Advancing the Department's Response to Cyber Threats
2021-2025

"Since returning to the government and in my current seat as the Deputy Attorney General, I have been struck by an evolution: malicious cyber actors becoming more aggressive, more sophisticated, more belligerent and brazen – and an increased blurring of the line between state-sponsored cyberattacks and attacks by criminal groups." – Deputy Attorney General Monaco, July 2022

The range of severe cyber threats facing Americans today includes criminal groups abusing cryptocurrency and perpetrating ransomware attacks against hospitals, businesses, and critical infrastructure; state-sponsored hackers executing sophisticated intrusions, including hack-and-dump schemes and influence operations; and increasingly, state-sponsored actors working together with criminal groups to form a blended threat. ODAG prioritized building and refining the Department's capacity to respond effectively and creatively to this constantly evolving cyber threat landscape.

Core to this effort was reframing the Department's cyber strategy to prioritize victims and disruption. This pivot recognized that it is not enough to hold criminals accountable after the fact—the Department has an obligation to do all we can to stop the harms from cyber threats before they happen. This requires assessing at every step of the investigation whether there is an opportunity to disrupt the actors or reduce the risk to victims. It also requires looking to tools beyond traditional arrests and prosecutions to have an impact, such as providing technical expertise to disable infrastructure, distributing decryptor keys to victims, and supporting sanctions and the use of export controls to hold malicious actors accountable.

This reframing of the Department's cyber strategy enabled the Department to take historic, successful actions:

- Launched a Comprehensive Cyber Review to modernize and strengthen the Department's cyber capabilities and implement the overarching strategy that places victims first and prioritizes using all available tools to disrupt cybercriminals.
    - Recovered millions in ransomware payments through novel applications of traditional forfeiture authorities to digital assets, jumpstarting the Department's efforts to disrupt and deter ransomware attacks by making them more costly and less profitable for criminal enterprises, and to protect and achieve remediation for victims.
    - Disrupted major ransomware variants and cybercriminal services.
    - "Hacked the hackers"[1] and provided early notice to victims saving them from millions in losses through impending ransomware attacks.
    - Disrupted botnets used by both criminal groups and nation-state actors to target innocent Americans and wage influence operations.

[1] Deputy AG Monaco announcing the disruption of the Hive Ransomware variant on January 26, 2023.

- Created a dedicated cyber section in NSD – NatSec Cyber – to increase the scale and speed of disruptions and prosecutions of nation-state threat actors, state-sponsored cybercriminals, and other cyber-enabled threats to national security, including online FMI operations using sophisticated techniques such as fabricated personas and narratives and deepfakes spreading synthetic content.

- Tackled an explosion of ransomware threats and abuse of cryptocurrency that emerged in recent years:

    - Promoted a coordinated, Department-wide approach for investigating and disrupting ransomware groups by implementing new internal notification and reporting requirements for all federal prosecutors handling matters involving ransomware or digital extortion.

    - Created the Ransomware and Digital Extortion Task Force to dedicate criminal, civil, and national security resources in coordinated effort to combat the threat of ransomware.

    - Partnered with DHS and other federal agencies to launch the U.S. Government's first-ever one-stop hub for ransomware resources at StopRansomware.gov, a consolidated platform that provides information and guidance to help private and public organizations protect against ransomware attacks.

    - Launched the National Cryptocurrency Enforcement Team (NCET) – a team of prosecutors with expertise in money laundering, computer crimes, and forfeiture – to pursue and disrupt threat actors abusing cryptocurrency to commit crime. NCET has been integral to numerous impactful enforcement actions, including the largest-ever financial seizure in Department history – over $3.6 billion in stolen Bitcoin.

    - Facilitated the creation of the FBI's Virtual Asset Exploitation Unit, a specialized team that brings together cryptocurrency experts into a single nerve center to support the FBI's crypto-related enforcement efforts, including blockchain analysis and virtual asset seizure training.

    - Developed new avenues for enhanced international collaboration to address the global aspect of cyber threats, including creating the International Virtual Currency Initiative to increase international law enforcement cooperation and disruptive operations against crypto-related crime.

    - Created a Cyber Fellowship program to develop a new generation of prosecutors and attorneys equipped to handle emerging cyber threats.

- Revitalized the Department's own cybersecurity posture, including:

    - Upgraded the Department's cybersecurity defenses, culminating in 2024 with the Department achieving the top score (99%) across all executive agencies on the Federal Information Security Modernization Act (FISMA) metrics for mature information security policies and practices.

    - Developed a Justice Cyber Incident Playbook that provides senior Department leadership with a comprehensive guide on best practices in responding to a cyber incident affecting Department systems.

- Launched the Civil Cyber Fraud Initiative to use the Department's authorities under the False Claims Act to pursue civil actions against government grantees and contractors who fail to meet cybersecurity obligations.

- Enhanced cross-border cooperation against serious cybercrime-related threats with implementation of the first CLOUD Act agreements with the UK and Australia and key contributions to the new United Nations Convention against Cybercrime and US-EU Data Privacy Framework.

- Instituted an innovative all-tools approach to addressing the growing challenge of juvenile cybercrime actors, with an emphasis on disruption and accountability through diverse strategies and mechanisms, including partnerships with state and local law enforcement.