreements over to whom to attribute a given criminal act are bound to arise. Cybercriminals can manipulate their actions to give the appearance of being a state actor or not, or of being from a completely different country. Some crimes simply have unknown origins. States may have different standards of proof for assigning blame, or different incentives to prosecute within their own states. In a separate internationally-coordinated investigation, for example, suspects from Georgia, Moldova, and Ukraine are facing arrest and prosecution domestically; however, suspects living in Russia have yet to face any consequences. Unless the Russian government decides to act, there is little the international community can do to change this uneven enforcement.

**Stretching the Limits of Trust: Public-Private Partnerships in International Cybersecurity**

Finally, distrust between states and the lack of clarity around state-company relationships makes private partnerships even more fragile than they are domestically. There seems to have been little need for private sector assistance in the Alphabay-Hansa case, in part because of a separate German investigation which brought the Hansa administrators under arrest and allowed for a seamless takeover by Dutch police, and in part because of the relatively straightforward nature of the crimes themselves (buying and selling illicit items, mostly drugs). For more complex cybercrimes, however, governments often rely on private sector expertise. Some investigations depend on companies granting the government access to certain information or capabilities they have. These partnerships may be more or less formal, and many require a foundation of trust on an interpersonal level. As investigations become international and involve more governments and potentially more private actors from different countries, it will be difficult to maintain that trust on both sides. Private actors who are willing to assist in limited investigations may not want their identities or capabilities revealed more widely or may not trust other states to use data they provide responsibly, while outside states may require higher levels of transparency and accountability and themselves not trust foreign private actors. Even closely aligned countries can have significantly different attitudes and approaches towards the private sector’s role in cybersecurity and the amount of regulation that should be required.

Mutual trust is paramount to any successful cooperation between private companies or individuals and government actors, especially when it involves information sharing or use of the company’s technology to carry out an investigation. The more parties are involved in an investigation, the more wary companies and individuals will be of joining or aiding said investigation. Companies may also have concerns that sharing information could later lead to increased regulation. Conversely, countries with higher privacy standards than the United States may be reluctant to share information with private companies or individuals, especially US-based ones, to further an investigation. Both companies and states may face legal or political challenges at home about their ability to share information with foreign partners. As long as cybercrime enforcement continues to draw heavily on private partners, this mutual mistrust will hinder international coordination.
Takeaways and Areas for Further Study

The takedown of Alphabay and Hansa in 2017 provides one example of how law enforcement agencies can successfully work across national borders to fight cybercrime. This case was particularly well-suited for international cooperation, and provides insight into the types of cases that can be targeted with existing strategies, alliances, and techniques. However, addressing the wider range of cybercrimes will require new ideas, international coalition-building, and a careful balancing of values vs. security interests. The world needs strategies to ensure that cybercrime enforcement efforts do not become a tool for widespread human rights abuses, while accepting the potential for good-faith differences on questions like the scope of freedom of speech. Countries may need to give up some of the ambiguity that they currently benefit from in order to create clearer global norms about what acceptable and unacceptable state cyber action looks like. Formalization of the terms of private-public partnerships could provide accountability and transparency around those relationships, helping to build trust for expansion of those partnerships at the global level. Until these obstacles are addressed, cybercrime enforcement across national borders will struggle to keep up with criminal activity.

Recommended reading (also included as sources):

The Role of the State in the Private-Sector Cybersecurity Challenge, by Gabi Siboni and Ido Sivan-Sevilla

Interpol at 100: Does the World’s Police Force Work? by Kathy Gilsinan

Massive Blow to Criminal Dark Web Activities After Globally Coordinated Operation, Europol Press Release

Chinese Cyberhackers ‘Blurring Line Between State Power and Crime’ by Josh Taylor