U.S. Department of Justice

REPORT OF THE ATTORNEY GENERAL'S CYBER DIGITAL TASK FORCE

U. S. Department of Justice

Office of the Deputy Attorney General

The Deputy Attorney General

Washington, D.C. 20530

July 2, 2018

Dear Mr. Attorney General:

You have emphasized that "upholding the Constitution and protecting the rule of law is the foundation of everything we do" at the Department of Justice. Our important duties include keeping America safe by fighting crime and preserving the Nation's security.

As President Trump has observed, "The United States faces an extraordinarily dangerous world, filled with a wide range of threats that have intensified in recent years." Director of National Intelligence Dan Coats explained earlier this year that the cyber threat "is one of [our] greatest concerns and top priorities." The Department of Justice shares that assessment.

Every day, malicious cyber actors target our citizens, our businesses, our military, and all levels of our government. They cause billions of dollars in losses and attempt to undermine our democratic values. Combating cybercrime and cyber-enabled threats to our Nation's security must remain among the Department's highest priorities.

In February 2018, you directed the formation of a Cyber-Digital Task Force to undertake a comprehensive assessment of the Department's work in the cyber area, and to identify how federal law enforcement can even more effectively accomplish its mission in this vital and evolving area.

The initial assessment is complete. It is my privilege to present this report of the Attorney General's Cyber-Digital Task Force.

I hope this report will assist as all Americans keep moving forward to protect our people, promote our economy, and preserve our values.

Sincerely,

Rod J. Rosenstein
Deputy Attorney General

REPORT OF THE ATTORNEY GENERAL'S **CYBER DIGITAL** TASK FORCE

United States Department of Justice
Office of the Deputy Attorney General
Cyber-Digital Task Force
950 Pennsylvania Avenue, N.W.
Washington, D.C. 20530
https://www.justice.gov/cyberreport

Table of Contents

ATTORNEY GENERAL'S CYBER-DIGITAL TASK FORCE

Task Force Members

Sujit Raman, Chair
Associate Deputy Attorney General
Office of the Deputy Attorney General

John P. Cronan
Assistant Attorney General (Acting)
Criminal Division

John C. Demers
Assistant Attorney General
National Security Division

Carl Ghattas
Executive Assistant Director
Federal Bureau of Investigation

John M. Gore
Assistant Attorney General (Acting)
Civil Rights Division

Andrew E. Lelling
United States Attorney
District of Massachusetts

David T. Resch
Executive Assistant Director
Federal Bureau of Investigation

Beth A. Williams
Assistant Attorney General
Office of Legal Policy

Peter A. Winn
Chief Privacy & Civil Liberties Officer (Acting)
Director, Office of Privacy & Civil Liberties

Task Force Contributors

Matthew J. Sheehan
Counsel to the Deputy Attorney General
Staff Director

Elizabeth Aloi
Leonard Bailey
Michael F. Buchwald
Mark Champoux
Thomas Dettore
Richard Downing
Benjamin Fitzpatrick
Lindsey Freeman
Tashina Gauhar
Josh Goldfoot
Bonnie Greenberg
Brendan Groves
Aarash Haghighat
William Hall
Christopher Hardee
Adam Hickey
Ray Hulser
Anitha Ibrahim
Matthew Kluge
John T. Lynch, Jr.
Katrina Mulligan
Sean Newell
Erica O'Neil
Richard Pilger
Jason Poole
Andrew Proia
Kimberley Raleigh
Peter Roman
Opher Shweiki
Michael Stawasz
Andrew Warden
J. Brad Wiegmann
Cory Wilson

And representatives from:

Bureau of Alcohol, Tobacco, Firearms, and Explosives Office of Strategic Intelligence & Information
Drug Enforcement Administration Office of Investigative Technology
Federal Bureau of Investigation Counterintelligence Division
Federal Bureau of Investigation Counterterrorism Division
Federal Bureau of Investigation Criminal Investigative Division
Federal Bureau of Investigation Cyber Division
Federal Bureau of Investigation Digital Transformation Office
Federal Bureau of Investigation Information Technology Branch
Federal Bureau of Investigation Office of Private Sector
Federal Bureau of Investigation Office of the Chief Information Officer
Federal Bureau of Investigation Office of the Director
Federal Bureau of Investigation Office of the General Counsel
Federal Bureau of Investigation Operational Technology Division
INTERPOL Washington, the U.S. National Central Bureau
Justice Management Division Office of the Chief Information Officer/ Cybersecurity Services Staff
United States Marshals Service Investigative Operations Division
United States Marshals Service Judicial Security Division

Introduction

Cyber-enabled attacks are exacting an enormous toll on American businesses, government agencies, and families. Computer intrusions, cybercrime schemes, and the covert misuse of digital infrastructure have bankrupted firms, destroyed billions of dollars in investments, and helped hostile foreign governments launch influence operations designed to undermine fundamental American institutions.

The Department of Justice's primary mission is to keep the American people safe. We play a critical role in the federal government's shared effort to combat malicious, cyber-enabled threats.

In February 2018, the Attorney General established a Cyber-Digital Task Force within the Department and directed the Task Force to answer two basic, foundational questions: How is the Department responding to cyber threats? And how can federal law enforcement more effectively accomplish its mission in this important and rapidly evolving area?

This report addresses the first question. It begins by focusing on one of the most pressing cyber-enabled threats our Nation faces: the threat posed by malign foreign influence operations. Chapter 1 explains what foreign influence operations are, and how hostile foreign actors have used these operations to target our Nation's democratic processes, including our elections. This chapter concludes by describing the Department's protective efforts with respect to the upcoming 2018 midterm elections, and announces a new Department policy—grounded in our longstanding principles of political neutrality, adherence to the rule of law, and safeguarding the public trust—that governs the disclosure of foreign influence operations.

Chapters 2 and 3 discuss other cyber-enabled threats our Nation faces, particularly those connected with cybercrimes. These chapters describe the resources the Department is deploying to confront those threats, and how our efforts further the rule of law in this country and around the world. Chapter 4 focuses on a critical aspect of the Department's mission, in which the Federal Bureau of Investigation plays a lead role: responding to cyber incidents. Chapter 5 then turns the lens inward, focusing on the Department's efforts to recruit and train our own personnel on cyber matters. Finally, the report concludes in Chapter 6 with thoughts and observations about certain priority policy matters, and charts a path

for the Task Force's future work. Over the next few months, the Department will build upon this initial report's findings, and will provide recommendations to the Attorney General for how the Department can even more efficiently manage the growing global cyber challenge.

The Department's Cyber Mission

Computer intrusions and attacks are crimes, and the Department of Justice fights crime. That is true regardless of whether the criminal is a transnational organized crime group, a lone hacker, or an officer of a foreign military or intelligence organization. In addition, the Department has unique and indispensable cybersecurity roles in the realm of foreign intelligence and counterintelligence.

In fighting criminal computer intrusions and attacks, the Department identifies, dismantles, and disrupts cyber threats. In doing so, we provide justice to victims and deter others from committing similar offenses. To fulfill our mission, we deploy criminal justice and intelligence tools to find malicious hackers, arrest them, incarcerate them, and require them to pay restitution to their victims. We shut down the dark markets criminals depend upon to buy and sell stolen information. We deprive criminals of the tools and services they use to attack American families and businesses. Working with private sector partners, we seek to deny foreign governments the infrastructure they would use to conduct illegal influence operations. We seize or disable the servers, domain names, and other infrastructure that transnational criminals rely upon to penetrate our borders. We use legal authorities to take control of virtual infrastructure—such as networks of compromised computers called "botnets"—to prevent future victimization. We share information gathered during our investigations to help victims protect themselves. And we do all of these things to fight modern threats while remaining faithful to our Nation's respect for personal freedom, civil liberties, and the rule of law.

Where appropriate, we also work closely with our interagency partners to support financial, diplomatic, and military measures to bring all possible instruments of national power to bear against cyber threats. Other departments have the primary responsibility for helping victims recover from cyberattacks; we have the primary responsibility for conducting the investigation into who is responsible. We do not have the federal government lead for assisting election officials in securing their systems, but we do have the primary responsibility for investigating our foreign adversaries' efforts to target election infrastructure.

Similarly, we do not have the government's lead role in protecting private or government networks, in designing security standards, or in regulating how the private sector must defend itself. Those are important functions for which other government departments take responsibility—often, with our support and assistance. Our mission is to enforce the law, to ensure public safety, and to seek just punishment.

How We Succeed

By faithfully executing the Department's crime-fighting mission, we have produced tangible and positive results for the American people. These results are reflected by the caliber of criminals we have taken offline and taken off the streets; the millions of computers we have liberated from botnets that harness their processing power for fraud and theft; the web cameras that no longer spy on unwitting victims; the dark markets selling illicit drugs, weapons, and child pornography we have disrupted and shuttered; the virtual currency we have seized from criminals; and the malicious software that is no longer offered for sale.

These tangible results have a secondary effect: deterrence. Deterrence is one of the primary objectives of criminal law, and it is a key factor in improving our Nation's cybersecurity. An effective deterrence policy requires us to have a credible capability to enforce the law, and therefore to deter offenders. A credible capability to enforce the law, in turn, requires the Department to be able to credibly investigate cybercrime. Without evidence, there is no attribution. Without attribution, there will be no consequences for offenders, and thus no deterrence.

Yet, the reality is that identity-masking technologies and international investigative barriers pose unique challenges for deterring cyber threats. This report details the ways in which we approach those challenges. We depend upon legal authorities to investigate computer crimes; upon the cooperation of the public and of the private sector to report crimes and to help identify cyber threats; and upon the assistance of international partners to gather foreign evidence, apprehend criminals, and extradite suspects. Often, those authorities are exclusive to the Department of Justice and other law enforcement agencies. For example, the Department has the authority to obtain the subpoenas, court orders, and search warrants that the law requires in order to compel online service providers to produce crucial records that can reveal criminal activity.

> *"Our mission is to enforce the law, to ensure public safety, and to seek just punishment."*

Preserving these investigative authorities and capabilities, and using them responsibly and consistent with law, is therefore vital to the Nation's cybersecurity. It is also a Department priority. The Department's agents and prosecutors need the authority and tools to obtain evidence; the technical skill to understand it; and the ability to introduce that evidence at trial and explain what it means. Maintaining these capabilities is, in part, a question of making sure investigators retain the lawful authority to access evidence in a changing digital landscape. It is also a question of building and maintaining a talented and dedicated workforce.

The Department—along with the entire U.S. government—wants Americans to be able to

use their devices and computers secure in the knowledge that their data is safe. Many government departments and agencies are working toward that cybersecurity goal. And while this report catalogs the many ways that the Department is at the cutting edge of keeping Americans safe from cyber threats, we are also keenly aware that our tools and authorities are not sufficient by themselves to accomplish that goal. Our work is critical to cybersecurity, but our work, alone, is not enough to secure the Nation.

As Americans have shifted much of our economy, our communications, our news media, and our daily lives to the Internet, we are now discovering how vulnerable that shift makes us. To defend against cyberattacks from nation states and from equally sophisticated criminals, the American public should be able to turn to the government for leadership. This report details how the Department of Justice is responding to that call.

– Sujit Raman, *Chair,*
Attorney General's Cyber-Digital Task Force

Credit: Amy Mathers, U.S. Department of Justice

Attorney General Jeff Sessions announces law enforcement's July 2017 seizure of AlphaBay, what was then the world's largest "Dark Market." In addition to traditional criminal enforcement actions, disrupting and dismantling the illicit underworld's digital infrastructure is a major facet of the Department of Justice's broader fight against cybercrime.

Chapter 1
Countering Malign Foreign Influence Operations

Hostile foreign actors have long sought to influence, and to subvert, our Nation's democratic institutions. Modern technology—including the Internet and social media platforms—has both empowered and emboldened foreign governments and their agents in their attempts to affect U.S. attitudes, behaviors, and decisions in new and troubling ways.

The Department of Justice plays an important role in protecting the Nation's democratic processes from malign foreign influence operations. While the States, under the Constitution, have primary jurisdiction over the administration of elections,[1] the Department for decades has enforced federal criminal laws involving certain forms of ballot fraud.[2] We will continue our traditional commitment to combating such frauds, including any that foreign governments or their agents may attempt to perpetrate. (*See* page 4).

Foreign cyber-enabled and other active efforts to influence our democratic processes, including our elections, demand an urgent response. In the following pages, we provide background on malign foreign influence operations generally; outline five distinct types of foreign influence operations aimed at our elections or at broader political issues in the United States; and describe the Department's protective efforts with respect to such operations, including efforts designed to protect the upcoming 2018 midterm elections. We also announce a Department policy regarding the factors to be considered in disclosing malign foreign influence operations to victims, other affected individuals, and the public. This policy provides guideposts for Department action to expose and thereby counter foreign influence threats—consistent with the fundamental principle that we always must seek to act in ways that are politically neutral, compliant with the First Amendment, and designed to maintain the public trust.

Ultimately, one of the most effective ways to counter malign foreign influence operations is to shine a light on the activity and raise awareness of the threat. In order to prevail against our adversaries, all of society must work together: from government at all levels; to social media providers and others in the private sector; to political candidates and organizations; to, perhaps most significantly, an active and informed citizenry.

Malign Foreign Influence Operations

Foreign influence operations include covert actions by foreign governments intended to sow division in our society, undermine confidence in our democratic institutions, and otherwise affect political sentiment and public discourse to achieve strategic geopolitical objectives. Foreign influence operations can pose a threat to national security—and they can violate federal criminal law.[3] Operations

aimed at the United States are not new. These efforts have taken many forms across the decades, from funding communist newspapers and financing ostensibly independent nonprofit groups to promote favored policies, to more recent efforts at creating and operating false U.S. personas on Internet sites designed to attract U.S. audiences and spread divisive messages. The nature of the problem, however—and how the U.S. government must combat it—is changing, as advances in technology allow foreign actors to reach unprecedented numbers of Americans covertly and without setting foot on U.S. soil. Fabricated news stories and sensational headlines like those sometimes found on social media platforms are just the latest iteration of a practice foreign adversaries have long employed in an effort to discredit and undermine individuals and organizations in the United States. Although the tactics have evolved, the goals of these activities generally remain the same: to spread disinformation and to sow discord on a mass scale in order to weaken the U.S. democratic process, and ultimately to undermine the appeal of democracy itself.

Malign foreign influence operations need not favor one political figure, party, or point of view. Foreign adversaries can take advantage of social media platforms to send contrary (and sometimes false) messages simultaneously to different groups of users based on those users' political and demographic characteristics, with the goal of heightening tensions between different groups in our society. By exacerbating and inflaming existing divisions, foreign-promoted narratives seek to spread turmoil, mistrust, and acrimony. For example, Russian-affiliated social media activities have been detected promoting content on multiple sides of controversial issues including race relations and gun control.

As one component of this strategy, foreign influence operations have targeted U.S. elections. Elections are a particularly attractive target for foreign influence campaigns because they provide an opportunity to undermine confidence in a core element of our democracy: the process by which we select our leaders. As explained in a January 2017 Intelligence Community Assessment published by the Office of the Director of National Intelligence ("ODNI") addressing Russian interference in the 2016 U.S. presidential election, Russia has had a "longstanding desire to undermine the U.S.-led liberal democratic order," and that nation's recent election-focused "activities demonstrated a significant escalation in directness, level of activity, and scope of effort compared to previous operations."[4] Russia's foreign influence campaign, according to this assessment, "followed a longstanding Russian messaging strategy that blends covert intelligence operations—such as cyber activity—with overt efforts by Russian Government agencies, state-funded media, third-party intermediaries, and paid social media users or 'trolls.'" [5]

Malign foreign influence operations did not begin in 2016, but the Internet-facilitated operations in that year were unprecedented in scale. The threat such operations pose to our society is unlikely to diminish. As the Director of National Intelligence recently observed, "Influence operations, especially through cyber means, will remain a significant threat to U.S. interests as they are low-cost, relatively low-risk, and deniable ways to retaliate against adversaries, to shape foreign

perceptions, and to influence populations."[6] "Russia probably will be the most capable and aggressive source of this threat in 2018, although many countries and some nonstate actors are exploring ways to use influence operations, both domestically and abroad."[7] These actions require a strong and sustained response.

Types of Foreign Influence Operations Targeting Democratic and Electoral Processes

In advance of the 2018 midterm elections, the Department is mindful of ODNI's assessment that "Moscow will apply lessons learned from its campaign aimed at the U.S. presidential election to future influence efforts in the United States and worldwide, including against U.S. allies and their election processes."[8] The Intelligence Community ("IC") has recently assessed that Russia views the 2018 midterm elections as a potential target for continued influence operations.[9] Russia's strategy for conducting foreign influence operations against the United States, which may well inspire other countries to pursue similar operations, includes a broad spectrum of activity targeting U.S. democratic and electoral processes. We categorize such activity as follows:

1. Cyber operations targeting election infrastructure. Cyber operations could seek to undermine the integrity or availability of election-related data. For example, adversaries could employ cyber-enabled or other means to target election-associated infrastructure, such as voter registration databases and voting machines, or to target the power grid or other critical infrastructure in order to impair an election. Operations aimed at removing otherwise eligible voters from the rolls or attempting to manipulate the results of an election (or even simply spreading disinformation suggesting that such manipulation has occurred) could undermine the integrity and legitimacy of our free and fair elections, as well as public confidence in elec-

Credit: Cyber Threat Intelligence Integration Center

Foreign adversaries could target these categories of potential targets—or others—to interfere in U.S. elections through cyber operations.

DEPARTMENT OF JUSTICE PROGRAM FOR COMBATING BALLOT FRAUD

"Every voter in a federal . . . election, . . . whether he votes for a candidate with little chance of winning or for one with little chance of losing, has a right under the Constitution to have his vote fairly counted, without its being distorted by fraudulently cast votes." *Anderson v. United States,* 417 U.S. 211, 227 (1974). The Department has a longstanding program for predicating, investigating, and prosecuting ballot fraud schemes—which may overlap with a criminal or national security investigation into a foreign influence operation. The Department's ballot fraud program brings together several components, including the Federal Bureau of Investigation ("FBI"); the Criminal Division's Public Integrity Section ("PIN"); United States Attorney's Offices around the nation; the Civil Rights Division ("CRT"); and the Department of Homeland Security ("DHS"). (Each component's specific role in the program is described in the endnotes.[16])

In the weeks and months leading up to the 2018 midterm elections, these components will plan responses to election-related issues and identify lines of coordination and communication. On Election Day, they and a commissioner from the U.S. Election Assistance Commission will arrange regular secure video teleconferences with Department leadership and other agencies, including the National Security Council. Other PIN and CRT managers and personnel also will be available throughout the period to answer telephone calls about suspected ballot fraud activity and to respond to questions from federal prosecutors and law enforcement agents, who in turn will be in close communication with state and local partners.

tion results. To our knowledge, no foreign government has succeeded in perpetrating ballot fraud, but the risk is real.

2. Cyber operations targeting political organizations, campaigns, and public officials. Cyber operations could also seek to compromise the confidentiality or integrity of targeted groups' or targeted individuals' private information. For example, adversaries could conduct cyber or other operations against U.S. political organizations and campaigns to steal confidential information and use that information, or alterations thereof, to discredit or embarrass candidates, undermine political organizations, or impugn the integrity of public officials. The IC has assessed that, during the 2016 election cycle, "Russia's intelligence services conducted cyber operations against targets associated with the 2016 U.S. presidential election, including targets associated with both major U.S. political parties."[10]

3. Covert influence operations to assist or harm political organizations, campaigns, and public officials. Adversaries could also conduct covert influence operations to pro-

vide assistance that is prohibited from foreign sources to American political organizations, campaigns, and government officials. These operations might involve covert offers of financial, logistical, or other campaign support to—or covert attempts to influence the policies, positions, or opinions of—unwitting politicians, party leaders, campaign officials, or the public. For example, a federal grand jury indictment in February 2018 of thirteen Russian nationals recounts, among other things, instances in which Russians allegedly provided covert assistance and financial support to unwitting U.S. persons, unwitting individuals associated with a presidential campaign, and other unwitting political activists seeking to coordinate political activities.[11] The indictment also alleges that the Russians sought to discourage some Americans from voting in the 2016 presidential election, and denigrated certain candidates while supporting others. Russian actors also allegedly staged political rallies inside the United States while posing as U.S. grassroots entities and organized rallies inside the United States *after* the presidential election, both in protest of the election results and in support of the results.[12] Such covert influence operations could be reinforced by the use of "bots," which are automated programs that can expand and amplify social media messaging and bolster desired narratives. These operations can also be amplified by stolen information illicitly acquired through illegal cyber operations targeting government institutions, media, and political organizations or campaigns. Foreign agents could then use this stolen information to reinforce divisive narratives through systematic, controlled leaks timed to maximize political damage.

4. Covert influence operations, including disinformation operations, to influence public opinion and sow division. Using false U.S. personas, adversaries could covertly create and operate social media pages and other forums designed to attract U.S. audiences and spread disinformation or divisive messages. This could happen in isolation or in combination with other operations, and could be intended to foster specific narratives that advance foreign political objectives, or could be intended simply to turn citizens against each other. These messages need not relate directly to political campaigns. They could seek to depress voter turnout among particular groups, encourage third-party voting, or convince the public of widespread voter fraud to undermine confidence in election results. These messages could target discrete U.S. populations based on their political and demographic characteristics. They may mobilize Americans to sign online petitions and join issue-related rallies and protests, or even to incite violence. For example, advertisements from at least 2015 to 2017 linked to a Russian organization called the Internet Research Agency focused on divisive issues, including illegal immigration and gun rights, among others, and targeted those messages to groups most likely to react.

5. Overt influence efforts, such as the use of lobbyists, foreign media outlets, and other organizations, to influence policymakers and the public. Finally, adversaries could use state-owned or state-influenced media outlets, or employ lobbyists or lobbying firms, to reach U.S. policymakers or the public. Foreign governments can disguise these efforts as independent while using them to promote

divisive narratives and political positions helpful to foreign objectives. Overt influence efforts by foreign governments—including by our adversaries—may not be illegal, provided they comply with the Foreign Agents Registration Act ("FARA"),[13] and with Federal Communications Commission regulations. However, the American people should be fully aware of any foreign government source of information so they can evaluate that source's credibility and significance for themselves.

The Department of Justice's Role in Countering Malign Foreign Influence Operations

The Department of Justice has a significant role in investigating and disrupting foreign government activity in the United States that threatens U.S. national security. In particular, the Department has an important role in identifying and combating malign foreign influence operations, and in enforcing federal laws that foreign agents may violate when engaging in such operations.

Consistent with its longstanding mission, the Department has broad authorities in this area that encompass both its law enforcement and counterintelligence responsibilities:

- The FBI is the primary investigative agency of the federal government and is authorized to investigate all violations of federal laws that are not exclusively assigned to another federal agency. *See* 28 U.S.C. § 533. In addition, 28 C.F.R. § 0.85(d) designates the FBI to take charge of investigative work in matters relating to espionage, sabotage, subversive activities, and related matters.

- Various federal statutes authorize the FBI to conduct investigations of federal crimes, make seizures and arrests, and serve warrants, both under national security authorities (title 50 of the U.S. Code) and law enforcement authorities (title 18 of the U.S. Code). For example, the FBI has primary investigative authority for all computer network intrusions relating to threats to national security, including "cases involving espionage, foreign counterintelligence, [and] information protected against unauthorized disclosure for reasons of national defense or foreign relations . . ." 18 U.S.C. § 1030(d)(2).

- Executive Order ("E.O.") 12333, as amended, establishes the FBI as the lead counterintelligence agency within the United States, and authorizes the FBI to conduct counterintelligence activities, collect foreign intelligence, or support foreign intelligence collection requirements of other agencies within the IC, and produce and disseminate foreign intelligence and counterintelligence. *See* E.O. 12333, § 1.7(g).

- These lead responsibilities are also reflected in presidential policies, such as Presidential Policy Directive ("PPD")-41 and PPD-21.

Working closely with our IC partners, the Department uses these authorities to identify, analyze, and disrupt the most significant threats from foreign influence operations. As explained below, the Department can act against these threats in several ways, either using its own authorities or supporting the

actions of other agencies. The Department also uses its investigative authority to develop information that can inform private sector efforts to guard against or deter foreign influence operations.

