Criminal Division Strategic Approach to Countering Cybercrime

(October 2024)

The Criminal Division plays a unique and essential role in the Department of Justice's fight against cybercrime. This document sets out the Division's Strategic Approach to Countering Cybercrime, with a focus on using all tools to disrupt criminal activity and hold criminal actors accountable, developing law and policy to prevent and prosecute cybercrime, and promoting cybersecurity through capacity building and public education.

Mission and Support

The Division's cybercrime enforcement mission, achieved through its sections and offices, is to combat technology-enabled crime, protect public safety, and bring criminals to justice.

The Computer Crime and Intellectual Property Section (CCIPS) is a leader in the Division's and the Department's efforts to fight cybercrime. CCIPS "has primary responsibility for developing the Department's overall cyber, cyber-enabled, and intellectual property offense enforcement strategies, for providing programmatic support to the [Computer Hacking and Intellectual Property, or] CHIP Network of Assistant United States Attorneys (AUSAs), and for coordinating cyber and cyber-enabled crime and intellectual property investigations and cases that may significantly impact more than one district and/or other countries. In addition to developing and prosecuting their own cases and assisting CHIP prosecutors in cases on request, CCIPS supports the CHIP Network by serving as a source and conduit for information through CCIPS Online, a website of resource materials; providing information on cases and current events to the CHIP AUSAs; providing legal expertise through the distribution of manuals, monographs, case summaries, and legislative analysis; and developing and implementing training programs for CHIP and other prosecutors in conjunction with [the Office of Legal Education]." Justice Manual § 9-50.102.[1] CCIPS also serves as the Department's experts in collecting and using electronic evidence.

CCIPS is also a leader in the Department's efforts to address risks presented by emerging technology, such as virtual currency. The Criminal Division's National Cryptocurrency Enforcement Team (NCET), which sits within CCIPS, serves as a center of cryptocurrency excellence drawing on expertise across the Division. In addition, NCET leads and supports the Digital Asset Coordinator Network (DAC), which comprises over 150 selected federal prosecutors from U.S Attorney's Offices and across the Department's litigating components. CCIPS, through the DAC Network, ensures that Department prosecutors develop and share the best practices, training, and expertise necessary to prosecute digital asset crimes.

[1] "Investigations of national-security related cyber or cyber-enabled crimes fall within the scope of chapter 9-90.000 of the Justice Manual," which describes the responsibilities of the National Security Division and the National Security Cyber Specialists Network (NSCS) in the Department's cyber and cyber-enabled enforcement strategies. Justice Manual § 9-50.105. "CCIPS, the CHIP network, NSD, and the NSCS network all support each other in the execution of their respective cyber and cyber-enabled crime responsibilities." *Id.*

Other sections and offices in the Criminal Division likewise advance the Department's cyber enforcement mission:

> The **Money Laundering and Asset Recovery Section (MLARS)** leads the Division's and the Department's money laundering, seizure, and asset forfeiture enforcement efforts, as well as the Department's Asset Forfeiture Program. Enforcement efforts that include seizure, forfeiture, and money laundering are critical for combatting cybercrime. MLARS partners with CCIPS to support the NCET. In particular, the Division relies upon the powerhouse combination of MLARS's expertise in money laundering, financial institutions, anti-money laundering, the Bank Secrecy Act, cryptocurrency, tracing, seizure and forfeiture, and CCIPS's expertise in emerging technologies, blockchain, and cryptocurrency to ensure the success of the NCET and advance the Division's mission to disrupt cybercrime.
>
> **The Office of Enforcement Operations (OEO)** provides guidance and assistance regarding electronic surveillance of cybercrime actors.
>
> The **Office of International Affairs (OIA)** serves as the Central Authority for the United States and plays a crucial role in nearly every major cyber case by coordinating with foreign partners, securing foreign evidence, and ensuring the arrest and extradition of defendants who flee overseas or operate from abroad. OIA also gathers requested electronic evidence within the control of U.S. service providers on behalf of foreign authorities for use in foreign investigations and prosecutions, to support the investigation of transnational criminals and disrupt malicious cyber actors.
>
> The **Office of Overseas Prosecutorial Development, Assistance and Training (OPDAT)** partners with CCIPS to implement the International Computer Hacking and Intellectual Property (ICHIP) network, a global law enforcement network dedicated to building capacity and reliable partners to fight cybercrime worldwide.

Cybercrime also intersects with areas of subject matter expertise assigned to other sections within the Criminal Division, such as offenses related to child exploitation, drug trafficking, financial fraud and identity theft, public corruption, and violent crime. For example, through the **Child Exploitation and Obscenity Section**, the Division develops and advances the Department's National Strategy for Child Exploitation Prevention and Interdiction, which describes the growing scale, complexity, and dangerousness of online threats to children, and sets forth proposed solutions for combatting these threats.