First, the Department's investigations may reveal conduct that warrants criminal charges. Criminal charges not only are a tool the Department uses to pursue justice, but also can help deter similar conduct in the future. We will work with our international partners to obtain custody of foreign defendants whenever possible. Those who seek to avoid justice in U.S. courts will find their freedom of travel significantly restricted. Criminal charges also provide the public with information about the illegal activities of foreign actors we seek to hold accountable.

Second, in some cases, the Department's investigations can support other U.S. government agencies' actions, such as financial sanctions or diplomatic and intelligence efforts. After a federal grand jury indicted thirteen Russians in connection with their alleged influence activities, for example, the Secretary of the Treasury imposed financial sanctions against those individuals under an executive order that authorizes sanctions for malicious cyber-enabled activity. The Department of the Treasury's actions blocked all property and interests in property of the designated persons subject to U.S. jurisdiction, and prohibited U.S. persons from engaging in transactions with the sanctioned individuals. In addition, the State Department often uses information from our investigations and criminal indictments in diplomatic efforts to attribute malign conduct to foreign adversaries, to build consensus with other nations to condemn such activities, and to build coalitions to counter such activities. Likewise, we work closely with DHS to share information about foreign influence operations in furtherance of DHS's election security mission.

Third, the Department's investigations produce information about threats and vulnerabilities that we can share with State and local election officials, political organizations, and other potential victims. Because these entities lack the FBI's investigative resources and legal authorities, sharing investigative information about the nature of the threat posed by foreign influence operations can help these entities detect and prevent operations that target them.

Fourth, the Department maintains strategic relationships with social media providers that reflect the private sector's critical role in addressing this threat. Social media providers have unique insight into their own networks and bear the primary responsibility for securing their own products, platforms, and services. The FBI can assist the providers' voluntary efforts to identify foreign influence activity and to enforce terms of service that prohibit the use of their platforms for such activities. This approach is similar to the Department's recent approaches in working with providers to address terrorist use of social media, and more traditional collaboration to combat child pornography, botnets, Internet fraud, and other misuse of digital infrastructure. By providing information about potential threats, the Department can help social media providers respond to malign use of their platforms, identify foreign influence

operations on those platforms, share information across diverse products and services, and better ensure their users are not exposed to unlawful foreign influence.

Finally, information developed in our investigations can be used—either by the Department or in coordination with the Intelligence Community and other government partners—to help protect the public by exposing the nature of the foreign influence threat. The Department may alert victims or targets about foreign influence operations consistent with its longstanding policies and practices. As discussed below, in certain circumstances, public disclosure and attribution can also be an important means of countering the threat and rendering those operations less effective.

The Department of Justice's Framework to Counter Malign Foreign Influence Operations

The Department is preparing ahead of the 2018 midterm elections to ensure that we address as effectively as possible the five distinct types of foreign influence operations described above. To underscore this priority, the FBI in November 2017 established the Foreign Influence Task Force ("FITF"), which serves as the central coordinating authority within the FBI for investigations concerning foreign influence operations. The FITF integrates the FBI's cyber, counterintelligence, counterterrorism, and criminal law enforcement resources to ensure that the Department better understands the threat presented by malign foreign influence operations. An important part of the FITF's responsibility is coordinating the Department's counter-foreign influence efforts with other federal agencies, including DHS, the State Department, the National Security Agency, and the Central Intelligence Agency. The FBI is also responsible for developing strategic relationships with state and local authorities, international partners, and the private sector, including social media and other technology companies, as part of a comprehensive approach to combating the foreign influence problem.

Armed with a deeper understanding of our foreign adversaries' operational methods and committed to leveraging the full range of our authorities, the Department has developed a strategic framework for countering foreign influence operations. *See* **Fig. 1**. This framework seeks to employ the Department's longstanding authorities proactively to pursue aggressive countermeasures—using traditional law enforcement tools, sharing information with potential victims and the private sector where appropriate, and exposing and attributing foreign influence operations where doing so is in the national interest. The Department's strategy aims to increase the resilience of democratic and election processes against the foreign influence threat, while recognizing that we cannot expect to eliminate those activities unless the responsible foreign governments alter their behavior.

1. Cyber operations targeting election infrastructure. Although the States are responsible for administering elections, and DHS has the federal government lead for assisting election officials in securing their systems, the FBI has the primary responsibility for investigating our foreign adversaries'

Figure 1:

Department of Justice Framework to Counter Malign Foreign Influence Operations

Cyber operations targeting election infrastructure (integrity and availability of data)	Cyber operations targeting political parties, campaigns, and public officials (confidentiality of data)	Covert influence operations to assist or harm political organizations, campaigns and public officials	Covert influence operations to influence public opinion and sow division	Overt influence efforts to influence policymakers and the public
DOJ and FBI Actions • Identify threats and warn potential targets (state officials), with DHS. • Investigate and disrupt intrusions and attacks, alerting victims consistent with applicable guidance. • Prosecute where possible. • Respond to reports of election day crimes (e.g. voter suppression, computer intrusions).	**DOJ and FBI Actions** • Identify threats and warn potential targets, with DHS. • Investigate and disrupt intrusions and attacks, alerting victims consistent with applicable guidance. • Prosecute where possible. • Raise awareness about malicious cyber operations, mitigation, and maintaining "cyber hygiene."	**DOJ and FBI Actions** • Investigate and disrupt activity by unregistered foreign agents. • Brief potential targets, consistent with applicable guidance. • Prosecute where possible. • Raise awareness about malicious cyber operations, mitigation, and maintaining "cyber hygiene."	**DOJ and FBI Actions** • Investigate and, as appropriate, disrupt foreign influence operations. • Attribute and expose activity, consistent with applicable guidance. • Prosecute where possible. • Notify social media, other providers of foreign influence operations and other abuse of their platforms.	**DOJ and FBI Actions** • Investigate possible FARA violations. • Prosecute where possible. • Compel registration as appropriate.
Other Agencies and Their Activities • IC produces intelligence on malicious cyber operations. • DHS shares intelligence (warnings) and best practices with victims and assists with recovery efforts *after* an intrusion (if requested). • Possible diplomatic, financial, or operational responses.	**Other Agencies and Their Activities** • IC produces intelligence on malicious cyber operations. • DHS shares intelligence (warnings) and best practices with victims and assists with recovery efforts *after* an intrusion (if requested). • Possible diplomatic, financial, or operational responses.	**Other Agencies and Their Activities** • IC produces intelligence on foreign influence efforts, goals. • DHS and State Dept. conduct outreach on trends in influence operations to domestic and foreign audiences. • Possible diplomatic, financial, or operational responses.	**Other Agencies and Their Activities** • DHS and State Dept. conduct outreach on trends in influence operations to domestic and foreign audiences. • DHS provides tools to private industry to protect against malign influence. • Possible diplomatic, financial, or operational responses.	**Other Agencies and Their Activities** • DHS and State Dept. conduct outreach on trends in influence operations to domestic and foreign audiences. • State Dept. responds to violations of norms by foreign actors.
Key Considerations • States own the election systems and are responsible for their administration and security.	**Key Considerations** • Private parties own systems and data and are responsible for their security. • Limited ability to protect against misuse of stolen information.	**Key Considerations** • May require cooperation of affected individuals and organizations to counter the threat. • Many engagements with foreign governments are legitimate.	**Key Considerations** • Technology companies bear primary responsibility for securing their own products, platforms, and services.	**Key Considerations** • Open communications by registered foreign media may be lawful.

efforts to target election infrastructure. In the event of a known or suspected cyber incident, the FBI will investigate the intrusion and will alert targets of the intrusions where appropriate. Prosecutors will follow the *Principles of Federal Prosecution*[14] in determining whether federal criminal charges are appropriate. The FBI also may identify threats and vulnerabilities to election infrastructure in the course of other criminal or intelligence investigations. Consistent with the Department's disclosure policy (described below), it will attempt to warn State and local officials who operate election systems about attempts to penetrate their systems and to share appropriate information about vulnerabilities they should patch or mitigate. In this regard, the FBI works closely with DHS and with the U.S. Election Assistance Commission, which certifies voting systems and establishes voting system guidelines.

To that end, in February 2018, the FBI, together with DHS and the IC, provided classified briefings to election officials from all 50 States to help increase awareness of foreign adversary intent and capabilities against the States' election infrastructure, as well as actions State and local officials can undertake to mitigate those threats. Establishing close relationships with those officials, in partnership with DHS, is critical because the Department's ability to identify and disrupt cyber actors who target election infrastructure requires the officials who operate that infrastructure to promptly share threat information with the FBI. The Department has emphasized the need for State and local officials promptly to share threat information with the FBI's National Cyber Investigative Joint Task Force ("NCIJTF"). NCIJTF includes over 20 partnering agencies from across law enforcement, the IC, and the Department of Defense, with representatives who are co-located and work jointly to accomplish the organization's mission from a whole-of-government perspective.

Establishing close relationships with State and local officials is also important to enable the Department to respond quickly to a major cyber intrusion before or during an election. The Department works closely with DHS in connection with such incidents. The Department will continue to work with DHS and State and local officials to plan what they should do, whom they should contact, and what assistance they may seek in the event of a significant intrusion into their systems. The FBI's general incident response activities are described in greater detail in Chapter 4.

2. Cyber operations targeting political organizations, campaigns, and public officials. The FBI investigates computer intrusions and attacks against U.S. victims, using its broad investigative authority and leveraging its close relationship with other IC agencies that have the authority to collect foreign intelligence outside the United States. Federal prosecutors may then charge the perpetrators, as appropriate. The FBI also alerts victims where possible and helps them respond to intrusions, often working closely with DHS, and provides threat information when necessary to address a specific threat or incident.

The FBI is working with DHS to ensure that political organizations and individuals within such organizations whom foreign adversaries may target are aware of the specific cyber

DEPARTMENT OF JUSTICE POLICY REGARDING NON-INTERFERENCE WITH ELECTIONS

The Department of Justice has a strong interest in the prosecution of election-related crimes, such as those involving federal and State campaign finance laws, federal patronage laws, and corruption of the election process, and Department employees must safeguard the Department's reputation for fairness, neutrality, and non-partisanship.

Partisan political considerations must play no role in the decisions of federal investigators or prosecutors regarding any investigations or criminal charges. Law enforcement officers and prosecutors may never select the timing of investigative steps or criminal charges for the purpose of giving an advantage or disadvantage to any candidate or political party.

For further guidance, prosecutors and law enforcement officers may contact the Criminal Division's Public Integrity Section. More detailed guidance is also available in sections 1-4.000 and 9-85.000 of the United States Attorneys' Manual, and in a treatise published by the Department called FEDERAL PROSECUTION OF ELECTION OFFENSES (8th ed. 2017).[17]

threats and vulnerabilities we are monitoring. These efforts have included providing defensive briefings to major political organizations such as the Republican and Democratic National Committees.

3. Covert influence operations to assist or harm political organizations, campaigns, and government officials. The FBI counters the activities of foreign governments and their proxies by proactively investigating unregistered foreign agents in the United States, alerting these foreign agents' targets (or intended targets) where appropriate, and raising public awareness of foreign influence methods and effective countermeasures both through appropriate enforcement actions and through assistance to other federal agencies and State or local authorities with enforcement authority.

The Department will aggressively enforce federal laws that require foreign agents to register with the U.S. government and that prohibit foreign nationals from tricking unwitting Americans into participating in, or accepting support from, foreign influence efforts. Along those lines, the Department has stepped up enforcement efforts against individuals and entities that had not fulfilled their obligations under the Foreign Agents Registration Act ("FARA"), including by educating prosecutors and agents nationwide about the importance of the statute and how to investigate it; expanding our outreach to individuals and entities who may be required to register; and achieving the registrations of sophisticated individuals and entities that had not fulfilled their legal obligations, including the American agents of Russian state-funded media networks (RT and Sputnik). Going forward, we will increase FARA awareness and compliance through increased outreach,

by making additional advisory opinions public, and by issuing guidance if appropriate under Department policy. In addition, we will investigate and prosecute criminal violations of FARA and other laws that restrict the activities of foreign agents acting within the United States.

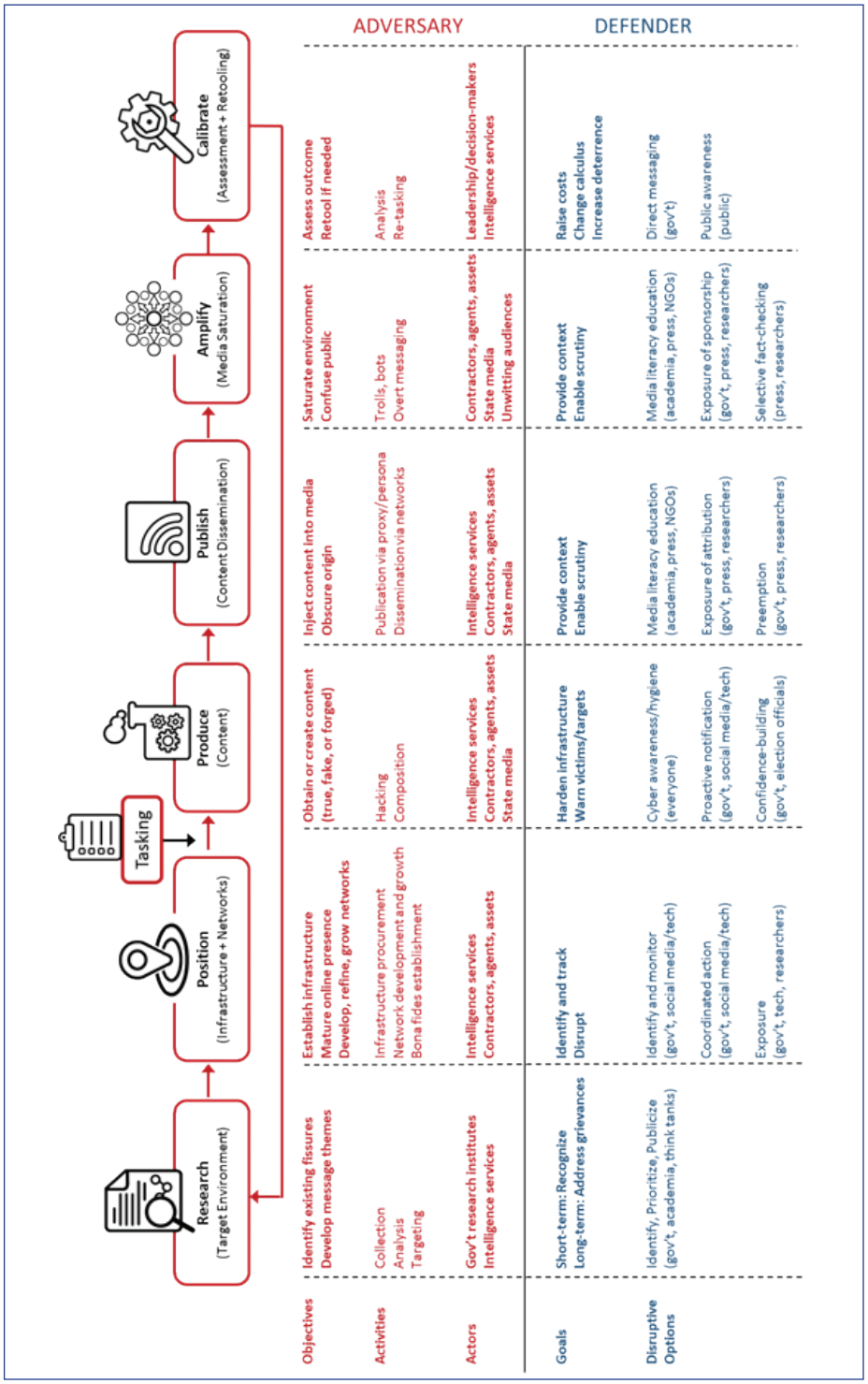
The Department also will seek to increase understanding of the foreign intelligence threat in order to reduce the effectiveness of covert activities and efforts to obscure the true motivation and origin of foreign influence operations. The FBI can provide defensive counterintelligence briefings to political organizations and campaigns as necessary to protect against and improve awareness of the foreign influence threat. In addition, the FBI continues to pursue criminal and traditional counterintelligence investigations to address the range of potential covert operations targeting political organizations.

4. Covert influence operations, including disinformation operations, to influence public opinion and sow division. Depending on the facts, a foreign government's efforts to use the Internet as part of a hostile effort to multiply its propaganda's malign influence on the American public may violate a number of federal laws on which the Department may base criminal investigations and prosecutions. The Department is also considering whether new criminal statutes aimed more directly at this type of activity are needed.

The Department has crafted a strategy to counter each phase of the foreign malign influence campaign cycle. *See* **Fig. 2**. While the success of a foreign influence campaign via the Internet and social media depends heavily on the adversary's ability to obscure the true motivation and origin of its activities—something the Internet can facilitate—the infrastructure of online accounts required to carry out such a campaign also provides the Department with opportunities for identification and disruption. For example, the FBI and IC partners may be able to identify and track foreign agents as they establish their infrastructure and mature their online presence, in which case authorities can work with social media companies to illuminate and ultimately disrupt those agents' activities, including through voluntary removal of accounts that violate a company's terms of service.

In addition to these activities, in some circumstances, public exposure and attribution of foreign influence operations, and of foreign governments' goals and methods in conducting them, can be an important means of countering the threat and rendering those operations less effective. Of course, partisan politics must play no role in the decision whether to disclose the existence of a foreign influence operation, and such disclosures must not be made for the purpose of conferring any advantage or disadvantage on any political or social group. In addition, the Department must seek to protect intelligence sources and methods and operational equities, and attribution itself may present challenges. It is also important not to take actions that merely exacerbate the impact of a foreign influence operation, or that re-victimize its victims. Given the competing in-

Figure 2: The Malign Foreign Influence Campaign Cycle



terests sometimes at stake, the Department has established a formal policy on the disclosure of foreign influence operations to guide its actions in this critically important area. That policy is found at pages 16–17.

5. Overt influence efforts, such as the use of foreign media outlets to influence policymakers and the public. Overt foreign government efforts to influence the American public or policymakers may be lawful so long as the relevant government complies with U.S. laws requiring public disclosure, along with other applicable laws. When foreign media outlets or lobbyists act as agents of foreign governments, they may be required to register as foreign agents under FARA. Media outlets with links to China, Japan, Russia, and South Korea have done so. Apart from enforcing such laws, the Department—in concert with the U.S. government as a whole, as well as with American society more broadly—can help increase public understanding of foreign influence operations.

Conclusion

The nature of foreign influence operations will continue to change as technology and our foreign adversaries' tactics change. Our adversaries will persist in seeking to exploit the diversity of today's information space, and the tactics and technology they employ will continue to evolve.

The Department plays an important role in combating foreign efforts to interfere in our elections, but it cannot alone solve the problem. There are limits to the Department's role—and the role of the U.S. government—in addressing foreign influence operations aimed at sowing discord and undermining our Nation's institutions. Combating foreign influence operations requires a whole-of-society approach that relies on coordinated actions by federal, State, and local government agencies; support from potential victims and the private sector; and the active engagement of an informed public.

Even so, investigating and prosecuting those who violate our laws, disrupting particular operations, and exposing covert foreign activities can be useful in defending against this threat. It is therefore critical that the Department consistently evaluate existing law and policy governing its actions, as well as its strategic approach to the problem. In the short term, the Department must use all current authorities to counter the foreign influence threat, working closely with the IC, DHS, State and local governments, and where appropriate, the private sector.

We also must ensure that we are sharing information about the threat with potential victims, other affected individuals, and the public, consistent with our policies and our national security interests. In the longer term, we must consider what additional authorities or policies would be useful and appropriate to enable us to respond as effectively as possible to the foreign influence threat.

* * *

The story is told that a woman named Elizabeth Powel approached Benjamin Franklin when he was walking home after the Constitutional Convention in the summer of 1787. Powel asked Franklin what type of govern-

ment the Founders had created. Franklin replied: "A republic, madam, if you can keep it." Powel's question illustrates that it was not inevitable that our Nation would begin as a democratic republic. Franklin's answer reminds us that it is not inevitable that we will remain a democratic republic.[15]

Our Nation's democratic processes are strong. But the Constitution comes with a condition: we need to keep it. We are all keepers of the republic, and it is incumbent upon all of us, as a society, to counter the foreign influence threat. The Department of Justice will certainly play its part.

DEPARTMENT OF JUSTICE POLICY ON DISCLOSURE OF FOREIGN INFLUENCE OPERATIONS

Foreign influence operations include covert actions by foreign governments intended to sow divisions in our society, undermine confidence in our democratic institutions, and otherwise affect political sentiment and public discourse to achieve strategic geopolitical objectives. Such operations are often empowered by modern technology that facilitates malicious cyber activity and covert or anonymous communications with U.S. audiences on a mass scale from abroad.

Our Nation's democratic processes and institutions are strong and must remain resilient in the face of this threat. It is the policy of the Department of Justice to investigate, disrupt, and prosecute the perpetrators of illegal foreign influence activities where feasible. It is also the Department's policy to alert the victims and unwitting targets of foreign influence activities, when appropriate and consistent with the Department's policies and practices, and with our national security interests.

It may not be possible or prudent to disclose foreign influence operations in certain contexts because of investigative or operational considerations, or other constraints. In some circumstances, however, public exposure and attribution of foreign influence operations can be an important means of countering the threat and rendering those operations less effective.

Information the Department of Justice collects concerning foreign influence operations may be disclosed as follows:

- To support arrests and charges for federal crimes arising out of foreign influence operations, such as hacking or malicious cyber activity, identity theft, and fraud.
- To alert victims of federal crimes arising out of foreign influence operations, consistent with Department guidelines on victim notification and assistance.[18]
- To alert unwitting recipients of foreign government-sponsored covert support, as necessary to assist in countering the threat.
- To alert technology companies or other private sector entities to foreign influence operations where their services are used to disseminate covert foreign government propaganda or disinformation, or to provide other covert support to political organizations or groups.

DEPARTMENT OF JUSTICE POLICY ON DISCLOSURE OF FOREIGN INFLUENCE OPERATIONS, *Continued*

- To alert relevant Congressional committees to significant intelligence activities, consistent with statutory reporting requirements and Executive Branch policies.

- To alert the public or other affected individuals, where the federal or national interests in doing so outweigh any countervailing considerations.[19]

In performing these functions, the Department will be mindful of the following principles and policies:

- Partisan political considerations must play no role in efforts to alert victims, other affected individuals, or the American public to foreign influence operations against the United States. Such efforts must not be for the purpose of conferring any advantage or disadvantage on any political or social group or any individual or organization.

- In considering whether and how to disclose foreign influence operations, or the details thereof, the Department will seek to protect intelligence sources and methods, investigations, and other U.S. government operations.

- Foreign influence operations will be publicly identified as such only when the Department can attribute those activities to a foreign government with high confidence. Disinformation or other support or influence by unknown or domestic sources not acting on behalf of a foreign government is beyond the scope of this policy.

- Where a criminal or national security investigation during an election cycle is at issue, the Department must also be careful to adhere to longstanding policies regarding the timing of charges or taking overt investigative steps.[20]

The Department (including the FBI) will not necessarily be the appropriate entity to disclose information publicly concerning a foreign influence operation. Where a Department component is considering whether to alert the general public to a specific foreign influence operation, consultation with the National Security Division is required. Nothing in this policy is intended to impair information sharing undertaken by Department components for investigative or intelligence purposes.

NOTES

[1] *See* U.S. Const. art. I, § 4 (Congressional elections) & art. II, § 4 (Presidential elections).

[2] The term "ballot fraud" in this context includes fraud in the processes by which voters are registered or by which votes are cast or tabulated.

[3] Foreign influence operations, while not always illegal, can implicate several U.S. federal criminal statutes, including (but not limited to): 18 U.S.C. § 371 (conspiracy); 18 U.S.C. § 951 (acting in the United States as an agent of a foreign government without prior notification to the Attorney General); 18 U.S.C. § 1001 (false statements); 18 U.S.C. § 1028A (aggravated identity theft); 18 U.S.C. § 1030 (computer fraud and abuse); 18 U.S.C. §§ 1343, 1344 (wire fraud and bank fraud); 18 U.S.C. § 1519 (destruction of evidence); 18 U.S.C. § 1546 (visa fraud); 22 U.S.C. § 618 (Foreign Agents Registration Act); 52 U.S.C. §§ 30109, 30121 (soliciting or making foreign contributions to influence federal elections, or donations to influence State or local elections).

[4] Office of the Director of National Intelligence, Background to "Assessing Russian Activities and Intentions in Recent U.S. Elections": The Analytic Process and Cyber Incident Attribution ii (Jan. 2017) ("ODNI Report"), available at: https://www.dni.gov/files/documents/ICA_2017_01.pdf (last accessed June 29, 2018).

[5] ODNI Report at 2; *see also* U.S. House of Representatives Permanent Select Committee on Intelligence, Report on Russian Active Measures viii (March 2018) ("In 2015, Russia began engaging in a covert influence campaign aimed at the U.S. presidential election. The Russian government, at the direction of Vladimir Putin, sought to sow discord in American society and undermine our faith in the democratic process."), available at: https://intelligence.house.gov/uploadedfiles/final_russia_investigation_report.pdf (last accessed June 29, 2018); Minority Members of the House Permanent Select Committee on Intelligence, Report on Russian Active Measures 12 (March 2018), available at: https://democrats-intelligence.house.gov/uploadedfiles/20180411_-_final_-_hpsci_minority_views_on_majority_report.pdf (last accessed June 29, 2018) (summarizing Russian covert cyber efforts and other intelligence and social media operations during the 2016 elections); U.S. Senate Select Committee on Intelligence, Russian Targeting of Election Infrastructure During the 2016 Election: Summary of Initial Findings and Recommendations 1 (May 2018) ("In 2016, cyber actors affiliated with the Russian Government conducted an unprecedented, coordinated cyber campaign against state election infrastructure . . . This activity was part of a larger campaign to prepare to undermine confidence in the voting process. The Committee has not seen any evidence that vote tallies were manipulated or that voter registration information was deleted or modified."), available at: https://www.burr.senate.gov/imo/media/doc/RussRptInstlmt1-%20ElecSec%20Findings,Recs2.pdf (last accessed June 29, 2018).

[6] Daniel R. Coats, Dir. of National Intelligence, "Statement for the Record: Worldwide Threat Assessment of the U.S. Intelligence Community," at 11 (Feb. 13, 2018), available at: https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf (last accessed June 29, 2018).

[7] *Id.*

[8] ODNI Report at 5.

[9] Daniel R. Coats, Dir. of National Intelligence,

"Annual Threat Assessment: Opening Statement," *Worldwide Threats: Hearing Before the Senate Select Comm. on Intelligence*, 115TH CONG. (Feb. 13, 2018), at 18, available at: https://www.dni.gov/files/documents/Newsroom/Testimonies/ATA2018-asprepared.pdf (last accessed June 29, 2018).

[10] ODNI Report at 2.

[11] Indictment in *United States v. Internet Research Agency*, et al., No. 18-cr-32-DLF (D.D.C. Feb. 16, 2018), available at: https://www.justice.gov/file/1035477/download (last accessed June 29, 2018).

[12] *Id.*

[13] 22 U.S.C. § 611 *et seq*.

[14] *See* "Principles of Federal Prosecution," U.S. ATTORNEYS' MANUAL, TITLE 9, SECTION 27.000, available at: https://www.justice.gov/usam/usam-9-27000-principles-federal-prosecution (last accessed June 29, 2018).

[15] This story and its associated lessons are recounted in Rod J. Rosenstein, Deputy Attorney General, "Constitution Day Address," National Constitution Center (Sept. 18, 2017), available at: https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-delivers-constitution-day-address (last accessed June 29, 2018).

[16] As part of the Department's ballot fraud program, the **FBI** must maintain an Election Crimes Coordinator ("ECC") in each of its Divisions. The ECCs are the Department's primary liaison with State and local police agencies, and election administrators, as well as with other federal agencies, in the field. They attend regular trainings, coordinate local task force communications with State and local counterparts during elections, and handle intake reporting of ballot fraud allegations from non-government groups or individuals. The FBI then investigates properly-predicated ballot fraud cases, in coordination with a local **U.S. Attorney's Office ("USAO").** The FBI and USAO are free to exercise their discretion to conduct a preliminary investigation after assessing the case and ensuring non-interference with the election process. They may pursue a full field and grand jury investigation, and seek charges, after consultation with the Criminal Division's **Public Integry Section ("PIN").** However, the FBI and other federal law enforcement agencies may not conduct investigations that would infringe the Department's non-interference with elections policy (*see* page 11), or that would unlawfully result in an armed federal presence at a polling site. *See* 18 U.S.C. § 592. For almost forty years, PIN has provided the field with an Election Crimes Branch Director. Pursuant to the United States Attorneys' Manual, the Director, assisted as needed by other managers and staff at PIN, functions as a mandatory consultant for the USAOs on all ballot fraud matters that progress beyond a preliminary investigation, see U.S.A.M. § 9-85.210, and as a subject matter expert available to provide advice and assistance to USAOs and the FBI. The Director coordinates and conducts mandatory live training with designated field personnel of the USAOs and FBI. The Director also leads an Election Day Watch program during federal election seasons to monitor and coordinate responses to election events while the polls are open on each federal election day. The Election Day Watch program is the Department's mechanism for ensuring consistent and efficient communication and coordination between interagency representatives, federal prosecutors and investigators in the field, and State and local partners. Each USAO must maintain a District Election Officer ("DEO") among its cadre of Assistant United States Attorneys. The DEOs are the Department's primary liaison with State and local counterparts in the field. They attend regular trainings, and as part of the Election Day

Watch program, coordinate local task force communications with State and local counterparts leading up to and during the elections. DEOs also coordinate press releases concerning election-day procedures to facilitate reporting to the federal government of ballot fraud allegations from non-government groups or individuals. The Voting Section and Criminal Section of the Department's **Civil Rights Division ("CRT")** coordinates regularly with PIN to ensure that ballot fraud allegations are routed to the best response entity. CRT maintains a hotline that operates all year, including throughout federal election days, to facilitate reporting of allegations of potential voting-related federal law violations. CRT's Voting Section also enforces the civil provisions of a wide range of federal statutes that protect the right to vote, including the Voting Rights Act; the National Voter Registration Act; the Uniformed and Overseas Citizens Absentee Voting Act; the Help America Vote Act; and the Civil Rights Act. CRT's Criminal Section enforces federal criminal statutes that prohibit voter intimidation and voter suppression based on race, color, national origin, or religion. Finally, the **Department of Homeland Security ("DHS")** recently has joined existing efforts to combat ballot fraud in the specific area of cyber threats. In particular, DHS provides advice and resources to State and local counterparts to assess the risks to their computer systems for voter registration, balloting, and tabulation. DHS also has certain resources for incident response, though the FBI has greater local resources and, under PPD-41, retains the lead on incident response.

[17] This treatise is available online at: https://www.justice.gov/criminal/file/1029066/download (last accessed June 29, 2018). The most relevant discussion can be found at pages 84-85: "The Justice Department's goals in the area of election crime are to prosecute those who violate federal criminal law and, through such prosecutions, deter corruption of future elections. The Department does not have a role in determining which candidate won a particular election, or whether another election should be held because of the impact of the alleged fraud on the election . . . . In investigating an election fraud matter, federal law enforcement personnel should carefully evaluate whether an investigative step under consideration has the potential to affect the election itself. Starting a public criminal investigation of alleged election fraud before the election to which the allegations pertain has been concluded runs the obvious risk of chilling legitimate voting and campaign activities. It also runs the significant risk of interjecting the investigation itself as an issue, both in the campaign and in the adjudication of any ensuing election contest . . . . Accordingly, overt criminal investigative measures ordinarily should not be taken in matters involving alleged fraud in the manner in which votes were cast or counted until the election in question has been concluded, its results certified, and all recounts and election contests concluded. Not only does such investigative restraint avoid interjecting the federal government into election campaigns, the voting process, and the adjudication of ensuing recounts and election contest litigation, but it also ensures that evidence developed during any election litigation is available to investigators, thereby minimizing the need to duplicate investigative efforts. Many election fraud issues are developed to the standards of factual predication for a federal criminal investigation during post-election litigation."

[18] *See Attorney General Guidelines for Victim and Witness Assistance* (May 2012), available at: https://www.justice.gov/sites/default/files/olp/docs/ag_guidelines2012.pdf (last accessed June 29, 2018); *see also* 42 U.S.C. § 10607 (Victims' Rights and Restitution Act).

[19] For example, there may be an important federal or national interest in publicly disclosing a foreign influence operation that threatens to un-

dermine confidence in the government or public institutions; risks inciting violence or other illegal actions; or may cause substantial harm, alarm, or confusion if left unaddressed. On the other hand, in some cases, public disclosure of a foreign influence operation may be counterproductive because it may amplify or otherwise exacerbate the foreign government's messaging, or may re-victimize the victim.

[20] *See,* e.g., U.S. Dept. of Justice, Federal Prosecution of Election Offenses 8-9, 84-85 (8th ed. 2017), quoted in *supra* note 17.

Chapter 2
Categorizing Sophisticated Cyber Schemes

Malign foreign influence operations represent a significant cyber-enabled threat to American society and national security. But they are not the only one. Every day, criminals and other hackers within the United States and around the world seek to use computers, smart devices, and other chip-enabled technology—as well as the networks that connect them—to victimize American consumers and businesses, or to do our government harm.

In this chapter, we describe some of the most prevalent and dangerous types of cybercrime schemes our Nation currently faces. Various actors, with varying motivations, perpetrate these schemes, targeting various categories of victims. All of these schemes, however, rely on the malicious, unauthorized use of computers to penetrate into another person's computer or network. This technical baseline provides a set of common operational techniques across the range of complicated cybercriminal plots. Indeed, in a threat landscape that constantly evolves and features a diverse set of actors, motivations, and targets, the prevalence of certain key techniques is a significant and rare constant.

Cybercrime Schemes

In the current landscape, cyber-enabled schemes tend to fall into one or more of five basic categories: (1) damage to computer systems; (2) data theft; (3) fraud/carding schemes; (4) crimes threatening personal privacy; and (5) crimes threatening critical infrastructure.

1. Damage to computer systems

Many cyber threats directly target computer systems and networks, seeking to damage the integrity or availability of data and services housed on those systems. For example, a **Distributed Denial of Service ("DDoS") attack** involves the orchestrated transmission of communications engineered to overwhelm the victim network's connection to the Internet in order to impair or disrupt that network's ability to send or receive communications. Because they require the near simultaneous and sustained sending of communications against a discrete target, DDoS attacks usually are launched by a large network of hijacked computers called a botnet. (For further discussion of botnets, see page 41.) Common targets of DDoS attacks include websites that the criminals wish to disable and push off-line, either because they disagree with the content, or because they wish to drive traffic to sites they prefer.

DDoS attacks can have crippling, far-reaching effects. In October 2016, for example, a massive DDoS attack targeting a U.S.-based company that controls much of the Internet's domain name system infrastructure brought down many of the world's best-known websites for several hours, including sites belong-

ing to Twitter, Pinterest, CNN, Fox News, and Netflix. The botnet used to launch this attack was originally created a few years before. The Department recently convicted the botnet's creators after the leader of the group admitted that he and his conspirators developed it in part to initiate powerful DDoS attacks "against business competitors and others against whom [they] held grudges."[1] They also used the botnet—which, in an alarming new twist, enlisted everyday so-called "Internet of Things" devices into its network of hijacked machines, thereby amplifying its strength by orders of magnitude[2]—to provide a source of revenue, either by renting it out to third-parties in exchange for payment, or by employing it to "extort hosting companies and others into paying protection money in order to avoid being targeted" by DDoS attacks.[3]

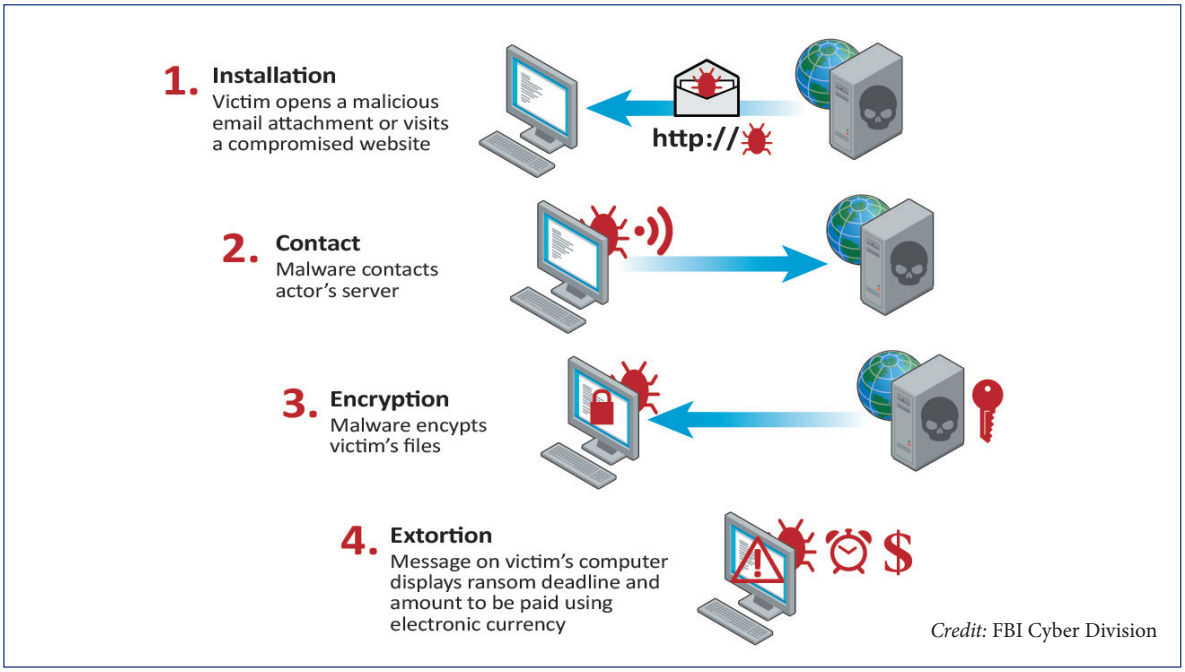
Hostile governments, too, may employ DDoS attacks to advance their geopolitical goals and undermine our national security. In March 2016, for example, a federal grand jury in New York indicted seven Iranian hackers belonging to two companies that worked for Iran's Islamic Revolutionary Guard Corps for their role in DDoS attacks targeting the public-facing websites of nearly fifty U.S. banks.[4] These DDoS attacks against the U.S. financial sector began in approximately December 2011, and occurred sporadically until September 2012, at which point they escalated in frequency to a near-weekly basis. On certain days during the DDoS campaign, victim computer servers were hit with massive amounts of traffic, which cut off hundreds of thousands of customers from online access to their bank accounts. These attacks collectively cost the banks tens of millions of dollars to remediate as they worked to neutralize and mitigate the attacks on their servers. In 2017, the Department of the Treasury added the seven hackers to the Office of Foreign Assets Control ("OFAC") Specially Designated National and Blocked Persons List.[5]

Malign actors also use **ransomware** to inflict damage to a victim's computer systems. Ransomware is malicious computer code (or "malware") that blocks a victim's access to data on its systems, typically by encrypting the data and demanding that the victim pay a ransom, often in the form of a difficult-to-trace virtual currency, to restore the data. *See* **Fig. 1**.

Ransomware can be delivered in a variety of ways, including through fraudulent e-mails. Such e-mails can be drafted to look like they are from trustworthy senders, containing malicious attachments or links that, once opened or clicked, activate the ransomware. Some variants also try, once they have gained a foothold in a victim's network, to spread laterally across the network to encrypt files on other computers or servers to which the victim's device has access. A second common method involves planting ransomware in hacked websites, which infect the computers of visitors to the sites. In addition, it is not uncommon for criminals to use botnet infrastructure and code to facilitate the widespread delivery of ransomware.

Like DDoS attacks, ransomware attacks can impose immense costs. For example, in 2017, the "WannaCry" ransomware attack spread rapidly and indiscriminately around the world over a mere four days. This campaign—which ultimately was attributed to

Figure 1: The Anatomy of a Ransomware Attack



Credit: FBI Cyber Division

the North Korean government—rendered useless "hundreds of thousands of computers in hospitals, schools, businesses, and homes in over 150 countries."[7] Total damages likely ran into the hundreds of millions of dollars. High-profile incidents such as the March 2018 attack that crippled Atlanta's city government make clear that ransomware schemes remain a threat.

Typically, cybercriminals run ransomware campaigns: the goal is to damage the victim's computer system in the short-term in order to get the victim to pay. If the scheme is to succeed, in other words, the victim needs to get their files back. By contrast, **destructive attacks**—another type of cyber threat that directly targets computer systems and networks—destroy the victim's data. For that reason, these attacks often are associated with nation states and other entities that have broader motivations. To be sure, destructive attacks may come disguised as ransomware campaigns; the malware linked to the notorious "NotPetya" attack launched by the Russian military in June 2017, for example, locked up its victims' files and purported to demand a ransom. It soon became clear, however, that this cyberattack was "meant to paralyze, not profit," as victims who tried to pay found it almost impossible to do so.[9] This attack, which was "part of the Kremlin's ongoing effort to destabilize Ukraine," resulted in "the most destructive and costly cyberattack in history," "causing billions of dollars in damage across Europe, Asia, and the Americas."[10] Similarly, the "WannaCry" attack described above did not prove to be very lucrative to the attackers. Rather, it was a reckless attack that resulted in havoc and

Credit: FBI Cyber Division

destruction; any money that was raised was purely a side benefit.[11]

Perhaps the most notorious example of a destructive attack launched against a U.S. company was the November 2014 cyberattack by North Korea on Sony Pictures Entertainment ("SPE"). This attack destroyed much of SPE's computer systems, compromised private information, released valuable corporate data and intellectual property, and threatened employees, customers, and film distributers with violence. The attackers stole a large number of files—which included private correspondence, unreleased films, salary records, and social security numbers—and released much of the information to the public, imposing significant financial and other consequences. The attack forced SPE to take its company-wide computer network offline and left thousands of its computers inoperable.

In response to the cyberattack on SPE, the U.S. government publicly attributed the incident to the North Korean government, and then sanctioned a North Korean government agency, two trading companies, and ten North Korean individuals.[13]

2. Data Theft

As the world grows increasingly reliant on digital technology, and as companies store ever larger quantities of data about their customers and other individuals, criminals have sought to steal and profit from control over that data. The past decade has witnessed numerous publicly reported instances of criminals hacking into computer systems and stealing **personally identifying information ("PII")** about hundreds of millions of individuals.

According to one report, there were at least 686 data breaches reported in the first quarter of 2018, resulting in the theft of as many as 1.4 billion records.[14] Stolen PII can include dates of birth, social security numbers, credit card numbers, e-mail addresses, drivers' license numbers, payroll and tax information, and even answers to security questions used to log into systems—namely, everything needed to misappropriate victims' identities, make fraudulent purchases (including filing fraudulent claims for tax refunds), and craft phishing and other social engineering attacks on specific targets. Breaches of major retailers can reveal transaction information and expose these companies to massive financial losses, while imposing upon members of the public the risk that their identities will be used to commit other financial crimes, with all of the associated impacts. Crimes of this sort are tremendously costly to all involved. According to one estimate, the average total cost in 2017 to a victim company from a data breach was approximately $7.35 million.[15] The Internet Crime Complaint Center ("IC3"), the FBI unit that receives and tracks cybercrime complaints from victims, received a total of 3,785 complaints of corporate data breach in 2017, with reported losses exceeding $60 million.[16]

Government agencies face similar threats. As agencies try to use new information technologies to make it easier for individuals and entities to submit and obtain information necessary for paying taxes, obtaining benefits, or providing services, the avenues for potential breaches dramatically increase. Of course, government agencies collect and store sensitive information concerning not only the general public, but also their own employees. This fact makes them valuable targets. For example, the U.S. Office of Personnel Management announced in 2015 it had been victimized through two separate but related cyberattacks that resulted in the theft of highly sensitive background investigation records of current, former, and prospective federal employees and contractors, as well as the theft of personnel data of over 21 million people.[17] Data breaches like these degrade public trust in government agencies.

Sometimes, nation states facilitate the work of criminals who seek to steal and profit from user data. In March 2017, the Department announced criminal charges against two officers of the Russian Federal Security Service ("FSB") and two additional conspirators involving computer hacking, economic espionage, and other offenses in connection with a conspiracy to access Yahoo's network as well as information concerning millions of individual webmail accounts.[18] Those charges revealed that officers from the FSB unit that serves as the FBI's point of contact in Moscow on cybercrime matters were using criminal hackers—one of whom already had been publicly charged in two separate investigations in the United States—to target American webmail providers and technology companies, among others.

The public revelation that FSB officers for years had worked with a wanted cybercriminal, and had allowed him to further victimize his targets (for example, by searching compromised accounts for credit card and other information that could be monetized), laid bare for the public and international com-

munity the nexus between the Russian state apparatus and the Russian criminal underworld. These charges also demonstrated that the Russian government has not always been a responsible stakeholder in the fight against international cybercrime. One of the indicted hackers was arrested in Canada and brought to the United States; he pled guilty to eight criminal counts in U.S. federal court in November 2017, and was sentenced to a five-year prison term in May 2018.[19] In December 2016, OFAC designated the FSB under a new executive order issued to expand the authority under E.O. 13694, which empowers the President to block the property of persons who engage in significant malicious cyber-enabled activities.[20] On March 15, 2018, the Department of the Treasury also designated the FSB pursuant to section 224 of the Countering America's Adversaries Through Sanctions Act, which targets cyber actors operating on behalf of the Russian government in particular.

Malign actors can also use data thefts to further terrorist acts. In June 2015, an ISIL-linked hacker named Ardit Ferizi stole PII belonging to tens of thousands of customers of a U.S. company, including members of the military and other government personnel. Ferizi subsequently culled the PII belonging to 1,300 particular individuals employed by the U.S. government and provided that information to Junaid Hussain, a now-deceased ISIL recruiter and attack facilitator. In August 2015, Hussain posted the names on Twitter in the name of the Islamic State Hacking Division with a message saying, in part: "We are in your emails and computer systems, watching and recording your every move, we have your names and addresses, we are in your emails and social media accounts, we are extracting confidential data and passing on your personal information to the soldiers of the khilafah, who soon with the permission of Allah will strike at your necks in your own lands!" Malaysian authorities detained Ferizi, who subsequently consented to extradition to the United States. He pleaded guilty and was sentenced to 20 years in prison for providing material support to ISIL, and for accessing a protected computer without authorization and obtaining information in order to provide material support to a designated foreign terrorist organization.[21]

THE COSTS OF INTELLECTUAL PROPERTY CRIME

Estimates vary regarding the size of economic loss that can be attributed to the theft of intellectual property and trade secrets. The Commission on the Theft of American Intellectual Property has estimated that the annual cost to the U.S. economy through the theft of trade secrets, and through counterfeit goods and pirated software, exceeds $225 billion and could be as high as $600 billion.[22] According to a cybersecurity industry report, the direct costs of cyber theft in 2014 for over 50 U.S.-based private and public sector organizations ranged from just under $2 million to $65 million each year per company, an increase of 82 percent over six years.[23] Pricewaterhouse Coopers estimated in 2014 that the United States lost between one and three percent of its gross domestic product each year due to trade secret theft.[24]

The **theft of intellectual property** represents another significant data theft problem. The two most notable types of cyber-enabled intellectual property crime are the infringement of copyrighted material over the Internet and the misappropriation of trade secrets stored in a digital format. Internet sites that profit from the unauthorized distribution of copyrighted movies, music, software, and other digital works can have a global reach, generate millions of dollars of illicit revenue for the operators, and cause extensive financial harm to the owners of the works being shared. While copyrighted works generally are intended to be accessible to the public under terms set by the copyright owner, trade secrets receive criminal protection specifically because they involve knowledge that is not known to the public and derive value from remaining secret.