Alignment with Department and Government-Wide Cyber Strategies

The National Cybersecurity Strategy outlines an all-of-government approach to strengthen the nation's cybersecurity and defend against cyber threats. The Criminal Division executes many of the Department's responsibilities under the Strategy, specifically the Strategy's goal to "disrupt and dismantle threat actors" by leading many of the U.S. government's most effective and visible disruptions of cybercrime. A key strategic objective of the Strategy and a Department priority goal is to defeat ransomware. CCIPS, with the FBI, leads the Department's ransomware efforts.

To that end, CCIPS, working with its law enforcement partners, has disrupted multiple prolific ransomware actors by seizing ransomware infrastructure, prosecuting culpable individuals, and taking other enforcement actions to dismantle the criminal ecosystem used by ransomware groups.

The Division's long track record of successful cyber disruptions also fulfills the Department's strategic plan to "Enhance Cybersecurity and Fight Cybercrime" through efforts to "Deter, Disrupt, and Prosecute Cyber Threats." By disrupting cyber threats and prosecuting bad actors, the Criminal Division deters cybercrime, in some instances causing cybercrime groups to shutter in the wake of disruption actions.

The Department's strategic objective to enhance cybersecurity and fight cybercrime also includes strengthening international and public-private partnerships to fight crime. CCIPS' Cyber Operations International Liaison (COIL) focuses on identifying and increasing opportunities for internationally coordinated disruption of cybercrime, and the NCET facilitates public-private partnerships to combat criminal abuse of cryptocurrency.

In keeping with the directives of the Comprehensive Cyber Review, the Criminal Division and CCIPS have (1) prioritized targeting of key ransomware and cybercrime actors; (2) taken steps to attack key infrastructure—including technology, tools, and financial services—upon which cybercriminals depend; and (3) combatted cyber threats with existing tools and developed new tools that account for the fast-evolving nature of this threat.

Goals

To achieve its Strategic Approach to Countering Cybercrime, the Criminal Division, working in partnership with United States Attorneys' Offices and other Department components, will pursue the following goals:

1. Lead the Department in deterring and disrupting cybercrime, such as ransomware, through sustained and focused investigations, arrests, extraditions, prosecutions, seizures and other enforcement activity, coordinated with domestic and foreign partners, to target the most significant cyber-criminal activity.

Actions in support of this goal:

- Conduct sustained and targeted cybercrime disruption campaigns, including prosecution of threat actors and seizure and forfeiture of criminal assets and infrastructure, all prioritizing criminal groups engaged in:
    - ransomware extortion;
    - creating, expanding, or operating harmful botnets;
    - obtaining and selling access credentials or personally identifiable information;
    - providing criminal infrastructure and services, such as malware developers, bulletproof hosting providers, crypters, counter-antivirus service providers, booters and loaders, and initial access brokers; and
    - hacks of virtual asset platforms.

- Make data-driven decisions that prioritize key threats.
- Build and draw upon international cooperation to obtain evidence and extradite defendants.
- Coordinate with other agencies to use all tools throughout the U.S. Government to combat cyber threats.

2. Ensure the Department has effective tools and policies to combat cybercrime, put victims first, and protect civil rights in all its cybercrime investigations, disruptions, and prosecutions.

Actions in support of this goal:

- Lead the Department's efforts to develop law governing the use of judicial authorities to disrupt cyber threats.
- Drive the development of responsible Department policies surrounding the use of judicial authorities related to cyber investigations and prosecutions, including authorities related to reliable forensic analysis and juvenile cybercrime.
- Manage risk in cyber investigations and operations, drawing on broad Criminal Division experience in conducting sensitive undercover investigations in multiple enforcement areas.
- Advise Department leadership on legislative proposals concerning the investigation, prosecution, and prevention of cybercrime.
- Advance a victim-centered approach to fighting cybercrime, *e.g.*, providing ransomware decryptors to victims as soon as possible and before investigation and prosecution is concluded.

3. Promote national cybersecurity and the government's ability to address cybercrime through capacity-building, public education, and information sharing.

Actions in support of this goal:

- Lead the Department's efforts to address emerging technologies and creative misuse of emerging technologies to commit cybercrime, including cryptocurrency, swatting, SIM-swapping, and artificial intelligence.
- Educate the public about emerging criminal threats such as cryptocurrency confidence scams (formerly known as "pig butchering"), SIM swaps, and swatting, so that citizens may better protect themselves against such threats.
- Advance private-sector cybersecurity by: providing information to assist in defense, resilience, and recovery; using all appropriate tools to protect victims and recover stolen or extorted funds; and encouraging contact with law enforcement as early as possible.
- Maintain and enhance cybercrime, intellectual property rights protection, and cryptocurrency prosecution talent throughout the Department through hands-on experience and training.

- Expand international legal frameworks, outreach, relationships, and assistance to foster international cooperation, and harmonize law across borders.
- Promote deterrence by publicizing CCIPS's and the Division's work and accomplishments and speaking publicly on the Division's successes consistent with Department policy.