Kim Dotcom, Finn Batato, Mathias Ortmann, Bram van der Kolk, and others are members of a worldwide criminal organization whose members allegedly engaged in criminal copyright infringement with estimated harm to copyright holders well in excess of $400 million, and which yielded over $175 million in illicit proceeds.[25] The conspirators operated a commercial website and service called Megaupload.com, which reproduced and distributed copies of popular copyrighted content without authorization and claimed at one time to account for four percent of total Internet traffic—including more than one billion total visits, 150 million registered users, and 50 million daily visitors. A federal grand jury charged members of the conspiracy with a number of conspiracy, racketeering, copyright infringement, money laundering, and fraud offenses. Dotcom and the others were arrested in 2012 in New Zealand, but their extraditions to the United States still remain on appeal in that nation. Despite delays in the criminal case, the Department of Justice has prevailed in a civil forfeiture action in U.S. federal court to forfeit the proceeds of the criminal conspiracy.

Following the takedown of Megaupload.com, other online piracy sites grew in popularity. On July 20, 2016, Artem Vaulin of Ukraine was arrested in Poland based on U.S. federal charges for conspiracy to commit criminal copyright infringement, conspiracy to commit money laundering, and criminal copyright infringement.[26] Vaulin is alleged to have run one of the world's most visited illegal file-sharing websites, Kickass Torrents ("KAT"), which was seized as part of the operation. KAT enabled users to illegally reproduce and distribute hundreds of millions of copyrighted motion pictures, video games, television programs, musical recordings, and other electronic media. Initial investigation indicates that the copyrighted material was collectively valued at well over $1 billion, and that the site, which was in the top 100 most frequently visited sites on the Internet, received more than 50 million unique visitors each month.

On the trade secret front, the Department obtained a conviction in January 2018 in U.S. federal court against a China-based manufacturer and exporter of wind turbines that stole trade secrets from a U.S.-based company. The Chinese company, Sinovel Wind Group Co. Ltd., conspired with others to steal proprietary wind turbine technology from the American corporate victim in order to produce its own wind turbines and to retrofit

existing wind turbines with stolen technology. These crimes cost the victim more than $1 billion in shareholder equity and almost 700 jobs—over half its global workforce.[27]

In addition, the Department has pursued charges not only against criminals seeking monetary gain, but also against nation-state actors engaged in economic espionage through cyber means. In May 2014, for example, a federal grand jury indicted five uniformed members of the Chinese military on charges of hacking and conducting economic espionage against large U.S. entities in the nuclear power, metal, and solar energy industries. The lengthy statement of charges described numerous specific instances where officers of the People's Liberation Army ("PLA") were alleged to have hacked into the computer systems of U.S. victims to steal

WANTED
BY THE FBI

Conspiring to Commit Computer Fraud; Accessing a Computer Without Authorization for the Purpose of Commercial Advantage and Private Financial Gain; Damaging Computers Through the Transmission of Code and Commands; Aggravated Identity Theft; Economic Espionage; Theft of Trade Secrets

WANG DONG
Aliases: Jack Wang, UglyGorilla"

SUN KAILIANG
Aliases: Sun Kai Liang, Jack Sun

WEN XINYU
Aliases: Wen Xin Yu, WinXYHappy , Win XY", Lao Wen

HUANG ZHENYU
Aliases: Huang Zhen Yu, hzy lhx"

GU CHUNHUI
Aliases: Gu Chun Hui, KandyGoo

DETAILS

On May 1, 2014, a grand jury in the Western District of Pennsylvania indicted five members of the People s Liberation Army (PLA) of the People s Republic of China (PRC) for 31 criminal counts, including: conspiring to commit computer fraud; accessing a computer without authorization for the purpose of commercial advantage and private financial gain; damaging computers through the transmission of code and commands; aggravated identity theft; economic espionage; and theft of trade secrets.

The subjects, Wang Dong, Sun Kailiang, Wen Xinyu, Huang Zhenyu, and Gu Chunhui, were officers of the PRC s Third Department of the General Staff Department of the People s Liberation Army (3PLA), Second Bureau, Third Office, Military Unit Cover Designator (MUCD) 61398, at some point during the investigation. The activities executed by each of these individuals allegedly involved in the conspiracy varied according to his specialties. Each provided his individual expertise to an alleged conspiracy to penetrate the computer networks of six American companies while those companies were engaged in negotiations or joint ventures or were pursuing legal action with, or against, state owned enterprises in China. They then used their illegal access to allegedly steal proprietary information including, for instance, e mail exchanges among company employees and trade secrets related to technical specifications for nuclear plant designs.

If you have any information concerning these individuals, please contact your local FBI office or the nearest American Embassy or Consulate.

Figure 2: Chinese Military Officers Charged with Hacking and Economic Espionage

trade secrets and sensitive, internal communications for commercial advantage or private financial gain. *See* **Fig. 2**. Although the five charged PLA officers remain at large, this case illustrated how the Department's independent investigations and actions can play an important role as part of a broader, coordinated approach designed to support American companies, deter our adversaries, and otherwise change their behavior.

The indictment sent a clear message that the state-sponsored theft of trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors, is unacceptable. This norm thereafter gained widespread acceptance, most notably in a bilateral agreement between the United States and China in September 2015,[28] and among the G20 at the Antalya Summit in Turkey in November 2015.[29] Although some U.S. cybersecurity firms indicate that computer intrusions by Chinese state-sponsored hackers targeting U.S. firms have decreased since then,[30] the U.S. government continues to monitor China's compliance with the norm, and with that nation's September 2015 commitment to cooperate on investigations of crimes emanating from its territory. To that end, in late 2017, the Department charged three Chinese nationals who worked for the purported Internet security firm known as Boyusec with stealing trade secrets and other confidential information from American firms until as recently as May 2017—long after the Chinese commitments of September 2015.[31] After the Department sought assistance from the Chinese authorities in investigating the allegations and "received no meaningful response,"[32] the Department acknowledged as much and unsealed the indictment, providing insight into the status of China's adherence to norms it purportedly had embraced.

3. Fraud/Carding Schemes

At the core of fraud lies deceit. It can manifest in an intent to deceive by those one knows and trusts, or, as is often the case with cybercrime, by criminals defrauding victims by abusing the Internet's lack of a trusted and effective means to authenticate another's identity. Online systems with weak authentication and few indications for determining another's true identity have opened the door for fraudsters to commit numerous crimes by faking their online identities or fraudulently adopting the identities of others. Cyber fraud schemes take many forms, including Nigerian-letter scams in which fraudsters e-mail victims claiming to be Nigerian government officials in need of assistance in transferring stolen funds out of Nigeria. Recipients who respond are encouraged to cover upfront the supposed expenses for the transfers themselves, upon the fraudulent promise of later repayment, and to provide personal banking information and other identifying information—which is later used to drain victims' bank accounts.[33] Other forms include frauds that convince victims to donate to fake charities, especially after natural disasters, and fraudulent online transactions or exchanges in which no payment is made to, or no good or service is received by, the victim.[34]

Other schemes entice victims to purchase investment and financial instruments, often

marketed with misleading claims of offering low-risk, high-reward guaranteed returns or overly consistent returns. Examples include Ponzi schemes, advance fee frauds, pyramid schemes, and market manipulation frauds. These schemes can target members of affinity groups, such as groups with a common religion or ethnicity, in order to exploit that supposed connection to build trust and operate the investment fraud against the victim.[35] Carding schemes are another major financial threat. These schemes involve criminals selling and purchasing hacked credit card information, typically through dark markets devoted to criminal activity, that is then used to commit fraudulent ATM transactions, purchase pre-paid gift cards, and buy goods that are then re-shipped to criminal organizations. In just one example, a group of Russian criminals hacked into systems at credit card processors, banks, retailers, and other companies, and stole over 160 million credit card numbers.[36]

4. Cyber-enabled crimes threatening personal privacy

Criminals regularly abuse the global reach, connectivity, and anonymity of information technology services to commit a wide range of crimes targeting specific individuals. Many of these behaviors represent reprehensible and often dangerous violations of the victim's privacy rights, and can have lasting, damaging impact. Examples of these crimes include sextortion and non-consensual pornography (sometimes colloquially called "revenge porn"), as well as cyber-enabled harassment and stalking of victims. Criminals are using online tactics—including computer hacking, phishing attacks, and social media manipulation—to gain access to sensitive, often sexually explicit information that they use to extort, harass, or stalk all types of people, including vulnerable youth and young adults.

Sextortion fact patterns vary, but some typical scenarios have emerged. A common fact pattern involves a perpetrator demanding something of value, typically sexually explicit images, from a victim. The perpetrator enforces these demands through threats to distribute material that the victim seeks to keep private, such as embarrassing or sexually explicit images involving the victim, or through threats to harm the victim's friends or family, for example by using stolen account information to bankrupt them. A primary tactic that sextortionists use is to lure the victim to share a compromising image or information, which, once obtained, the criminal can use to blackmail the victim into providing additional images or videos. Often, criminals use social engineering tactics to target victims. A common approach is to misrepresent themselves as peers—for example, using profile photos or avatars on social media websites bearing images close in age to the victim—to convince victims they are communicating with an age-appropriate individual who is actually interested in them. By fraudulently building a rapport using flattery, romance, and manipulation, criminals are able to befriend victims and entice them to share sensitive images or information. Other criminals have presented themselves as representatives from a modeling agency that is interested in representing the victim; still others have successfully impersonated the victim's partner in order to trick the victim. In addition,

criminals also obtain material from victims' online social media accounts, such as personal information and "friends lists," which the criminals exploit to present themselves as acquaintances or someone with similar interests. Finally, some criminals simply hack into a victim's computer and install malware that controls the device's cameras, thereby surreptitiously capturing compromising or personal video footage of the victim. As major consumers of social media, children and young adults are particularly vulnerable to these types of offenses.

Non-consensual pornography describes the distribution of nude or sexually explicit images and videos of an individual without the victim's consent. Images taken consensually during an intimate relationship are released once the relationship ends. Other times, perpetrators obtain consensually produced images by hacking into systems, or obtain non-consensually produced imagery through hidden cameras or by recording sexual assaults. The images may be posted online, often with identifying information and links to social media profiles, or may be sent directly to the victim's co-workers, friends, and family.[37] Non-consensual pornography sometimes overlaps with sextortion, particularly when the perpetrator threatens to distribute sexually explicit images of the victim unless the victim provides additional images or some other thing of value.

Cyber-enabled stalking and **harassment** are other particularly pernicious cyber threats against individuals. These terms cover similar criminal activity that threatens victims, though only cyberstalking is explicitly defined in federal criminal law.[38] Cyberstalking includes any course of conduct or series of acts taken by the perpetrator that places the victim in reasonable fear of death or serious bodily injury, or causes, attempts to cause, or would reasonably be expected to cause substantial emotional distress to the victim or the victim's immediate family. Prohibited acts include repeated, unwanted, intrusive, and frightening communications from the perpetrator by phone, e-mail, or other forms of communication; harassment and threats communicated through the Internet, such as social media sites; and the posting of information or spreading rumors about the victim on the Internet. Cyber-enabled harassment, by contrast, involves more generalized threats to victims, and includes swatting and doxxing. **Swatting** involves deceiving emergency responders to dispatch a SWAT team or other police unit to the victim's home or location, purportedly because the victim has taken hostages or is otherwise armed and dangerous, which tragically has resulted in deadly outcomes. **Doxxing** involves broadcasting personal information about the victim on the Internet, exposing him or her to further harassment by others.

The Department vigorously pursues these acts when they rise to the level of federal crimes. As just one example, we prosecuted a Department of State employee at the U.S. Embassy in London for engaging in a widespread international computer hacking, cyberstalking, and sextortion campaign.[39] This defendant's scheme involved, among other steps, sending e-mails to thousands of potential victims pretending to be from his targets' e-mail provider. The defendant then used these e-mails to trick victims into revealing their account passwords, which

he then used to hack into the accounts and search for sexually explicit photographs. Once the defendant located private photos, he searched for additional personal information about his victims, such as addresses and family member names. Using this information and the stolen explicit images, he then engaged in a cyberstalking campaign, threatening to release the photos if victims did not comply with his demands. This defendant ultimately was sentenced to 57 months in federal prison.[40]

5. Cyber-enabled crimes threatening critical infrastructure

Our Nation's critical infrastructure provides the essential services that underpin American society and serves as the backbone of our economy, security, and health systems.[41] Critical infrastructure includes the financial services sector, the electrical grid, dams, electoral systems, and over a dozen other sectors of society whose assets, systems, and networks are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on our national security, national economic security, national public health or safety, or any combination thereof.[42] These sectors are highly reliant on IT systems and networks. As such, threats targeting critical infrastructure deserve particular attention. For example, major energy systems, such as pipelines and refineries, operate using networked industrial control systems that permit remote operation of massive, geographically dispersed facilities and machines. These systems rely on sophisticated computer and communication networks that adversaries target by seeking to identify vulnerabilities that can be used in the future to disrupt operations or to steal valuable proprietary information. In addition, perpetrators of ransomware schemes, as described above, have sought to exploit society's need for critical infrastructure to remain continuously operational by targeting (and extorting) hospitals, and other vital institutions, that cannot afford any downtime.

Increased connectivity has helped U.S. companies manage and monitor their businesses, but it also has made critical infrastructure vulnerable to cyberattack. Modernization has been a double-edged sword: while it has unlocked new potential for efficiency and performance, the resulting increased connectivity between devices and systems, and especially vital systems like the electrical grid and water treatment facilities, have also created new vulnerabilities and attack vectors that must be defended.[43] As a result, the industrial-control systems that manage and monitor many of our most important industrial facilities and systems are increasingly being targeted by adversaries intent on wreaking havoc.[44] This is not a hypothetical threat: one of the Iranian hackers indicted for the DDoS attacks against the U.S. financial sector is also alleged repeatedly to have gained access to the Supervisory Control and Data Acquisition ("SCADA") system of a dam in New York, allowing him to obtain information regarding the dam's status and operation. Had the system not been under maintenance at the time, the hacker would have been able to control the dam's sluice gate.[45]

Because private entities own and operate the vast majority of the Nation's critical infrastructure, the FBI works to make threat

information available to affected sectors through briefings and widely distributed technical alerts developed jointly with DHS. In March 2018, for example, the FBI and DHS announced that for at least two years, Russian government cyber actors had "targeted government entities and multiple U.S. critical infrastructure sectors, including the energy, nuclear, commercial facilities, water, aviation, and critical manufacturing sectors."[46] This technical alert described a multistage Russian intrusion campaign that compromised small commercial facilities' networks and used them to stage malware and to conduct spear-phishing attacks, which allowed the Russians to gain remote access into energy sector networks. The Russian cyber actors then conducted network reconnaissance, before moving laterally across the network and collecting information pertaining to Industrial Control Systems. U.S. Treasury Secretary Steven Mnuchin referenced this activity when announcing that OFAC had sanctioned five Russian entities and nineteen Russian individuals.[47]

Likewise, in May 2018, the FBI and DHS issued a technical alert notifying the public about the FBI's high confidence that malicious North Korean government cyber actors have been using malware since at least 2009 "to target multiple victims globally and in the United States," across various sectors—including critical infrastructure sectors.[48]

* * *

This non-exhaustive list highlights the varied nature of the most serious cyber threats our Nation faces. To the extent the Department's most important responsibility is to keep Americans safe, it must continue combating these threats and aggressively monitoring how they evolve. One of the most important ways we can stay abreast (if not ahead) of cybercriminals is to fully understand the techniques they use to cause harm. The threats themselves will likely change, but the methods and tools these criminals use to commit computer intrusions and to steal from others have shown remarkable resilience.

Techniques Used to Facilitate Cyber Attacks

The availability of sophisticated technology allows criminals to commit crimes from distant locations, and to avoid detection by victims and law enforcement. Indeed, these technologies greatly expand our adversaries' reach and impact, permitting a small number of criminals to execute intrusions, schemes, and attacks that affect millions of victims. Four of the most common tools that criminals exploit to increase the scale of their attacks include social engineering, malicious software, botnets, and criminal infrastructure.

1. Social Engineering

Social engineering is a tactic criminals use to convince or trick targets into engaging in a specific activity, often by adopting a false identity online of someone the target knows or otherwise believes to be innocuous. Unfortunately, because it preys upon widespread trust that online identities are legitimate, social engineering is surprisingly effective and

is a technique used in the vast majority of data breaches and online scams that the FBI investigates.[49]

In a **phishing** scam, for example, criminals impersonate a person or entity trusted by the victim in order to pressure the victim to engage in conduct that benefits the criminal. These schemes may involve sending fraudulent e-mails that appear to come from a legitimate source, such as a victim's bank or Internet Service Provider ("ISP"), requesting the recipient to click on a link to a website controlled by the criminals and to divulge personal account information, or seeking to get the victim to download malware under false pretenses.[50] Other fraudsters use intimidation and threats to entice the victim to act, such as by threatening to close an account, and often ask for usernames, passwords, dates of birth, Social Security numbers, bank numbers, PIN numbers, payment card numbers, or a mother's maiden name. The goal is to acquire PII that the fraudsters can then sell or use to commit other crimes, such as making fraudulent purchases, or to gain access to the victim's computer to steal information or install malware.

Business e-mail compromise ("BEC") scams are another variant of social engineering, where the goal is not to have the victim provide information, but rather to transfer money. Sometimes operating as part of sophisticated transnational criminal organizations, BEC scammers can send e-mails to employees with access to a company's financial system, tricking them into wiring payments to accounts controlled by the criminals. The e-mails often are designed to look as if they came directly from a senior executive, such as the company's Chief Executive Officer. In some cases, the scammers pick an address that does not belong to the executive but appears to be a real address for the executive, such as being off by one letter. In more sophisticated schemes, BEC fraudsters gain access to the victim company's e-mail system and send requests from the senior executive's actual e-mail account. In 2016, these schemes caused over $360 million of losses reported to the FBI—the largest of any category of cybercrime tracked by IC3.[52] In 2017, IC3 received over 15,000 BEC complaints with adjusted losses of over $675 million, which once again placed these schemes at the top of the loss list.[52]

2. Malware

Malware is malicious software that disrupts, damages, or otherwise compromises the integrity of computer systems and networks. It is frequently disseminated by fraudulently or otherwise unlawfully obtaining access to a victim's computer or system and then launching a malicious payload on the victim's system. Malware takes many different forms. Some versions are written to erase data or even render computers unusable, for example by overwriting critical information on their hard drives, thereby preventing the computers from starting. Other types of malware, such as ransomware programs (discussed above), render the data inaccessible by encrypting victims' systems and demanding a ransom with the promise of restoring the victims' data upon payment—a promise that is not always fulfilled. Spyware, including keyloggers, secretly record users' activities on computers, especially the entering of passwords, and transmit sensitive informa-

tion back to criminals for further exploitation. Any of these actions may be performed by Trojans, which are programs disguised as legitimate software that, once uploaded onto victims' systems, launch hidden malicious software that operates in the background without the victims' knowledge.

3. Botnets

Botnets are vast networks of malware-infected computers and devices that criminals remotely control to conduct a wide range of cybercrime, including sending malware and spam against targets, launching DDoS attacks, and providing infrastructure for ransomware schemes. Botnets—a shortening of "ro***bot net***works"—operate as force multipliers for criminals, giving them control of hundreds, thousands, or even millions of computers to advance their schemes. Because of the relatively low cost of attempting to infect computers with malware, even a comparatively low infection rate can populate a botnet with a vast haul of compromised computers. Further, botnets help criminals cover their tracks from law enforcement by creating an intermediary layer of remotely controlled compromised systems between the criminals and investigators, making it even more challenging for law enforcement to determine who controls the botnet. Moreover, criminals running botnets often are located abroad, which further protects them due to the numerous challenges the Department faces in investigating foreign threats: limited access to digital evidence; delays caused by reliance on mutual legal assistance processes; and the possibility of safe haven from arrest or prosecution in their country of residence. The threat from botnets has increased as individual hackers and organized criminal groups have used ever more sophisticated techniques to infect computers, encrypt communications, and avoid detection by investigators. Finally, as **Fig. 3** illustrates, the recent staggering growth in Internet-connected consumer devices—the so-called "Internet of Things"—has allowed malicious actors to build botnets from under-protected IoT devices to launch DDoS attacks.[53]

4. Criminal Infrastructure

Operating a criminal enterprise with some form of online presence requires a backend technical infrastructure that can be hidden from law enforcement. While some criminals may rely on their own computers and servers, more sophisticated operations lease services from "**bulletproof hosters**," that is, web hosting companies and data centers that purposefully are extremely lenient in what content they will host, make little to no effort to verify the true identity of their customers, and are designed to be unhelpful to law enforcement requests for information about their customers. Bulletproof hosters often are located in countries with less stringent cyber regulations and under-developed domestic cybercrime law enforcement capabilities, and are akin to digital safehouses where criminals can stash malware exploit kits, run botnets, and store PII stolen from hacked databases.

In addition to bulletproof hosters, cybercriminals regularly use the Dark Web, the collection of hidden sites and services that are only accessible to users of specific routing and anonymizing services and software. In recent years, criminals have launched so-

October 16, 2016 – ***Hajime*** – Targets devices with default credentials; Uses obfuscation techniques to hide infection on devices; Communicates with C2 server through a Peer to Peer (P2P) Network

April 5, 2017 – ***Brickerbot*** – Targets devices with default credentials; After infection conducts a Permanent Denial of Service attack on device designed to corrupt storage, disrupt connectivity, and delete files, rendering devices useless

July 2016 – ***Mirai*** – Most significant IoT botnet responsible for largest DDoS attacks ever recorded; Hundreds of spinoff variants due to public source code availablity; Targets devices with default user credentials

November 16, 2016 – ***RSOCKS*** – Targets IoT devices via SSH brute force attacks; Uses compromised devices as proxies criminals can purchase for anonymization and other criminal activity

JUL | AUG | SEP | OCT | NOV | DEC | JAN | FEB | MAR | APR

2016

Figure 3: Significant Internet of Things (IoT) Botnets

July 2017 – ***Masuta*** – DDoS botnet; Based off of Mirai; Targets default user credentials; Source code available in a Dark Market forum

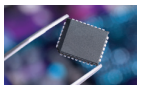
August 2017 – ***RouteX*** – Targets a known vulnerability in Netgear routers; Turns infected devices into proxies for credential validation attacks targeting financial institution and brokerage customer accounts

September 13, 2017 – ***Reaper*** – First major IoT botnet to significantly vary from Mirai; Targets devices with 32 vulnerabilities, capable of more complex attacks, and scans devices less aggressively to avoid detection

November 23, 2017 – ***Satori*** – DDoS botnet; Targets a zero-day vulnerability in Huawei Home Gateway routers and customer-premises equipment; Programmed with 65,000 default credentials combinations

November 2017 – ***Nexus_Mirai*** – A variant of Masuta/Satori; Based on Mirai source code; Targets devices with default credentials; Named after author whose moniker is 'Nexus'

January 14, 2018 – ***Okiru*** – DDoS botnet; Based off of Masuta; Targets IoT devices with ARC Processors, used in more than a billion products each year



January 23, 2018 – ***Pure Masuta*** – DDoS botnet; Created by the same author as Satori/Masuta; Targets a flaw in D-Link routers and exploits a bug in the Home Network Administration Protocol

January 24, 2018 – ***Hide'N Seek*** – Primarily targets IP Cameras with open telnet ports; Uses P2P to spread to other devices

February 1, 2018 – ***Jen X*** – Connected to a gaming server rental business; DDoS capabilities available for $20; Targets a vulnerability in Huawei routers and a vulnerability in the firmware component of a wireless chipset

MAY | JUN | JUL | AUG | SEP | OCT | NOV | DEC | JAN | FEB

2017 2018

Credit: FBI Cyber Division

called dark markets, that is, websites hosted on the Dark Web in which vendors and buyers congregate to buy, sell, and trade illicit goods such as narcotics, credit card numbers, hacking tools, and stolen PII in an environment that protects the vendors' and buyer's anonymity. In the midst of an ongoing opioid crisis, the open availability of dark markets where fentanyl and other illicit narcotics are available for purchase and are delivered direct to consumers in the United States poses a significant public health threat.

Another persistent problem on the Dark Web are online child exploitation communities where like-minded sex offenders gather to promote the sexual abuse of children, provide an environment where such conduct seems "normal," educate each other about how to perpetrate child sex abuse without getting caught, incentivize the production of images that document child sex abuse, and share images and videos depicting the sexual abuse and exploitation of children as young as infants and toddlers. Such communities are disturbingly commonplace, and frequently involve tens of thousands of members.

The growth and continued operation of these sites and communities is made possible by anonymizing technology that effectively hides the servers hosting the sites, as well as users, from normal law enforcement techniques. The best-known technology of this type is free software called The Onion Router ("Tor"). Tor transmits internet traffic through a global volunteer network of thousands of relays (i.e., proxy computers), using layers of encryption to obscure users' identities and geographical locations. Tor not only

THE ONION ROUTER (TOR)

Tor operates by routing encrypted communications through a series of relay computers. This obscures the route of the communications, thereby frustrating monitoring by third-parties, such as law enforcement. Communications sent from a computer using Tor are bounced through a series of intermediary servers, known as relays or nodes, chosen from among thousands of servers located throughout the world that individuals have volunteered to be part of the Tor network. Communications sent through these nodes—known as the Guard, Relay, and Exit nodes—are encrypted in a manner that conceals both the contents of the communication and the IP address of the computer that sent the communication. Each node knows only which other node gave it data, and which node is receiving data. None of the intermediate Tor nodes ever has access to both the sender's true IP address and the actual content of the communication.

anonymizes criminals' Internet traffic, but also allows them to host websites, called Hidden Services, on servers whose location is similarly masked using Tor. Criminals have exploited Hidden Services to facilitate numerous forms of illicit commercial and other criminal activity. Some of the most infamous Hidden Services are dark markets, including the now-shuttered Silk Road and AlphaBay, as well as notorious child exploitation communities. The Department's successes in shutting down these illicit marketplaces are described in further detail in Chapter 3.

Criminals' exploitation of increasingly sophisticated technologies to cover their tracks and avoid being caught represents a significant challenge to law enforcement. Criminals executing ransomware schemes often use anonymizing networks such as Tor to communicate with victims, even going so far as to set up Tor Hidden Services websites to answer victims' questions and to facilitate payment. In addition, the use of anonymizing proxy networks interferes with law enforcement's ability to trace these communications and identify the actors running the ransomware. Criminals also increasingly require payments to be made using virtual currencies or other mechanisms that complicate law enforcement efforts to track those payments. We discuss the impact of such anonymizing technologies on our investigations in Chapter 3. For now, suffice it to say that no discussion of the cyber threats our Nation confronts would be complete without the simple observation that as the Department continues to wage battle against cybercriminals, it will need to adequately meet the challenges posed by anonymizing technologies.

NOTES

[1] From the guilty plea materials in *United States v. Paras Jha,* No. 17-CRM-164 (D. Alaska, Dec. 5, 2017), available at: https://www.justice.gov/opa/press-release/file/1017546/download (last accessed June 29, 2018).

[2] *See* "Alert (TA16-288A): Heightened DDoS Threat Posed by Mirai and Other Botnets," United States Computer Emergency Readiness Team, U.S. Dept. of Homeland Security (last revised Oct. 17, 2017), available at: https://www.us-cert.gov/ncas/alerts/TA16-288A (last accessed June 29, 2018).

[3] *Jha* guilty plea, *supra* note 1.

[4] *See* Indictment in *United States v. Ahmad Fathi,* et al., No. 16-CRM-48 (S.D.N.Y., March 24, 2016), available at: https://www.justice.gov/opa/file/834996/download (last accessed June 29, 2018).

[5] *See* Press Release, "Treasury Targets Supporters of Iran's Islamic Revolutionary Guard Corps and Networks Responsible for Cyber-Attacks Against the United States," U.S. Dept. of Treasury (Sept. 14, 2017), available at: https://www.treasury.gov/press-center/press-releases/Pages/sm0158.aspx (last accessed June 29, 2018).

[6] *See* Sujit Raman, "Petya or NotPetya? It All Just Makes You WannaCry!" RSA Conference 2018 (April 16, 2018) at 3, available at: https://published-prd.lanyonevents.com/published/rsaus18/sessionsFiles/8546/SEM-M03-Ransomware-and-Destructive-Attacks-Raman.pdf (last accessed June 29, 2018).

[7] "Press Briefing on the Attribution of the WannaCry Malware Attack to North Korea," The White House (Dec. 19, 2017), available at: https://www.whitehouse.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917/ (last accessed June 29, 2018).

[8] Andrew E. Kramer, "Ukraine Cyberattack Was Meant to Paralyze, not Profit, Evidence Shows," N. Y. Times (June 28, 2017), available at: https://www.nytimes.com/2017/06/28/world/europe/ukraine-ransomware-cyberbomb-accountants-russia.html (last accessed June 29, 2018).

[9] *See* the grugq, "Pnyetya: Yet Another Ransomware Outbreak," The Medium (June 27, 2017), available at: https://medium.com/@thegrugq/pnyetya-yet-another-ransomware-outbreak-59afd1ee89d4 (last accessed June 29, 2018) (contemporaneous reporting noting that "the worm . . . has an extremely poor payment pipeline," observing that "the pseudo-ransomware is in fact a wiper, with no potential for successfully recovering from an attack," and concluding: "[T]he real Petya was a criminal enterprise for making money. This is definitely not designed to make money. This is designed to spread fast and cause damage, with a plausibly deniable cover of 'ransomware.'").

[10] "Statement from the Press Secretary," The White House (Feb. 15, 2018), available at: https://www.whitehouse.gov/briefings-statements/statement-press-secretary-25/ (last accessed June 29, 2018).

[11] "Press Briefing on the Attribution of the WannaCry Malware Attack to North Korea," The White House (Dec. 19, 2017), available at: https://www.whitehouse.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917/ (last accessed June 29, 2018).

[12] *See* Keith Wagstaff, "Sony Hack Exposed 47,000 Social Security Numbers, Security Firm Says," NBC News (Dec. 5, 2014), available at:

http://www.nbcnews.com/storyline/sony-hack/sony-hack-exposed-47-000-social-security-numbers-security-firm-n262711 (last accessed June 29, 2018).

[13] Press Release, "Treasury Imposes Sanctions Against the Government of The Democratic People's Republic Of Korea," U.S. Dept. of Treasury (Jan. 2, 2015), available at: https://www.treasury.gov/press-center/press-releases/Pages/jl9733.aspx (last accessed June 29, 2018).

[14] Risk Placement Services, Data Breach QuickView Report, First Quarter 2018 2, 9 (2018), available at: https://www.rpsins.com/knowledge-center/items/data-breach-report-q1-2018/ (last accessed June 29, 2018).

[15] Ponemon Institute, 2017 Cost of Data Breach Study: United States, p. 1, available at https://www.ponemon.org/library/2017-cost-of-data-breach-study-united-states (last accessed June 29, 2018).

[16] Federal Bureau of Investigation, 2016 Internet Crime Report 20, 21, available at: https://pdf.ic3.gov/2016_IC3Report.pdf (last accessed June 29, 2018).

[17] "What Happened," Office of Personnel Management Cybersecurity Resource Center (2015), available at: https://www.opm.gov/cybersecurity/cybersecurity-incidents/ (last accessed June 29, 2018).

[18] "U.S. Charges Russian FSB Officers and Their Criminal Conspirators for Hacking Yahoo and Millions of Email Accounts," U.S. Dept. of Justice (March 15, 2017), available at: https://www.justice.gov/opa/pr/us-charges-russian-fsb-officers-and-their-criminal-conspirators-hacking-yahoo-and-millions (last accessed June 29, 2018).

[19] "Canadian Hacker Who Conspired With and Aided Russian FSB Officers Pleads Guilty," U.S. Dept. of Justice (November 28, 2017), available at: https://www.justice.gov/opa/pr/canadian-hacker-who-conspired-and-aided-russian-fsb-officers-pleads-guilty (last accessed June 29, 2018).

[20] Executive Order 13757, "Taking Additional Steps to Address the National Emergency with respect to Significant Malicious Cyber-Enabled Activities," available at: https://www.treasury.gov/resource-center/sanctions/Programs/Documents/cyber2_eo.pdf (last accessed June 29, 2018). This order was later modified to permit U.S. persons shipping technology goods to Russia to obtain licenses from the FSB, as required by the Russian government. "General License No. 1, Authorizing Certain Transactions with the FSS," available at: https://www.treasury.gov/resource-center/sanctions/Programs/Documents/cyber_gl1.pdf (last accessed June 29, 2018).

[21] Press Release, "ISIL-Linked Kosovo Hacker Sentenced to 20 Years in Prison," U.S. Dept. of Justice (Sept. 23, 2016), available at: https://www.justice.gov/opa/pr/isil-linked-kosovo-hacker-sentenced-20-years-prison (last accessed June 29, 2018).

[22] Commission on the Theft of American Intellectual Property, *Update to the IP Commission Report*, at 1 (2017), available at: http://www.ipcommission.org/report/IP_Commission_Report_Update_2017.pdf (last accessed June 29, 2018).

[23] National Counterintelligence and Security Center, *Evolving Cyber Tactics in Stealing U.S. Economic Secrets: Report to Congress on Foreign Economic Collection and Industrial Espionage in Cyberspace*, at 1 (Nov. 2016).

[24] Center *for* Responsible Enterprise And Trade & PricewaterhouseCoopers LLP, Economic Impact of Trade Secret Theft 3 (2014), available at: https://create.org/wp-content/uploads/2014/07/

CREATe.org-PwC-Trade-Secret-Theft-FINAL-Feb-2014_01.pdf (last accessed June 29, 2018).

[25] Press Release, "Member Of Megaupload Conspiracy Pleads Guilty to Copyright Infringement Charges and is Sentenced to One Year in U.S. Prison," U.S. Dept. of Justice (Feb. 13, 2015), available at: https://www.justice.gov/opa/pr/member-megaupload-conspiracy-pleads-guilty-copyright-infringement-charges-and-sentenced-one (last accessed June 29, 2018).

[26] Press Release, "U.S. Authorities Charge Owner of Most-Visited Illegal File-Sharing Website with Copyright Infringement," U.S. Dept. of Justice (July 20, 2016), available at: https://www.justice.gov/opa/pr/us-authorities-charge-owner-most-visited-illegal-file-sharing-website-copyright-infringement (last accessed June 29, 2018).

[27] *See* Press Release, "Chinese Company Sinovel Wind Group Convicted of Theft of Trade Secrets," U.S. Dept. of Justice (Jan. 24, 2018), available at: https://www.justice.gov/opa/pr/chinese-company-sinovel-wind-group-convicted-theft-trade-secrets (last accessed June 29, 2018).

[28] *See* Press Release, "FACT SHEET: President Xi Jinping's State Visit to the United States," The White House (Sept. 25, 2015), available at: https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states (last accessed June 29, 2018).

[29] *See* Press Release, "FACT SHEET: The 2015 G-20 Summit in Antalya, Turkey," The White House (Nov. 16, 2015), available at: https://obamawhitehouse.archives.gov/the-press-office/2015/11/16/fact-sheet-2015-g-20-summit-antalya-turkey (last accessed June 29, 2018).

[30] "Findings of the Investigation into China's Acts, Policies, and Practices related to Technology Transfer, Intellectual Property, and Innovation under Section 301 of the Trade Act of 1974," Office of the United States Trade Representative (March 22, 2018), at 169, available at: https://ustr.gov/sites/default/files/Section%20301%20FINAL.PDF (last accessed June 29, 2018) (citing reports).

[31] Press Release, "U.S. Charges Three Chinese Hackers Who Work at Internet Security Firm for Hacking Three Corporations for Commercial Advantage," U.S. Dept. of Justice (Nov. 27, 2017), available at: https://www.justice.gov/opa/pr/us-charges-three-chinese-hackers-who-work-internet-security-firm-hacking-three-corporations (last accessed June 29, 2018).

[32] Elias Groll, "Feds Quietly Reveal Chinese State-Backed Hacking Operation," Foreign Policy (Nov. 30, 2017), available at: http://foreignpolicy.com/2017/11/30/feds-quietly-reveal-chinese-state-backed-hacking-operation/ (last accessed June 29, 2018) (quoting Department spokesperson).

[33] Federal Bureau of Investigation, "Nigerian Letter or '419' Fraud," available at: https://www.fbi.gov/scams-and-safety/common-fraud-schemes/nigerian-letter-or-419-fraud (last accessed June 29, 2018).

[34] Federal Bureau of Investigation, "Business Fraud," available at https://www.fbi.gov/scams-and-safety/common-fraud-schemes/business-fraud (last accessed June 29, 2018).

[35] Federal Bureau of Investigation, "Investment Fraud," available at https://www.fbi.gov/scams-and-safety/common-fraud-schemes/investment-fraud (last accessed June 29, 2018).

[36] Press Release, "Two Russian Nationals Sentenced to Prison for Massive Data Breach Conspiracy," U.S. Dept. of Justice (Feb. 15, 2018),

available at: https://www.justice.gov/opa/pr/two-russian-nationals-sentenced-prison-massive-data-breach-conspiracy (last accessed June 29, 2018).

[37] *See* Joey L. Blanch & Wesley L. Hsu, "An Introduction to Violent Crime on the Internet," United States Attorneys' Bulletin (May 2016), at 2.

[38] *See* 18 U.S.C. § 2261A.

[39] Press Release, "Former U.S. State Department Employee Sentenced to 57 Months in Extensive Computer Hacking, Cyberstalking and "Sextortion" Scheme," U.S. Dept. of Justice (March 21, 2016), available at: https://www.justice.gov/opa/pr/former-us-state-department-employee-sentenced-57-months-extensive-computer-hacking (last accessed June 29, 2018).

[40] This report does not detail related crimes involving the sexual exploitation of children. For more detail on this criminal threat, *see* U.S. Dept. of Justice, The National Strategy for Child Exploitation Prevention and Interdiction (Apr. 2016), available at: https://www.justice.gov/psc/file/842411/download (last accessed June 29, 2018).

[41] "Critical Infrastructure Security," U.S. Dept. of Homeland Security, available at: https://www.dhs.gov/topic/critical-infrastructure-security (last accessed June 29, 2018).

[42] 42 U.S.C. § 5195c(e).

[43] *See* Richard J. Campbell, "Cybersecurity Issues for the Bulk Power System," Cong. Research Serv., 9R43989, at 9 (June 10, 2015), available at: https://www.fas.org/sgp/crs/misc/R43989.pdf ("Over time, modification of SCADA [Supervisory Control and Data Acquisition] systems has resulted in connection of many of these older, legacy systems to the Internet.") (last accessed June 29, 2018).

[44] *See id*.

[45] *See Fathi* indictment, *supra* note 4, at 14-16.

[46] Alert TA18-074A, "Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure," U.S. Computer Emergency Readiness Team, U.S. Dept. of Homeland Security (March 15, 2018), available at: https://www.us-cert.gov/ncas/alerts/TA18-074A (last accessed June 29, 2018).

[47] Press Release, "Treasury Sanctions Russian Cyber Actors for Interference with the 2016 U.S. Elections and Malicious Cyber-Attacks," U.S. Dept. of Treasury (Mar. 15, 2018), available at: https://home.treasury.gov/news/press-releases/sm0312 (last accessed June 29, 2018).

[48] Alert TA18-149A, "HIDDEN COBRA – Joanap Backdoor Trojan and Brambul Server Message Block Worm," U.S. Computer Emergency Readiness Team, U.S. Dept. of Homeland Security (last revised May 31, 2018), available at: https://www.us-cert.gov/ncas/alerts/TA18-149A (last accessed June 29, 2018).

[49] *See generally* Mollie Halpern & Patrick Geahan, "FBI, This Week: Social Engineering," Federal Bureau of Investigation (Oct. 14, 2016) (podcast transcript), available at: https://www.fbi.gov/audio-repository/ftw-podcast-social-engineering-101416.mp3/view (last accessed June 29, 2018).

[50] "Consumer Information: Phishing," Federal Trade Commission (July 2017), available at: https://www.consumer.ftc.gov/articles/0003-phishing (last accessed June 29, 2018).

[51] Federal Bureau of Investigation, 2016 Internet Crime Report 1, 9, available at: https://pdf.ic3.gov/2016_IC3Report.pdf (last accessed June 29, 2018).

[52] Federal Bureau of Investigation, 2017 Internet Crime Report 3, 12, available at: https://pdf.ic3.gov/2017_IC3Report.pdf (last accessed June 29, 2018).

[53] *See* "A Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats," U.S. Dept. of Commerce & U.S. Dept. of Homeland Security (May 22, 2018), available at: https://www.commerce.gov/sites/commerce.gov/files/media/files/2018/eo_13800_botnet_report_-_finalv2.pdf (last accessed June 29, 2018).

[54] Exploit kits are a type of malicious toolkit used to exploit security holes found in software applications for the purpose of spreading malware. These kits come with pre-written exploit code and target users running insecure or outdated software applications on their computers.

[55] Press Release, "Ross Ulbricht, The Creator And Owner Of The "Silk Road" Website, Found Guilty In Manhattan Federal Court On All Counts," U.S. Dept. of Justice (Feb. 5, 2015), available at: https://www.justice.gov/usao-sdny/pr/ross-ulbricht-creator-and-owner-silk-road-website-found-guilty-manhattan-federal-court (last accessed June 29, 2018).

[56] Press Release, "AlphaBay, the Largest Online 'Dark Market,' Shut Down," U.S. Dept. of Justice (July 20, 2017), available at: https://www.justice.gov/opa/pr/alphabay-largest-online-dark-market-shut-down (last accessed June 29, 2018).

[57] *See*, *e.g.*, Press Release, "Colorado and Illinois Men Sentenced to Prison for Engaging in Child Exploitation Enterprise," U.S. Dept. of Justice (Oct. 18, 2016), available at: https://www.justice.gov/opa/pr/colorado-and-illinois-men-sentenced-prison-engaging-child-exploitation-enterprise (last accessed June 29, 2018).

Chapter 3
Detecting, Deterring, and Disrupting Cyber Threats

The Department of Justice plays an essential role in detecting, deterring, and disrupting cyber threats. As the Nation's chief law enforcement officer, the Attorney General leads the Department's criminal and national security initiatives. Working with and through the Criminal Division, the National Security Division, and the 93 U.S. Attorney's Offices across the country, the Attorney General sets priorities for how those activities are conducted.[1]

Since the early 1990s, when the commercial Internet was in its infancy, the Department has combated computer crime. In the intervening years, the Department has expanded its focus to address burgeoning threats to public safety, economic security, and national security flowing from the widespread adoption of the Internet. Today, the Department deters and disrupts a broad spectrum of the Nation's cyber threats by enforcing federal laws through the array of legal tools and capabilities that its investigators and prosecutors have at their disposal.

In this chapter, we describe the key methods investigators and prosecutors use to gather evidence about cyber threats. We then explain the key legal authorities the Department applies to bring perpetrators to justice, or otherwise to disrupt and dismantle malicious cyber activity.

Key Investigative Techniques

To successfully bring malign cyber actors to justice, law enforcement first must gather evidence of their criminal activity and attribute that activity to particular individuals, organizations, or nation states. The key methods and sources of evidence for disrupting cyber threats include: gathering materials during incident response; reviewing open source data; conducting online reconnaissance; searching records from online providers; undertaking undercover investigations; engaging in authorized electronic surveillance; tracing financial transactions; searching storage media; and applying a variety of special techniques. Often, investigators also must work cooperatively with foreign partners to access evidence and disrupt transnational cyber threats.

1. Evidence Collection During Incident Response

Often the first evidence collected in an investigation concerning a cyber threat comes from the victim as part of the incident response. The Department encourages victims to contact law enforcement as soon as they believe they are the victim of a computer intrusion. Although many victims will simply provide consent to investigators collecting

digital evidence on scene, subpoenas and search warrants can be obtained if the victim prefers. In either case, investigators are committed to working collaboratively with victims to minimize any disruption to business during an investigation.

After obtaining digital copies of any affected devices, investigators may then turn to other devices in the victim's architecture, including firewalls, log servers, and routers, to look for additional evidence of the perpetrator's presence. Investigators will also image these devices, as needed, and forensically examine them. Such devices often contain traces of a criminal's passage through the infrastructure on the way to the affected device. In particular, many devices maintain log files that show when, and from where, the device was accessed. In addition to preserving and copying digital evidence, investigators may interview employees (especially those tasked with responding to cyber threats or securing infrastructure), regular users of the affected systems, and management.

2. Online Data Review and Reconnaissance

After reviewing information obtained from a victim or other primary sources of information regarding a cyberattack, investigators frequently will review online data, which may be open source, to determine their next investigative steps. In undertaking these actions, as with all their actions, investigators are trained to act consistently with our Nation's rule of law principles, and with our society's foundational respect for civil rights and civil liberties.[2]

The first step in online reconnaissance often involves use of the Internet Corporation for Assigned Names and Numbers' WHOIS database.[3] WHOIS is a directory of all of the IP addresses and domains on the Internet. WHOIS records usually display the name and contact information of the registrar (the business that sold the IP address or domain). Investigators can use the contact information to send legal process to the registrar in order to discover more information about the registrant (the user of the IP address or domain). WHOIS often contains self-reported information about the registrant, as well. In addition, an investigator often can tell from WHOIS and related information where a website is being hosted or who is hosting the e-mail server for a website, either (or both) of which can provide additional avenues for investigation.

After consulting WHOIS, investigators often perform online reconnaissance of the identifiers they have collected. This reconnaissance includes web searches looking for whether the identifiers have been used elsewhere and searches of social media to determine whether the identifiers are related to any accounts.

3. Searching Records from Online Providers

Successful WHOIS searches and online reconnaissance often results in the identification of e-mail providers, social media companies, registrars, and web hosting and computer hosting companies that may control additional evidence about a subject or

target of an investigation. At this stage, an investigator will rely heavily on the provisions of the Electronic Communications Privacy Act ("ECPA"),[4] which specifically permits investigators to request evidence from providers of electronic communications and computer processing. Investigative teams may issue subpoenas to collect basic information about a subscriber to an identified account. Investigators also may use court orders issued under the authority of section 2703(d) of title 18, United States Code, which allows them to access additional non-content records for online accounts, such as log files or the e-mail addresses of others with whom the subscriber has corresponded.

Finally, with probable cause, investigators can seek a search warrant from a judge to obtain the contents of accounts, including copies of e-mails, photographs, text messages, and any other files stored with a provider up to and including the contents of an entire computer belonging to a target of the investigation and hosted with the provider.[5] Because cyber threat actors often communicate with each other using electronic communications to plan and execute their activities, these accounts can contain vast quantities of useful evidence. In addition, cyber threat actors sometimes keep other evidence in the contents of their accounts, such as records of their criminal activities, pictures that place them at the scene or with other members of the conspiracy, and other evidence that can help identify the actors and connect them to the illicit activity.

4. Online Undercover Operations

In order to investigate cyber threat activity, investigators may establish covert personas or consensually assume the accounts and identities of victims or cooperators to communicate online with the targets of the investigation. From such undercover operations, investigators gather inculpatory contents from communications, additional accounts, IP addresses, criminal proceeds, and records of criminal transactions such as the purchase of malware, botnets, or stolen credit cards.

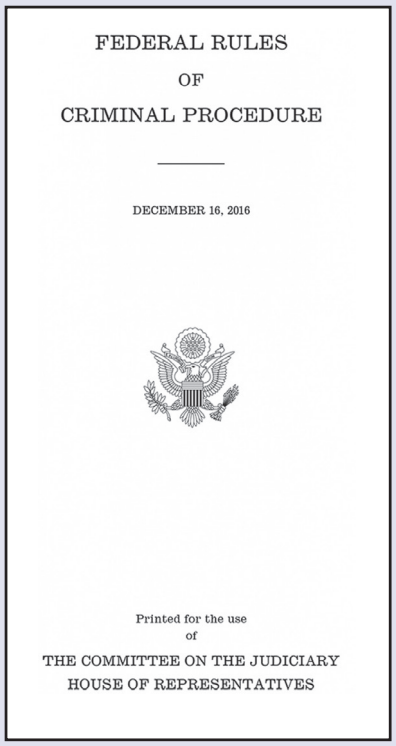
5. Electronic Surveillance

Investigators may also need to conduct online surveillance on their targets. There are three federal statutes that authorize the collection of data on a real-time basis: the pen register and trap and trace ("PRTT") statute,[6] the wiretap statute,[7] and the Foreign Intelligence Surveillance Act ("FISA").[8] All three generally require investigators to obtain court authorization.

A PRTT allows investigators to obtain the dialing, routing, addressing, and signaling information of communications, including dialed calls, IP addresses, and e-mail headers. PRTTs can be obtained for cell phones, e-mail accounts, and other social media or messaging applications. Although a PRTT does not obtain the content of any communications, it can be useful in determining whether an account is still being used for criminal purposes, to help identify co-conspirators, or to locate a target.

(NEW) RULE 41(b)(6)

Under Rule 41(b)(6) of the Federal Rules of Criminal Procedure, which went into effect in December 2016, "a magistrate judge with authority in any district where activities related to a crime may have occurred has authority to issue a warrant to use remote access to search electronic media and to seize or copy electronically stored information located within or outside that district if: (A) the district where the media or information is located has been concealed through technological means; or (B) in an investigation of a violation of 18 U.S.C. § 1030(a)(5), the media are protected computers that have been damaged without authorization and are located in five or more districts."


FEDERAL RULES
OF
CRIMINAL PROCEDURE

DECEMBER 16, 2016

Printed for the use
of
THE COMMITTEE ON THE JUDICIARY
HOUSE OF REPRESENTATIVES

This provision makes two narrow, but important, changes in the law. First, where a suspect has hidden the location of his or her computer using technological means, the new Rule ensures that federal agents know which judge to go to in order to apply for a warrant. Second, where the crime involves the hacking of computers located in five or more different judicial districts, the new Rule ensures that federal agents may identify one judge to review an application for a search warrant rather than having to submit separate warrant applications in each judicial district across the nation—up to 94—where a computer is affected. In sum, Rule 41(b)(6) addresses the unique challenges created by botnet activity by clarifying that courts may issue warrants authorizing the search of multiple computers when the identified computers are located in multiple judicial districts.

Court-authorized wiretaps under the Wiretap Act or FISA permit investigators to listen to or observe the contents of communications in or near real time. For example, investigators can intercept wire and electronic communications over a target's cell phone or read the target's e-mail as it is sent, allowing them to locate targets, confirm relationships within a conspiracy, disrupt new criminal activity, and confirm previous activity. Every federal wiretap application must be approved by a senior Department official before it is submitted to a court. Federal courts, in turn, apply rigorous standards both in authorizing and supervising wiretaps.

6. Special Techniques

Cyber threat actors often try to hide their identities by disguising their IP address. A common way to do this is by using a proxy computer, which sits between the actor and his victim, to obfuscate the actor's IP address. As described in Chapter 2, threat actors also will often use The Onion Router ("Tor"), which is a particularly sophisticated network of relay computers, to hide their true IP address. To circumvent the challenges presented by threat actors' use of proxies and Tor, investigators can use **Network Investigative Techniques ("NITs")**. NITs include computer code that investigators can send covertly to a device that is hidden behind proxies. Once installed, a NIT can send law enforcement particular information, often including the device's true IP address—which investigators then can use to identify the subscriber and user of the device.

As described in Chapter 2, botnets pose unique challenges for law enforcement and so require special techniques to investigate and disrupt them. Identifying victim computers (or "bots") can be very difficult because the bots may be spread throughout the world. Criminal dark markets that rent or sell botnet access often obfuscate the location and other identifying information about individual bots. Until recently, this posed a significant jurisdictional hurdle, as an investigator had to know the location of a bot to get a search warrant for it. Now, thanks to a recent Department-led initiative to amend the Federal Rules of Criminal Procedure (see page 52), magistrate judges can authorize search warrants even if the location of the subject of the warrant is unknown. Botnets are controlled by command and control servers ("C2 servers"), which periodically issue orders to the bots. One way to disrupt a botnet is to seize control of the C2 server. Investigators can use criminal authorities to seize C2 servers; they can also use civil injunctive authority to seek the redirection of computers under the control of the botnet to a server controlled by the court, instead of by the threat actor's C2 server.

7. Tracing Financial Transactions

Pursuing illicit assets is an important part of any fraud investigation, and computer crime cases are no exception. To pursue traditional bank accounts, the United States has made extensive use of asset forfeiture authorities, including seizures involving correspondent bank accounts, as well as of sanctions programs, including the Global Magnitsky sanctions authority, to keep tainted funds out of the U.S. financial system. Yet, cybercriminals increasingly use **virtual currencies** to advance their activities and to conceal their assets. Because most virtual currencies lack any central authority, seizing them requires different approaches.

In recent years, the Department has relied on a variety of legal authorities to seize virtual currency that has been derived from illegal activity. These authorities include civil forfeiture orders, seizure warrants, and search warrants. Where, for instance, a target of an investigation stores virtual currency with a third-party service—typically, a virtual currency exchanger—investigators may seize that virtual currency by obtaining a seizure warrant for the user's account at that

VIRTUAL CURRENCIES

"Virtual currencies" such as Bitcoin, Ether, and Monero are electronic assets that are circulated over the Internet as a form of value but are not backed by any government. Though virtual currencies have legitimate uses, they also often enable individuals to transfer money with high levels of anonymity to other users worldwide. Cyber criminals frequently transact in virtual currencies, and online criminal markets rely on virtual currencies to enable the purchase and sale of a wide variety of illegal goods and services. While law enforcement has made strides in its ability to trace virtual currency transactions, criminals often launder their virtual currency by mixing one user's money with multiple other users', or sending their virtual currency through a convoluted series of transactions, a process often called "mixing" or "tumbling."

third-party service. If the target stores the virtual currency locally (for example, on his own electronic devices, or on servers he controls), or even by printing the private keys onto a physical medium, investigators may seize the virtual currency through a traditional search warrant that allows the government to learn the private key. The seizure of virtual currency requires transferring the virtual currency to a government-controlled virtual currency wallet. If the virtual currency is stored with an overseas exchange, the Department will work with our foreign counterparts to effect the seizure.

Because of the risks that early conversion may pose, in most cases, virtual currency the government seizes is kept in the form it was seized and not liquidated (*i.e.*, converted to fiat currency or other virtual currency) until a final order of forfeiture is entered or an administrative forfeiture is final.[9] Agencies or prosecutors may, however, seek an order for the interlocutory sale of virtual currency at the request and/or consent of all parties with an ownership interest. Consultation with the Criminal Division's Money Laundering and Asset Recovery Section is required prior to any pre-forfeiture conversion, or seeking an order for interlocutory sale of virtual currency.

Any liquidation of virtual currency should be executed according to established written policies of the seizing agency and the U.S. Marshals Service.[10] The Department is developing guidance regarding disposition of alternative virtual currencies (*i.e.*, anonymity enhanced cryptocurrencies and ICO tokens) for which the Marshals Service does not yet have a process in place to take custody or liquidate via auction.

As detailed above, the Department in recent years has regularly used civil forfeiture au-

thorities[11] and seizure warrants to seize virtual currency derived from malicious cyber activity associated with the Dark Web and botnets. More recently, in July 2017, the Department announced the indictment of a Russian national and an organization he allegedly operated, BTC-e, for facilitating transactions for international cybercriminals, and for receiving the criminal proceeds of numerous computer intrusions and hacking incidents, as well as of other crimes.[12] According to the indictment, BTC-e's virtual currency exchange allegedly did not require users to validate their identity, obscured and anonymized transactions and source of funds, and eschewed any anti-money laundering processes. Perhaps unsurprisingly, the exchange is alleged to have become popular with criminals. At the time of the indictment, the investigation revealed that BTC-e was alleged to have received more than $4 billion worth of virtual currency through its operation.

In parallel with the Department's actions, the Financial Crimes Enforcement Network ("FinCEN") assessed a $110 million civil money penalty against BTC-e for willfully violating U.S. anti-money laundering laws. The operator of the exchange was assessed a $12 million penalty for his role in the violations. FinCEN's announcement underscored the importance of the Department's partnerships with regulatory agencies in seeking to deter those who facilitate ransomware, dark net drug sales, and other illicit activity using virtual currency.

Just as virtual currencies have provided a new way for criminals to launder money, they also provide another avenue for **tax evasion**. In particular, evaders can abuse the anonymous and decentralized structure of virtual currencies in an attempt to conceal their income and assets. The relative lack of reporting requirements for virtual currency also contributes to its secrecy and thus to its usefulness in committing tax crimes. And with the increase in value of virtual currencies in recent years, this anonymity and secrecy may tempt individuals not to report as income their gains from the sale of virtual currency.

This is a particularly novel area for tax enforcement. But investigators pursuing tax investigations involving virtual currency can employ many of the techniques learned from money laundering investigations involving virtual currency. For instance, investigators can track the movement of funds across the public ledger of a virtual currency and identify when money moves into or out of virtual currency through exchanges and other parties. Moreover, the Internal Revenue Service ("IRS") Criminal Investigation division is making criminal tax evasion using virtual currencies a focus of its efforts, and the IRS is also pursuing civil and administrative remedies. Within the Department, the Tax Division is partnering with the IRS and U.S. Attorneys' Offices to investigate and prosecute tax crimes involving virtual currencies, and to litigate civil enforcement actions. Recently, the Tax Division, working with the IRS, issued and enforced the first virtual-currency-related "John Doe" summons to Coinbase, one of the largest virtual currency exchanges in the world.[13] As a result of this civil enforcement action, in March 2018, the exchange turned over to the IRS information

regarding accounts "with at least the equivalent of $20,000 in any one transaction (buy, sell, send, or receive) in any one year during the 2013-2015 period."[14] This information should be useful in identifying particular individuals and transactions for further investigation.

In addition, Tax Division prosecutors are working with investigators and attorneys at IRS, as well as at the Department's Computer Crime and Intellectual Property section, to develop training and guidance for criminal tax cases involving virtual currencies. Because the tax treatment of virtual currencies is a new area, there are many uncertainties in the law that investigators and prosecutors will need to navigate. The Tax Division's trial attorneys also have worked with the FinCEN Intelligence, Cyber & Emerging Technology Section to identify appropriate techniques for civil tax investigations and litigation.

8. Traditional and Forensic Searches Involving Storage Media

Once a criminal is identified and arrested, investigators will seek electronic evidence from his personal storage media, including his laptops and phones. Such storage media often contain records that link the target to the evidence collected from providers or the victim, such as matching IP addresses, e-mail accounts, and photos and other personal identifiers. This evidence completes the connection between the criminal activity and the target. Such a search usually requires a traditional search warrant, based on probable cause. Investigators also will search a target's residence, business, or automobile, looking for storage media that may contain evidence of the cyber threat. As with storage media collected during the initial incident response, investigators will image any electronic storage media before searching it, to preserve the contents for future searches and for use in court.

9. Cooperation with Foreign Governments

Cyber threats often emanate from international locations and use criminal networks that stretch across jurisdictions, many of which are not friendly to the rule of law or democratic values. At the same time, foreign sovereigns—including some of our closest allies—put limits on our government's ability to act on its own in every investigation where the targets, or evidence of their crimes, are located in another jurisdiction. Fortunately, the Department has built relationships with its counterparts around the world, that facilitate nimble information sharing in the event of an incident. This information sharing enables mitigation of the incident, and also promotes the preservation of evidence, even in situations where the evidence (or the perpetrators) are located outside the United States.

For more formal use of the information (e.g., to support charges and hold criminal actors accountable), the Department employs a vast network of international treaties and other relationships. The Criminal Division's Office of International Affairs ("OIA"), for example, leverages extradition treaties, mutual legal assistance treaties ("MLATs"), and other in-

The CLOUD Act

Due in part to the large volume of foreign government requests seeking electronic evidence in the custody or control of U.S.-based service providers, and the pressure those requests were placing on the smooth functioning of the MLAT process, the U.S. Congress, in March 2018, enacted, and the President signed into law, a statute called the Clarifying Lawful Overseas Use of Data (CLOUD) Act.

The CLOUD Act has two major effects. First, it clarifies that all warrants, subpoenas, and court orders issued pursuant to the Stored Communications Act, 18 U.S.C. § 2701 *et seq*—the law that governs the disclsoure of stored communicatons and transactional records held by third-party Internet service providers—apply to all data within a provider's possession, custody, or control, regardless of whether the data is stored inside or outside the United States. Second, it allows for bilateral treaties between the United States and foreign countries for the direct sharing of electronic evidence, without needing to use the MLAT process. The CLOUD Act incorporates safeguards to assure that such agreements are entered into only with countries with robust privacy and civil liberties protections, and that adhere to the rule of law.

The CLOUD Act represents a major commitment by the American government to continue the global fight against crime by ensuring that rights-respecting and privacy-protecting foreign governments gain access to the electronic evidence they need to pursue their own investigations of serious crime, even as the Act reduces pressure on the MLAT process generally, and encourages higher privacy and civil liberties standards around the world.

struments and available legal tools to support U.S. investigations and prosecutions of cybercriminals by returning fugitives to the United States to face trial, and by obtaining the evidence located overseas that is needed to build a case against them. OIA also facilitates the extradition of fugitives located in the United States and transfers evidence to foreign partners for those nations' criminal investigations.

When a criminal located overseas is wanted for prosecution or to serve a criminal sentence in the United States, OIA uses all the legal tools at its disposal—extradition, deportation, and other lawful measures—to ensure that the defendant will be transferred to the United States to stand trial in a U.S. court and be held accountable. The processes that must be followed to effectuate this result vary greatly in each case and depend on a range of factors, including, among others, the location of the criminal actor, his or her nationality, our law enforcement relationship with the host country, and the alleged criminal conduct at issue.

The United States currently has bilateral **extradition** treaties with over 100 countries.[15] These treaties, which establish reciprocal obligations to extradite persons charged with or convicted of certain crimes, contain varying features, including some that give the requested state the discretion to decline to extradite its nationals. Other common treaty provisions can affect the charges an individual may face after extradition. These include the statute of limitations, assurances against the imposition of a capital sentence, and the rule of specialty. Extradition requests that result in defendants facing trial in the United States or serving a U.S. criminal sentence generally require carefully prepared documentary submissions and extensive coordination between OIA, U.S. prosecutors, and law enforcement, including the FBI, U.S. Marshals Service, the State Department, and the foreign government.

The ease and speed with which fugitives can travel across jurisdictions highlight the importance of a treaty-based mechanism known as a provisional arrest. When the United States learns that a fugitive will be traveling to—or through—a country with which it has an extradition treaty, there often is not enough time to assemble and submit a formal request for extradition. Where time is of the essence, OIA can submit a provisional arrest request, which will enable the foreign partner to arrest and detain the fugitive for a short period of time until OIA submits the formal extradition request.

There are also countries with which the United States does not maintain an extradition treaty. In cases where the United States seeks the return of a fugitive from a non-treaty partner, OIA attempts to accomplish this through other legal means, including, where possible, securing extradition under the domestic law of the foreign country, and requests for deportation, expulsion, or other lawful transfer. The range of options available varies from case to case, including using lawful measures to ensure the wanted person's transit to a country from which the United States can secure his extradition.

EXTRADITIONS

Successfully prosecuting international computer crime cases has been notoriously difficult. Fortunately, the Department's international outreach has made it easier. In addition, the Department has relied on longstanding tools and processes, such as extradition treaties and alternatives to extradition, to ensure that some of the most notorious cybercriminals face justice in the United States.

In August 2016, for example, a U.S. federal court jury convicted **Roman Seleznev,** a Russian national, of various crimes associated with his theft and sale on the black market of tens of thousands of credit card numbers, which resulted in over $170 million in fraudulent purchases. A "pioneer" cybercriminal who became "one of the most revered point-of-sale hackers in the criminal underworld," Seleznev is the "highest profile long-term cybercriminal ever convicted by an American jury."[16] Seleznev was arrested in the Maldives in July 2014 and was subsequently expelled to the United States, where he is currently serving a 27-year federal sentence for his hacking crimes, concurrent to a 14-year federal sentence stemming from his involvement in a $50 million cyberfraud ring.[17]

More recently, in February 2018, the alleged creator of the Kelihos botnet (see Appendix 2), a Russian national named **Peter Levashov,** was extradited from Spain, and in March 2018, **Yevgeniy Nikulin,** of Moscow, made his initial appearance in U.S. federal court following his extradition from the Czech Republic to face allegations that he illegally accessed computers belonging to LinkedIn, Dropbox, and Formspring.

As these cases and others like them demonstrate, we have successfully dismantled international criminal rings and apprehended some of the most notorious international cybercriminals. At times, we have received valuable evidence from foreign authorities, including Russian law enforcement. But challenges remain, including an increased willingness by the Russian government to protect its nationals from extradition or other removal to the United States when its nationals are located in a third country. In such circumstances, Russia has applied pressure on the U.S. partner, seeking to thwart the U.S. extradition or other removal request. This practice is yet another factor that complicates our efforts to bring international cybercriminals to justice in the United States.

In sum, cybercriminals should not be immune from justice simply because they operate outside of U.S. borders. Although there are state sovereignty principles that limit our ability to act unilaterally, OIA has a diverse toolkit that it can use to obtain foreign countries' cooperation and ensure that cybercriminals face justice in U.S. courts.

Investigating and prosecuting cyber criminals often also requires access to evidence located in foreign jurisdictions and assistance from foreign governments. This evidence and assistance may include electronic records, bank and business records, witness interviews, public records, investigative materials, and seizure of assets, to name a few examples. Each year, OIA receives thousands of such requests for mutual legal assistance from both domestic and foreign prosecutors seeking important evidence that may break open an investigative dead-end or secure a criminal conviction. Such requests for assistance to foreign governments are typically made pursuant to bilateral MLATs, regional instruments, or multilateral conventions, such as the international Convention on Cybercrime (known as the Budapest Convention). As the Central Authority for the United States under international instruments, OIA makes requests for assistance to treaty partners on behalf of U.S. prosecutors and executes requests it receives from abroad.

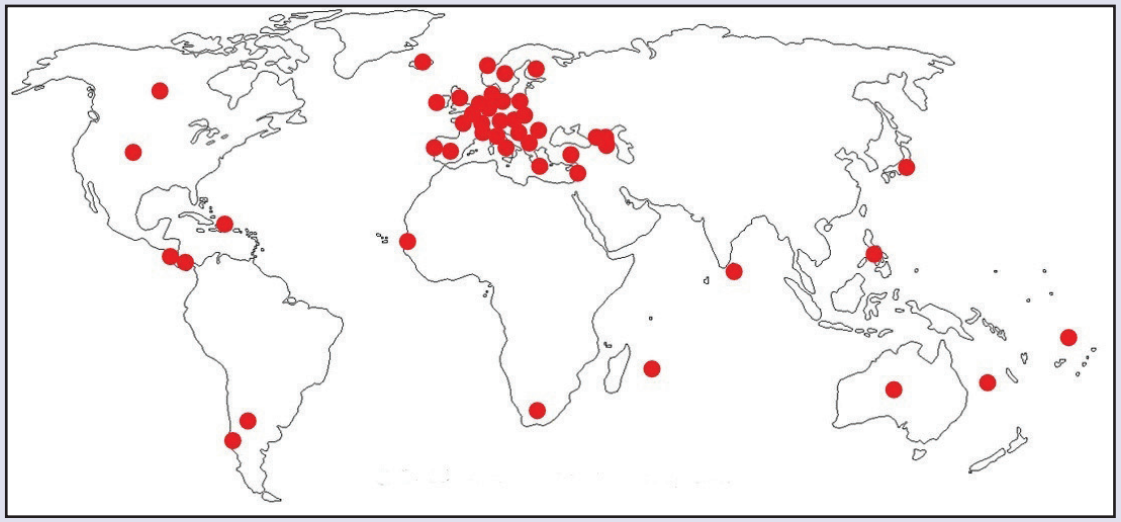
Many of the world's communications service providers are U.S. companies, and electronic records in their custody or control are often critical to cybercrime investigations, as well as other types of criminal and national security cases such as those targeting violent crime, terrorism, child exploitation, and criminal organizations using the Dark Web. As a result, OIA receives a high-volume of requests for electronic records in the custody or control of U.S. providers. OIA executes these requests—many of which concern cases involving foreign actors whose schemes have victimized U.S. citizens—as appropriate and pursuant to its treaty obligations. Doing so both increases the likelihood that foreign governments will be able to disrupt the illegal conduct and ensures their reciprocal cooperation when needed for the United States to obtain assistance from abroad.

Importantly, these cross-border requests for electronic evidence typically must meet the legal requirements of the requested state. In the United States, this means that for requests seeking the contents, say, of an e-mail account, a Department of Justice attorney—usually from OIA but sometimes from a partner U.S. Attorney's Office—must obtain a search warrant from a U.S. court on the foreign government's behalf. Probable cause is a distinctly American concept, and many countries struggle to articulate a sufficient basis in their requests to meet this legal standard. OIA works closely with requesting state partners to develop, where possible, the necessary basis to obtain a search warrant. Other U.S. legal requirements, including the "filtering" of any resulting productions, add to the complexity of this practice.

Because there are few rules governing most providers' retention of data in the normal course, it is important that electronic records associated with targeted accounts be "preserved" before they are deleted. Pursu-

THE BUDAPEST CONVENTION

The Budapest Convention (official name: the Council of Europe's Convention on Cybercrime) is a multilateral treaty that enhances international cooperation in cases involving computer-related crime. The treaty entered into force in 2004, requires Parties to have a basic level of domestic criminal law in the cyber field, and provides a platform for transnational law enforcement cooperation in investigations, evidence sharing, and extradition. The Convention also requires Parties to criminalize computer-related crimes such as computer hacking, fraud, and child sexual exploitation, and requires that Parties have the ability to effectively investigate computer-related crime through the collection and sharing of electronic evidence. Membership in the Convention is open to any nation. To date, nearly 60 countries spanning Europe, Asia, Australia, Africa, and North and South America have fully ratified the treaty, as illustrated below. The United States participated in the drafting of the Convention and became a Party to it in 2006.



ant to U.S. law, U.S. investigators and prosecutors preserve targeted account data prior to obtaining a search warrant or other legal process for its disclosure. OIA and the Department's Computer Crime and Intellectual Property section routinely assist prosecutors and law enforcement around the world in performing this early, but important, investigative step.

10. Joint or Parallel Investigations

Law enforcement agencies from separate countries may wish to cooperatively investigate crimes having relevance and jurisdiction in both countries through joint or parallel investigations. Although these investigations may be established in the absence of a treaty, a number of existing treaties address the

creation of joint investigative teams ("JITs"), thereby highlighting the potentially useful impact of such arrangements. These include, for example, global multilateral instruments like the 2000 United Nations Convention against Transnational Organized Crime,[18] and, in the case of the United States and the European Union, the 2003 Agreement on Mutual Legal Assistance between the United States of America and the European Union.[19] JITs can be useful tools to conduct joint operations, facilitate information sharing, and thwart criminal conduct. However, they are not perfect solutions for all cases with multi-jurisdictional dimensions. U.S. criminal law and practice differ in significant respects from that of foreign partners, and as a result, the prudent course is to assess opportunities for JITs on a case-by-case basis and to fashion cooperative efforts in a manner that works for all relevant participants.

Key Prosecution Tools

Once investigators have gathered evidence of cyber threat activity, the Department's prosecuting attorneys then determine whether that evidence is sufficient to bring charges under U.S. federal law. Cyber threat activity is a U.S. federal crime if it violates one or more of the following statutes, among others:

1. Computer Fraud and Abuse Act: 18 U.S.C. § 1030

The Computer Fraud and Abuse Act ("CFAA")[20] remains the U.S. government's principal tool for prosecuting computer crimes. In lay terms, the CFAA gives the owners of computers the right to control who may access their computers, take information from them, change how the computers work, or delete information on them. Just as the criminal laws against trespassing protect property rights in land, the CFAA protects property rights in computers. As such, the CFAA commits the United States to a cybersecurity policy that is founded on private property rights, and backed by enforcement of criminal law. The CFAA defines multiple crimes, and assigns each a different statutory maximum penalty.

Although a detailed description and analysis of each offense established by section 1030(a) is beyond the scope of this report,[21] below we provide a high-level overview of how the CFAA combats cyber threats.

Accessing a Computer and Obtaining Information: 18 U.S.C. § 1030(a)(2)

Section 1030(a)(2) protects the privacy of information stored on computers by criminalizing the act of accessing such information without authorization. The statute sets forth three distinct but overlapping crimes that collectively prohibit the unauthorized accessing of certain financial records stored on computers of financial institutions, of information from U.S. government computers, and of information from computers used in or affecting interstate or foreign commerce (for example, computers connected to the Internet). This provision applies both to outside hackers who gain access to victim computers without authorization from anywhere around the world, and to those who have

some authorization to access a computer, but who intentionally exceed that access.[22]

To violate section 1030(a)(2), a person must access, and thereby obtain, the prohibited information "intentionally." Mere mistake, inadvertence, or carelessness is insufficient.[23] Additionally, to be charged, the defendant must have understood that the access was unauthorized. Accordingly, federal prosecutions focus on hackers and insiders whose conduct evidences a clear intent to enter, without proper authorization, computer files or data belonging to another.

Damaging a Computer: 18 U.S.C. § 1030(a)(5)

Section 1030(a)(5) is a critical tool for prosecuting criminals who "damage" computers protected under the CFAA by causing computers to fail to operate as their owners intended. Section 1030(a)(5) is used to prosecute hackers or intruders who gain unauthorized access to a computer and commit criminal acts that, in any way, impair the integrity of data, a program, a system, or information, as well as change the way a computer is intended to operate. The statute extends to intruders who gain unauthorized access to a computer and send commands that delete files or shut the computer down. Subsection (a)(5) also may be used against cybercriminals who install malicious software that compromises a computer's integrity. Thus, installing remote access tools, bot code, and other attempts to persist on a victim's system are all chargeable under section 1030(a)(5). This provision is also an important tool for prosecuting criminals who cause intentional damage to computers by flooding an Internet connection with data during a distributed denial of service ("DDoS") attack.

Accessing a Computer to Defraud and Obtain Value: 18 U.S.C. § 1030(a)(4)

Section 1030(a)(4) establishes a felony offense that prosecutors use against hackers who access a protected computer without appropriate authorization in furtherance of a fraud to obtain something of value. The section bears similarities to the federal mail and wire fraud statutes (discussed below), but has a narrower jurisdictional scope by requiring that the cybercriminal victimize a protected computer without authorization or in excess of authorization.

Prosecutors use this provision against defendants who obtain information from a computer, and then later use that information to commit fraud. For example, section 1030(a)(4) was charged in a case involving a defendant who accessed a telephone company's computer without authorization, obtained calling card numbers, and then used those calling card numbers to make free long-distance telephone calls.[24] The provision also may be used to prosecute a defendant who alters or deletes records on a computer, and then receives something of value from an individual who relied on the accuracy of those altered or deleted records.[25]

Threatening to Damage a Computer: 18 U.S.C. § 1030(a)(7)

To deter high-tech attempts to commit old-fashioned extortion, section 1030(a)(7)

criminalizes threats to interfere in any way with the normal operation of a protected computer or system, as well as threats to compromise the confidentiality or integrity of information contained therein. This provision encompasses threats by criminals to deny access to authorized users, erase or corrupt data or programs, or slow down or shutdown the operation of the computer system, such as via a DDoS attack. The provision also reaches threats to steal confidential data.

Charging Policies

The Department's decisions about when to open an investigation or charge a case under the CFAA are guided by the Intake and Charging Policy for Computer Crime Matters.[26] As the policy explains, prosecutors must consider a number of factors in order to ensure that charges are brought only in cases that serve a substantial federal interest.[27] The policy also requires prosecutors to conduct certain consultations to assure consistent practice across the Department. In particular, prosecutors must consult with the Department's Computer Crime and Intellectual Property section before bringing charges under the CFAA.

2. Wire Fraud: 18 U.S.C. § 1343

The wire fraud statute is another particularly powerful and commonly applicable charge in computer crime cases involving fraud. Indeed, courts long have recognized that e-mails and other forms of Internet transmissions constitute "wire, radio, or television communication[s]" that may be punished under a wire fraud charge.[28] Section 1343 shares a number of common proof elements with section 1030(a)(4) of the CFAA, including the requirement that a defendant act with fraudulent intent; however, the wire fraud statute authorizes more punitive penalties that may be more commensurate to the harm suffered by victims in cases involving significant loss amounts. Section 1343 violations also can serve as a predicate for the Racketeer Influenced and Corrupt Organizations Act ("RICO") and money laundering charges, whereas most CFAA violations cannot.[29] Accordingly, the wire fraud statute is a particularly effective tool for prosecuting intricate networks of criminal hacker groups engaged in transnational organized crime.[30]

3. Identity Theft: 18 U.S.C. §§ 1028(a)(7) and 1028A

Cybercriminals often commit computer intrusions to compromise and steal PII that may be sold on the black market, or directly used to commit other crimes, such as wire fraud. A criminal who misuses or traffics in stolen PII often violates a variety of identity theft statutes, including 18 U.S.C. §§ 1028(a)(7) and 1028A.

In relevant part, section 1028(a)(7) criminalizes the unauthorized transfer, possession, or use of a "means of identification of another person" with the intent to commit (or aid and abet) a violation of federal law, or any State or local felony. The term "means of identification," in turn, broadly refers to "any name or number that may be used, alone or

in conjunction with any other information, to identify a specific individual."[31]

In computer intrusion cases, the Department also uses section 1028A (the "aggravated" identity theft statute) to prosecute individuals who engage in the unauthorized transfer, possession, or use of a "means of identification of another person" during and in relation to felony violations of certain enumerated federal offenses that are commonly associated with computer crime.[32] For example, "carders" who sell or trade stolen credit or debit card account information on online forums, or "phishers" who obtain the same type of information via fraudulent e-mails, often violate a predicate crime for a section 1028A violation. Similarly, defendants who violate the CFAA and obtain identity or account information may also violate this section. Although section 1028A is limited to a far narrower list of predicate offenses than section 1028(a)(7), it is an important and powerful tool in the Department's prosecutions of cybercriminals because those who are convicted of section 1028A are subject to a mandatory minimum two-year term of imprisonment.[33]

4. Economic Espionage and Theft of Trade Secrets: 18 U.S.C. §§ 1831-32

Trade secret law prohibits the unauthorized disclosure of confidential and proprietary information (for example, a formula or compilation of information) when that information possesses an independent economic value because it is secret, and the owner has taken reasonable measures to keep it secret.[34] Although the problem of trade secret theft predates the modern era of cybercrime, the increased digitalization of trade secrets, the rise of cyber espionage, and the global expansion of online marketplaces that traffic in intellectual property, have significantly magnified the threats that insiders, hackers, and nation states present to U.S. individuals and companies who maintain valuable trade secrets.[35] Indeed, in recent years, businesses across key sectors of the U.S. economy have suffered sophisticated and systematic cyber intrusions designed to steal sensitive commercial data from compromised networks, including research and design data, software source code, and plans for commercial and military systems.

The Department's principal tool for preventing and deterring serious instances of trade secret theft is the Economic Espionage Act ("EEA"). The EEA criminalizes two types of trade secret misappropriation: economic espionage under section 1831, and trade secret theft under section 1832. The economic espionage provision prohibits the theft of trade secrets for the benefit of a foreign government, instrumentality, or agent. The theft of trade secrets provision prohibits the commercial theft of trade secrets to benefit someone other than the owner. Although the provisions define separate offenses, they share a number of common proof elements. Notably, conviction under either statute requires the government to demonstrate beyond a reasonable doubt that: (1) the defendant misappropriated information; (2) the defendant knew or believed this information was proprietary and that he had no claim to it; and (3) the information was in fact a trade secret (unless the crime charged is a conspir-

acy or an attempt). Further, both provisions are subject to the EEA's broad definition of a "trade secret," which includes all types of information that the owner has taken reasonable measures to keep secret and that itself has independent economic value.[36] Both provisions also punish attempts and conspiracies to misappropriate trade secrets.[37] To promote enforcement, federal law provides special protections to victims in trade secret cases to ensure that the confidentiality of trade secret information is preserved during the course of criminal proceedings.[38]

5. Criminal Copyright: 17 U.S.C. § 506

Copyright law provides federal protection against infringement of certain exclusive rights, such as reproduction and distribution, of "original works of authorship," including computer software, literary works, musical works, and motion pictures.[39] As with trade secrets, the increased digitalization of copyrighted materials, as well as the global expansion of online marketplaces that traffic in intellectual property, have enhanced their attractiveness and, in turn, vulnerability to cybercriminals.

The Department's principal tool for preventing and deterring serious instances of copyright infringement is section 506(a) of title 17, United States Code, which criminalizes willful copyright infringement if committed "for purposes of commercial advantage or private financial gain," or "by the reproduction or distribution" of copyrighted works during a 180-day period that satisfies the statute's minimum retail value. Section 506(a)(1)(C) also makes it a crime to pre-release copyrighted materials, such as a commercial film, song, video game, or software, that are still "being prepared for commercial distribution," by making the material "available on a computer network accessible to members of the public."

6. Access Device Fraud: 18 U.S.C. § 1029

Section 1029 of title 18, United States Code, broadly prohibits the production, use, possession, or trafficking of unauthorized or counterfeit "access devices," such as PII, instrument identifiers, or other means of account access that may be used "to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds." Prosecutors commonly bring charges under section 1029 in "phishing" cases, in which a cybercriminal uses fraudulent e-mails to obtain bank account numbers and passwords. Section 1029 also is an effective tool in "carding" cases where a defendant purchases, sells, or transfers stolen bank account, credit card, or debit account information. Forfeiture is also available in many cases.[40]

7. Racketeer Influenced and Corrupt Organizations (RICO) Act: 18 U.S.C. §§ 1961–1968

Computer hacking conducted by transnational criminal groups poses a significant threat to American cybersecurity. Equipped with sizable funds, organized criminal groups operating abroad employ highly sophisticated malicious software, spear-phish-

ing campaigns, and other hacking tools—some of which rival in sophistication those that nation states use—to hack into sensitive financial systems, conduct massive data breaches, spread ransomware, attack critical infrastructure, and steal critical intellectual property. For transnational cybercrime rings engaged in "racketeering" activity, such as identity theft, access device fraud, or wire fraud, a RICO charge may be a particularly effective tool for prosecuting individual members of the group. For instance, the RICO statute authorizes more severe penalties than the CFAA, including maximum sentences of 20 years or more depending on the nature of the predicate offense,[41] consecutive sentencing for RICO substantive and conspiracy convictions or violations of two substantive RICO subsections,[42] and forfeiture of all reasonably foreseeable proceeds of racketeering activity on a joint and several basis.[43] Section 1963(d)(2) of title 18, United States Code, also empowers prosecutors to obtain a pre-trial restraining order that preserves any assets that may be subject to forfeiture following conviction. In addition, a RICO conspiracy charge under section 1962(d) of title 18 allows prosecutors to hold one defendant responsible for the conduct of the enterprise.

8. Wiretap Act: 18 U.S.C. § 2511

The same surveillance statutes that empower law enforcement to collect evidence also protect the privacy of innocent Americans by criminalizing the unlawful collection of private communications. For example, the Wiretap Act shields private wire, oral, or electronic communications from illegal interception by another,[44] prohibits disclosure of any illegally intercepted communication,[45] and criminalizes unlawful use of that communication.[46] The Wiretap Act has proven to be an especially valuable tool for prosecuting cases involving spyware users and manufacturers, intruders using packet sniffers (i.e., tools that intercept data flowing in a network), persons improperly cloning e-mail accounts, and other cases involving the surreptitious collection of communications from a victim's computer.

To prosecute a defendant under this statute, however, federal courts have generally required that the "intercepted" communications be acquired "contemporaneously" or at approximately the same time as their transmission.[47] Accordingly, merely obtaining a copy of the contents of a recorded communication—for example, a year-old e-mail on a mail server—is not necessarily a criminal "intercept[ion]" of the communication under the Wiretap Act, though such an action may violate other provisions of law, including the Stored Communications Act, 18 U.S.C. § 2701.[48]

9. Money Laundering: 18 U.S.C. §§ 1956, 1957

Cybercrimes are often committed for financial gain. And as with other crimes, those committing cybercrimes will seek ways to conceal and spend their ill-gotten gains. Federal money laundering laws are thus an important tool for combatting cybercrime. These laws criminalize certain transactions undertaken with the proceeds of designated crimes, referred to as "specified unlawful ac-

tivity" ("SUA").[49] Crimes classified as SUAs include many common charges brought in cybercrime cases, such as violations of the CFAA and wire fraud.

Section 1956 of title 18, United States Code, is the main money laundering charge. Among other things, this statute makes it a crime for a person to carry out a financial transaction involving SUA proceeds when the person knows the transaction involves illicit proceeds of some kind, and the transaction is designed to promote the carrying on of an SUA,[50] or to conceal "the nature, the location, the source, the ownership, or the control of the proceeds"[51] of the predicate crime. Section 1957 prohibits knowingly conducting certain monetary transactions involving SUA proceeds when the value is greater than $10,000.

Courts have broadly interpreted the scope of the transactions covered by the money laundering laws. In particular, courts have upheld the use of money laundering charges involving transactions in virtual currencies.[52]

10. Controlling the Assault of Non-Solicited Pornography and Marketing Act: 18 U.S.C. § 1037

The Controlling the Assault of Non-Solicited Pornography and Marketing ("CAN-SPAM") Act of 2003[53] provides a means for prosecuting those responsible for sending large amounts of unsolicited commercial e-mail messages (i.e., "spam"), including messages sent on social media sites. Although civil and regulatory provisions are the Act's primary enforcement mechanisms, it also created several new criminal offenses. Section 1037 addresses more egregious violations of the CAN-SPAM Act, particularly where the perpetrator has taken significant steps to hide his or her identity, or the source of the spam, from recipients, ISPs, or law enforcement agencies. Prosecutors have used this statute in the context of disrupting or dismantling botnets.

11. National Security Statutes

Some statutes that protect sensitive national security information are implicated in computer hacking investigations, when that information is targeted or stolen. For example, defense articles and services listed on the U.S. munitions list, 22 C.F.R. § 121.1, cannot be exported without a license without violating the Arms Export Control Act, 22 U.S.C. § 2778 ("AECA"). Other U.S.-origin items and related technology that have both commercial and military applications or otherwise warrant control are subject to the Export Administration Regulations ("EAR"), 15 C.F.R. pts. 730-74, and may require a license for export to certain countries or for certain uses. The statute that criminalizes violation of the EAR (among other regulations) is the International Emergency Economic Powers Act, 50 U.S.C. § 1705 ("IEEPA"). A Chinese aerospace engineer was recently convicted of violating AECA for helping hackers in the Chinese air force choose which defense contractors to target and which files related to military projects

to steal;[54] and a network of Iranian computer hackers (one of whom was apprehended) was charged with violating AECA and Iranian sanctions under IEEPA for stealing specialized software from the networks of American software companies, which the defendants are alleged to have resold for profit to Iranian government entities.[55] Classified information and national defense information, too, are protected by a number of criminal statutes. The CFAA specifically prohibits obtaining certain restricted data and information protected against disclosure for reasons of national defense or foreign relations through unauthorized access to a computer, *see* 18 U.S.C. § 1030(a)(1), and espionage statutes prohibit the unauthorized retention of national defense information or its dissemination to an unauthorized person (whatever the means of doing so). *See* 18 U.S.C. §§ 793 & 794.

Finally, material support to terrorists is likewise prohibited, even if that support is provided online. *See* 18 U.S.C. §§ 2339A, 2339B. As discussed in Chapter 2, for example, Ardit Ferizi was an Islamic State of Iraq and the Levant ("ISIL")-linked hacker living in Malaysia who may never have met ISIL recruiters in Iraq. But when Ferizi broke into the networks of an American retailer, stole PII for thousands of U.S. persons, and culled that list down to approximately 1,300 military and other government personnel that he shared with ISIL for purposes of publishing a kill list and enabling ISIL to "hit them hard," he provided such support. Ferizi was apprehended, brought to the United States, and is now serving a 20-year sentence for providing material support to ISIL.[56]

Other Means of Dismantling, Disrupting, and Deterring Computer Crimes

While criminal prosecutions of malicious cyber activity (and seizing the ill-gotten gains of such activity) are an important aspect of the Department's approach to combating cybercrime, we recognize that the United States cannot simply prosecute its way out of the problem. Instead, the Department has embraced a comprehensive approach to deterring cyber threats that builds upon a broad array of criminal, civil, and national security authorities, tools, and capabilities. Indeed, the government as a whole relies on a range of civil and administrative tools to raise the costs associated with malicious cyber activity, and to disrupt ongoing activities in the cyber underworld.

To support this broader approach, we work to interdict cyber threats before they become actual incidents by denying malign actors access to infrastructure, tools, funds, and victims, as well as by working with international partners and members of the private sector, who often may be better positioned to prevent cybercrime.

Congress has given the Department the legal authority to disrupt, dismantle, and deter cyber threats through a blend of civil,

criminal, and administrative powers beyond traditional prosecution. As a result, the Department has been a driving force behind the U.S. government's most notable and effective measures to disrupt online crime. As mentioned above, the Department often uses civil injunctions, as well as seizure and forfeiture authorities, to disrupt cybercriminal groups by seizing the computer servers and domain names those actors use to operate botnets. In cases where the actors cannot quickly be identified, such tools—exercised with proper judicial oversight—have helped the Department disrupt and dismantle ongoing criminal schemes, thereby protecting the public from further victimization. Finally, the Department, with the assistance of other U.S. government and international partners, also executes trade actions, and participates in various cyber operations designed to neutralize and eradicate international cyber threats.

1. Disrupting and Disabling International Botnets

In recent years, the Department has successfully disrupted and disabled a number of international botnets not only by arresting and prosecuting the criminals involved in their creation and administration, but also by leveraging other civil, criminal, and administrative authorities. For instance, the Department uses civil injunctive authority under section 1345 (injunctions against fraud) and section 2521 (injunctions against illegal interception) to authorize actions—such as seizing domains the botnet is using to communicate with command-and-control servers—to disrupt and disable a botnet's ongoing commission of fraud crimes or illegal wiretapping. Accompanying temporary restraining orders ("TROs") secured under Rule 65 of the Federal Rules of Civil Procedure also are important to disrupting

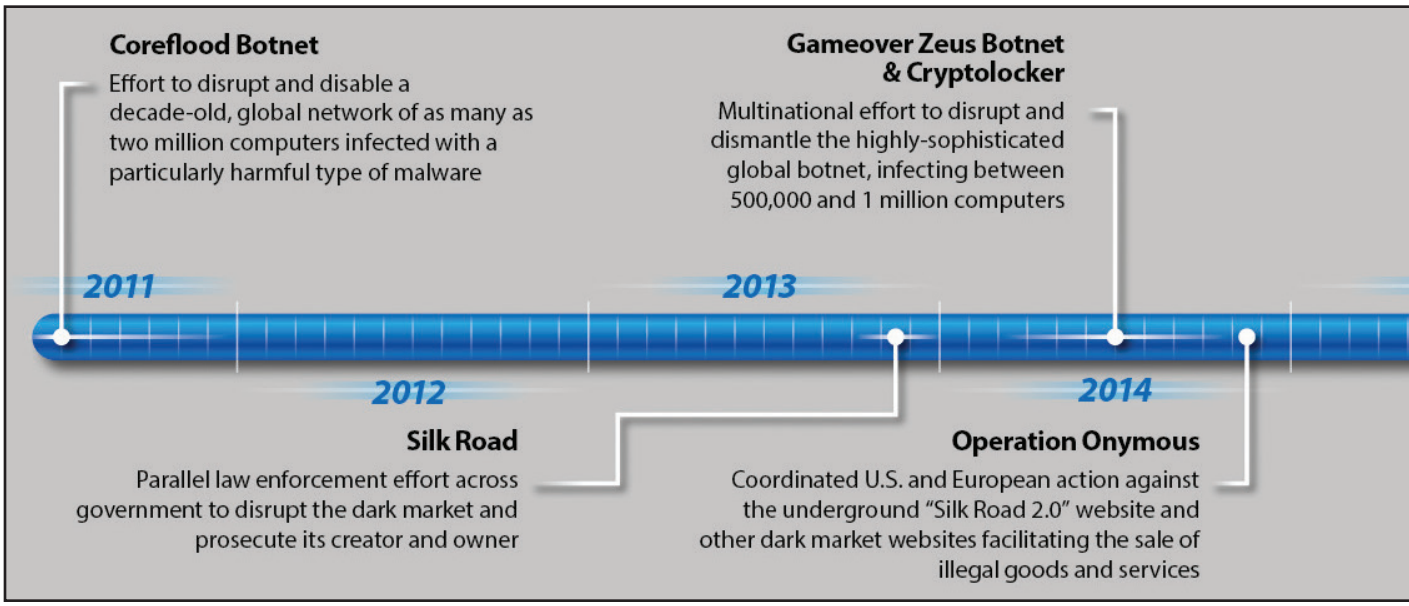


Figure 1: Recent Department efforts to dismantle botnets and dark markets.

a botnet, and taking immediate steps to prevent it from reconstituting.

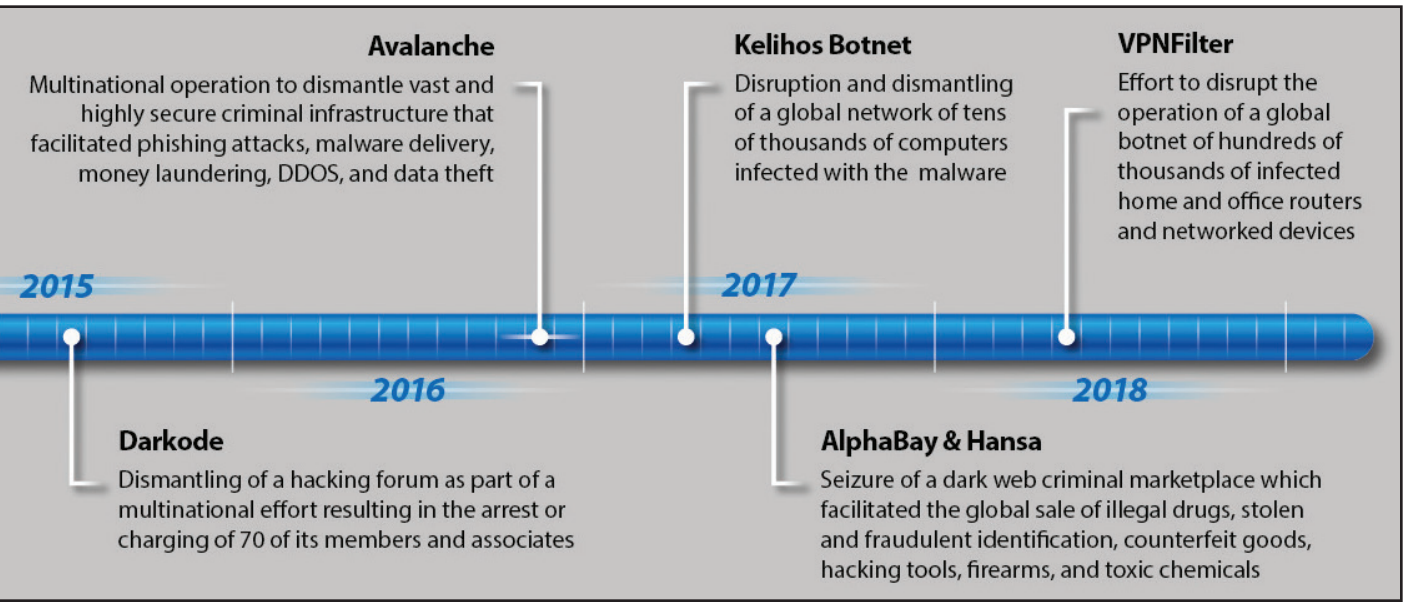
Further, as discussed above, if law enforcement is able to take over the command-and-control structure of a botnet, the Department may now use the recently promulgated venue provision of criminal Rule 41(b)(6)(B) to issue commands to bots across a number of districts. For example, law enforcement may obtain identifying information from affected bot computers in order to contact owners and warn them of the infection. In addition, law enforcement might engage in an online operation designed to disrupt the botnet and restore full control over computers to their legal owners. Rule 41(b)(6)(B) allows the government to apply for warrants in a single judicial district to use these techniques.

Several successful examples of the Department's strategy for disrupting and disabling botnets are illustrated in **Fig. 1,** and described in greater detail in Appendix 2.

2. Dark Web Disruptions

In recent years, the Dark Web's anonymity and low barriers to entry have attracted scores of criminals to Dark Web markets, including those trafficking in child pornography, illicit firearms, illegal drugs, murder-for-hire, and human trafficking. Sophisticated hackers also frequent Dark Web forums for the newest malware or stolen data, and might use the Tor network to host botnet command-and-control infrastructure that is more resistant to disruption and take-downs.

Despite the many challenges the Dark Web poses, law enforcement around the world have successfully disrupted criminals operating in the cyber underground by de-anonymizing users engaging in illegal activity;



seizing their websites, domains, servers, and ill-gotten gains; and criminally prosecuting them. For instance, to pierce the Dark Web's anonymizing technology, the Department diligently pursues traditional investigative techniques, studies patterns of criminal activity, collaborates with international law enforcement partners, and develops human sources. Further, where anonymizing technologies make less intrusive investigative options ineffective, the Department also obtains warrants to perform remote searches using network investigative techniques under limited circumstances.[57] For example, appropriate scenarios for seeking a warrant to authorize a remote search include, but are not limited to: (1) obtaining stored content from a hidden provider by using a username and password; (2) identifying a criminal using a web-based e-mail account by sending a NIT to the criminal's e-mail account; and (3) identifying users of a hidden child pornography forum by sending a NIT to each computer used to log on to the website.

Once the cloak of anonymity has been pulled back, the Department leverages a range of civil and criminal tools, including civil and criminal forfeiture authorities, seizure warrants, and requests under mutual legal assistance agreements to dismantle the infrastructure undergirding the Dark Web systems and recover the proceeds of these illegal activities. Further, in many instances, individuals responsible for creating, operating, and using Dark Web forums and marketplaces are also criminally prosecuted. We describe in Appendix 3 some recent prominent examples of the Department's comprehensive strategy to combat malicious activity on the Dark Web.

3. Sanctions and Designations

To ensure that investigative information is used effectively to protect the Nation, the Department regularly interacts with the Departments of Commerce, Treasury, and State, as well as with other agencies and regulatory bodies, to support those departments' actions to identify and impose sanctions on malicious cyber actors.

Sanctions imposed by the Office of Foreign Assets Control at the Department of the Treasury can deprive subjects of their access to the U.S. financial system and their ability to do business with U.S. persons, and can be particularly effective in reaching foreign companies that benefit from stolen information. Since 2011, the Treasury Department has had the authority to block the property of transnational criminal organizations under Executive Order 13581 ("Blocking Property of Transnational Criminal Organizations"). Treasury also makes use of country-specific regimes to respond to nation-state behavior. As mentioned in Chapter 2, following North Korea's destructive malware attack on Sony Pictures Entertainment, the President in 2015 issued Executive Order 13687 ("Imposing Additional Sanctions with Respect to North Korea"). Using this new sanction authority, the Treasury Department designated three entities for being "controlled entities of the Government of North Korea" and ten

individuals for being "agencies or officials of the North Korean government."[58]

In 2015, the President also issued Executive Order 13694 ("Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities"), which authorized the Secretary of the Treasury, in consultation with the Attorney General and the Secretary of State, to impose sanctions on individuals or entities that engage in malicious cyber-enabled activity that results in, or materially contributes to, a significant threat to the national security, foreign policy, or economic health or financial stability of the United States.[59] In December 2016, the President amended this executive order in "order to take additional steps to deal with the national emergency with respect to significant malicious cyber-enabled activities . . . in view of the increasing use of such activities to undermine democratic processes or institutions."[60] The 2016 amendment expanded cyber-related sanctions and in an annex designated five Russian entities—including that nation's domestic and foreign intelligence services—and four Russian individuals who were determined to have interfered with or undermined U.S. election processes or institutions.[61] The list of designated parties was expanded again on March 15, 2018,[62] and yet again on June 11, 2018.[63]

Designations under E.O. 13694 are not limited to Russian actors. On March 23, 2018, in consultation with the Department, OFAC designated an Iranian entity, the Mabna Institute, and ten Iranian individuals who

Credit: Amy Mathers, U.S. Department of Justice

Deputy Attorney General Rod Rosenstein announces on March 23, 2018 the filing of criminal charges against nine Iranians alleged to have conducted a massive cyber theft campaign on behalf of the Islamic Revolutionary Guard Corps. The Treasury Department imposed sanctions the same day.

engaged in theft of valuable intellectual property and data from hundreds of U.S. and third-country universities and a media company for private financial gain.[64] (That same day, the Department unsealed criminal charges against the same entity and nine individuals.[65] *See* page 73.)

The Department will continue to support sanctions under such authorities by helping the Treasury Department draft sanction nomination packages based on the information gathered during our investigations. Where, for example, investigations identify hackers who victimize U.S. individuals or companies, or those who profit from criminal hacking by using stolen personal information or trade secrets, the Department works with the Treasury Department to craft appropriate sanctions against those responsible.

Similarly, the Commerce Department can place persons and companies on its Entity List if it finds that they are engaged in activities that are contrary to U.S. national security or foreign policy interests.[66] Persons and entities on the Entity List are subject to special licensing requirements for the export, re-export, and/or transfer (in-country) of items listed in the EAR. In 2014, for example, in addition to the Department of Justice's prosecution of a Chinese engineer for consulting with Chinese military hackers who stole aerospace technology, the Commerce Department placed his company on the Entity List, based on the FBI's nomination.[67] Such a listing can have dramatic consequences, cutting the firm off from U.S. exports and causing U.S. and foreign businesses to reconsider doing business with the designated entity.

4. Trade Actions

The Office of the United States Trade Representative ("USTR") can raise the issue of foreign cyber intrusions against American businesses in the context of its trade actions under various U.S. laws or trade agreements. As declared in a USTR report made public in April 2017, "The United States uses all trade tools available to ensure that its trading partners provide robust protection for trade secrets and enforce trade secrets laws."[68] The Department has worked closely with USTR to ensure that the Trade Representative is appropriately informed about cyber-enabled activity by nation states that may be actionable under U.S. trade laws.

Due in part to China's cyber-enabled theft of U.S. intellectual property and sensitive commercial information, the U.S. government in March 2018 announced various tariffs against China and various restrictions on Chinese investments.[69] The announcement came after USTR released a comprehensive public report as part of its investigation under section 301 of the Trade Act of 1974.[70] The USTR report establishes a clear record of China's cyber intrusions and cyber theft based on information provided by the Department, among other parts of the U.S. government. The report indicates that the Chinese government has used cyber intrusions to serve its strategic economic objectives and that "incidents of China's cyber intrusions against U.S. commercial entities align closely with China's industrial policy objectives."[71] For example, the PLA's theft of trade secrets from Westinghouse, Inc., as documented in an indictment brought by the Depart-

ment, illustrates how China uses cyber-enabled theft as one of multiple instruments to achieve its state-led technology development goals.[72] Likewise, the USTR report noted that "[i]n September 2017, the Department filed an indictment against three Chinese nationals who were owners, employees, and associates of the Guangzhou Bo Yu Information Technology Company Limited ("Boyusec"), a company that cybersecurity firms have linked to the Chinese government."[73] The USTR report contains other examples that illustrate how China uses cyber-enabled intrusions to further the commercial interests of Chinese state-owned enterprises, to the detriment of its foreign partners and competitors. Available evidence also indicates that China uses its cyber capabilities as an instrument to achieve its industrial policy and science and technology objectives. The Department has played an important role in bringing these threats to our national security to light.

5. Cyber Operations

Finally, the Department also assists other agencies in analyzing the legal and policy implications of operations conducted through cyberspace, and ensuring that these operations comply with the Constitution and applicable law. Where additional authority or injunctive relief is required to address conduct within the United States, the Department works with investigators and, as appropriate, the U.S. Attorney community, to pursue it. Intelligence gathered by the FBI using its national security investigative authorities may also assist agencies in planning or carrying out such operations.

NOTES

[1] The Department components responsible for this work are described in Chapter 5.

[2] For example, the FBI, as the federal government's primary investigative agency, must comply with *The Attorney General's Guidelines for Domestic FBI Operations*, available at: https://www.justice.gov/archive/opa/docs/guidelines.pdf (last accessed June 29, 2018), and the *FBI Domestic Investigations and Operations Guide*, available at: https://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29/fbi-domestic-investigations-and-operations-guide-diog-2013-version/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29%202013%20Version%20Part%2001%20of%2001/view (last accessed June 29, 2018), which standardizes the FBI's criminal, national security, and foreign intelligence investigative activities. The *Attorney General's Guidelines* establish a set of basic principles that serve as the foundation for all FBI mission-related activities, and the professional identity of each FBI agent, including: (1) protecting the public includes protecting their rights and liberties; (2) investigating only for a proper and authorized law enforcement, national security, or foreign intelligence purpose; (3) ensuring that an independent, authorized law enforcement or national security purpose exists for initiating investigative activity—race, ethnicity, religion, or national origin alone can never constitute the sole basis for initiating investigative activity; (4) performing only authorized activities in pursuit of investigative activities; (5) employing the least intrusive means for investigation that do not otherwise compromise FBI operations; and (6) applying best judgment to the circumstances at hand to select the most appropriate investigative means to achieve the investigative goal.

[3] *See* ICANN WHOIS, available at: https://whois.icann.org/en (last accessed June 29, 2018).

[4] Pub. L. No. 99–508, 100 Stat. 1848 (1986) (codified at 18 U.S.C. § 2510 *et seq.*).

[5] *See* 18 U.S.C. § 2703.

[6] *Id.* § 3121 *et seq.*

[7] *Id.* § 2510 *et seq.*

[8] 50 U.S.C. § 1801 *et seq*.

Virtual currency seizures with a value of $500,000 or more must be forfeited judicially. The value is assessed on the date of agency seizure.

[10] *See*, *e.g.*, "For Sale Approximately 3,813.0481935 Bitcoins," U.S. Marshals Service (Jan. 2018), available at: https://www.usmarshals.gov/assets/2018/bitcoinauction/ (last accessed June 29, 2018).

[11] 18 U.S.C. §§ 981-983.

[12] *See* Press Release, "Russian National And Bitcoin Exchange Charged In 21-Count Indictment For Operating Alleged International Money Laundering Scheme And Allegedly Laundering Funds From Hack Of Mt. Gox," U.S. Dept. of Justice (July 26, 2017), available at: https://www.justice.gov/usao-ndca/pr/russian-national-and-bitcoin-exchange-charged-21-count-indictment-operating-alleged (last accessed June 29, 2018).

[13] A "John Doe" summons is an administrative summons that may be used, with court approval, to seek information about an ascertainable group or class of persons who may be involved in violating federal tax laws. *See* 26 U.S.C. § 7609(f) (2012).

[14] *United States* v. *Coinbase, Inc. et al.*, Order Regarding Petition to Enforce IRS Summons at 14 (Doc. 78), Case No. 3:17-cv-01431 (N.D. Cal.).

[15] *See* 18 U.S.C. § 3181 note (listing the countries with which the United States currently has a bilateral extradition agreement).

[16] Quoted from the United States's sentencing memorandum in *United States* v. *Roman Seleznev*, No. 11-CRM-007 (W.D. Wa., Apr. 14, 2017), available at: https://assets.documentcloud.org/documents/3673513/Seleznev-US-Atty-Sentencing-Memo.pdf (last accessed June 29, 2018).

[17] *See* Press Release, "Russian Cyber-Criminal Sentenced to 14 Years in Prison for Role in Organized Cybercrime Ring Responsible for $50 million in Online Identity Theft and $9 Million Bank Fraud Conspiracy," U.S. Dept. of Justice (Nov. 30, 2017) (describing all of Seleznev's federal sentences), available at: https://www.justice.gov/opa/pr/russian-cyber-criminal-sentenced-14-years-prison-role-organized-cybercrime-ring-responsible (last accessed June 29, 2018).

[18] https://www.unodc.org/documents/middleeastandnorthafrica/organised-crime/UNITED_NATIONS_CONVENTION_AGAINST_TRANSNATIONAL_ORGANIZED_CRIME_AND_THE_PROTOCOLS_THERETO.pdf (Art. XIX) (last accessed June 29, 2018).

[19] https://www.state.gov/documents/organization/180815.pdf (Art. V) (last accessed June 29, 2018).

[20] Although the CFAA is primarily a criminal statute, individuals and companies may also bring private civil suits against CFAA violators. *See* 18 U.S.C. § 1030(g). This report does not address the civil provisions of the statute except as they may pertain to the criminal provisions.

[21] More specific guidance on the CFAA is available at: https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf (last accessed June 29, 2018).

[22] In the Second, Fourth, and Ninth Circuits, significant recent decisions have limited the definition of "exceeds authorized access" in 18 U.S.C. § 1030(e)(6) "to violations of restrictions on *access* to information, and not restrictions on its *use*." *See, e.g.*, *United States v. Nosal*, 676 F.3d 854, 863-64 (9th Cir. 2012). Other language in *Nosal* suggests that the Ninth Circuit's ultimate holding is broader: that an individual can "exceed[] authorized access" only by accessing data that he or she was never authorized to access, under any circumstances. Accordingly, in those circuits, the Department recommends against charging any case that relies on the definition of "exceeds authorized access" in 18 U.S.C. § 1030(e)(6), unless it can be proven that the computer user had *absolutely no authorization to access the relevant information*.

[23] *See*, *e.g.*, S. Rep. No. 432, 99th Cong., 2d Sess., *reprinted in* 1986 U.S.C.C.A.N. 2479, 2483.

[24] *See United States* v. *Lindsley*, 254 F.3d 71 (5th Cir. 2001).

[25] *See*, *e.g.*, *United States* v. *Butler*, 16 Fed. Appx. 99 (4th Cir. 2001) (unpublished).

[26] *See* Memorandum from Eric Holder, Attorney General, "Intake and Charging Policy for Computer Crime Matters," (Sept. 11, 2014), available at: https://www.justice.gov/criminal-ccips/file/904941/download (last accessed June 29, 2018).

[27] *See id*.

[28] *See*, *e.g.*, *United States* v. *Selby*, 557 F.3d 968, 978-79 (9th Cir. 2009) (finding defendant's act of

sending a single e-mail "sufficient to establish the element of the use of the wires in furtherance of the scheme"); *United States* v. *Drummond*, 255 Fed. Appx. 60, 64 (6th Cir. 2007) (unpublished) (affirming wire fraud conviction where defendant made airline reservation with stolen credit card over the Internet).

[29] As explained below, exceptions exist for terrorism-related violations of section 1030(a)(1) and 1030(a)(5)(A).

[30] The United States Attorneys' Manual provides further guidance regarding wire fraud charges, *see* U.S. Dept. of Justice, United States Attorneys' Manual, § 9-43.000, as does the manual, Identity Theft and Social Security Fraud (Office of Legal Education 2004).

[31] 18 U.S.C. § 1028(d)(7). Although there is little dispute about classifying a unique identifier, such as a social security number, as a "means of identification," some courts have questioned whether non-unique identifiers, such as names or birthdates, qualify as a "means of identification" when standing alone. *Compare United States v. Silva*, 554 F.3d 13, 23 n.4 (1st Cir. 2009) (finding doctor's signature constitutes a "means of identification"), *with United States v. Mitchell*, 518 F.3d 230, 232-36 (4th Cir. 2008) (requiring that non-unique identifiers be combined with additional information that permits the identification of a specific person).

[32] *E.g.*, 18 U.S.C. §§ 1028(a)(1)-(6), (8), 1029, 1030, 1037, 1343.

[33] 18 U.S.C. § 1028A(a)(1); *see also id.* § 1028A(a)(2) (providing a minimum five-year term for terrorism-related aggravated identity theft).

[34] *See* 18 U.S.C. §§ 1831, 1832.

[35] *Combating Economic Espionage and Trade Secret Theft, Hearing Before the S. Judiciary Comm., Subcomm. on Crime and Terrorism of the S. Judiciary Comm.*, 113 Cong. 4 (2016) (statement of Randall C. Coleman, Assistant Dir., Counterintelligence Div. FBI), available at: https://www.govinfo.gov/content/pkg/CHRG-113shrg96009/pdf/CHRG-113shrg96009.pdf (last accessed June 29, 2018).

[36] 18 U.S.C. § 1839(3).

[37] *See id.* §§ 1831(a)(4)-(5), 1832(a)(4)-(5). For an attempt, the defendant must (1) have the intent needed to commit one of the two crimes, and (2) perform an act amounting to a "substantial step" toward the commission of that crime. *United States* v. *Hsu*, 185 F.R.D. 192, 202 (E.D. Pa. 1999). For a conspiracy, the defendant must agree with one or more people to commit a violation, and one or more of the co-conspirators must commit an overt act to effect the object of the conspiracy. 18 U.S.C. §§ 1831(a)(5), 1832(a)(5).

[38] *See id.* § 1835.

[39] *See* 17 U.S.C. §§ 102(a), 106 (2012).

[40] *See* 18 U.S.C. § 1029(c)(1)(C), (c)(2).

[41] *Id.* § 1963(a).

[42] Organized Crime & Gang Section, U.S. Dept. of Justice, CRIMINAL RICO: 18 U.S.C. §§1961-1968, A Manual For Federal Prosecutors (May 2016), https://www.justice.gov/usam/file/870856/download (last visited June 29, 2018).

[43] *Id.* at 238-39.

[44] 18 U.S.C. § 2511(1)(a) & (b).

[45] *Id.* § 2511(1)(c) § (e).

[46] *Id.* § 2511(1)(d).

[47] *See, e.g.*, *In re Pharmatrak, Inc. Privacy Litig.*, 329 F.3d 9, 21 (1st Cir. 2003).

[48] Similarly, other surveillance statutes like the Pen Trap Act and FISA criminalize violations of their provisions. *See* 18 U.S.C. § 3121 (Pen Trap Act); 50 U.S.C. § 1809 (FISA).

[49] 18 U.S.C. § 1956(c)(7) (defining SUA).

[50] *Id.* § 1956(a)(1)(A)(i).

[51] *Id.* § 1956(a)(1)(B)(i).

[52] *See United States* v. *Budovsky*, 2015 WL 5602853, at *12-13 (S.D.N.Y. Sept. 23, 2015) (holding that virtual currency created by Liberty Reserve constituted funds within the meaning of § 1956); *United States* v. *Ulbricht,* 31 F. Supp. 3d 540, 569-70 (S.D.N.Y. 2014) (holding that transactions involving Bitcoin were financial transactions within the scope of § 1956).

[53] Pub. L. No. 108-187, 117 Stat. 2699 (2003).

[54] Press Release, "Chinese National Who Conspired to Hack into U.S. Defense Contractors' Systems Sentenced to 46 Months in Federal Prison," U.S. Dept. of Justice (July 13, 2016), available at: https://www.justice.gov/opa/pr/chinese-national-who-conspired-hack-us-defense-contractors-systems-sentenced-46-months (last accessed June 15, 2018).

[55] Press Release, "Two Iranian Nationals Charged in Hacking of Vermont Software Company," U.S. Dept. of Justice (July 17, 2017), available at: https://www.justice.gov/opa/pr/two-iranian-nationals-charged-hacking-vermont-software-company (last accessed June 15, 2018).

[56] Press Release, "ISIL-Linked Kosovo Hacker Sentenced to 20 Years in Prison," U.S. Dept. of Justice (Sept. 23, 2016), available at: https://www.justice.gov/opa/pr/isil-linked-kosovo-hacker-sentenced-20-years-prison (last accessed June 15, 2018).

[57] As with all investigative techniques, Department personnel are trained to use remote search tools appropriately and lawfully. Additionally, the FBI is required to adhere to the Attorney General's *Guidelines for Domestic FBI Operations* and the FBI's *Domestic Investigations and Operations Guide* in conducting remote searches and seizures; *see supra* note 2. These documents require the FBI to use the least intrusive method that is feasible when conducting a search. *See Guidelines for Domestic FBI Operations*, § 1(c)(2)(A); *Domestic Investigations and Operations Guide*, § 18.2.

[58] Press Release, "Treasury Sanctions Additional North Korean Officials and Entities in Response to the Regime's Serious Human Rights Abuses and Censorship Activities," U.S. Dept. of the Treasury (Oct. 26, 2017), available at: https://www.treasury.gov/press-center/press-releases/Pages/sm0191.aspx (last accessed June 29, 2018).

[59] Exec. Order No. 13694, 3 C.F.R. 297 (2016).

[60] Exec. Order No. 13757, 3 C.F.R. 1 (2017).

[61] *Id.*

[62] Press Release, "Treasury Sanctions Russian Cyber Actors for Interference with the 2016 U.S. Elections and Malicious Cyber-Attacks," U.S. Dept. of Treasury (March 15, 2018), available at: https://home.treasury.gov/index.php/news/press-releases/sm0312 (last accessed June 29, 2018).

[63] Press Release, "Treasury Sanctions Russian Federal Security Service Enablers," U.S. Dept. of Treasury (June 11, 2018), available at: https://home.treasury.gov/news/press-releases/sm0410 (last accessed June 29, 2018).

[64] Press Release, "Treasury Sanctions Iranian Cyber Actors for Malicious Cyber-Enabled Activities Targeting Hundreds of Universities," U.S. Dept. of Treasury (March 23, 2018), available

at: https://home.treasury.gov/news/press-releases/sm0332 (last accessed June 29, 2018).

[65] Press Release, "Nine Iranians Charged With Conducting Massive Cyber Theft Campaign on Behalf of the Islamic Revolutionary Guard Corps," U.S. Dept. of Justice (March 23, 2018), available at: https://www.justice.gov/opa/pr/nine-iranians-charged-conducting-massive-cyber-theft-campaign-behalf-islamic-revolutionary (last accessed June 29, 2018).

[66] Export Administration Regulations, Control Policy: End-User and End-Use Based, 15 C.F.R. §§ 744.1–.22 (2016), available at: https://www.gpo.gov/fdsys/pkg/CFR-2016-title15-vol2/xml/CFR-2016-title15-vol2-part744.xml (last accessed June 29, 2018).

[67] "Addition of Certain Persons to the Entity List," 79 Fed. Reg. 44680 (Aug. 1, 2014), available at: https://www.gpo.gov/fdsys/pkg/FR-2014-08-01/pdf/2014-17960.pdf (last accessed June 29, 2018) (adding PRC Lode Technology Corporation, a company owned by Su Bin, a Chinese national serving a prison term for conspiring with Chinese air force officers to exploit computer systems of U.S. companies and of DoD contractors to illicitly obtain and export information, including controlled technology, related to military projects).

[68] "2017 Special 301 Report," Office of the United States Trade Representative at 18 (April 2017), available at: https://ustr.gov/sites/default/files/301/2017%20Special%20301%20Report%20FINAL.PDF (last accessed June 29, 2018).

[69] *See* "Remarks by President Trump at Signing of a Presidential Memorandum Targeting China's Economic Aggression," The White House (March 22, 2018), available at: https://www.whitehouse.gov/briefings-statements/remarks-president-trump-signing-presidential-memorandum-targeting-chinas-economic-aggression/ (last accessed June 29, 2018).

[70] "Findings of the Investigation into China's Acts, Policies, and Practices related to Technology Transfer, Intellectual Property, and Innovation under Section 301 of the Trade Act of 1974," Office of the United States Trade Representative (March 22, 2018), available at: https://ustr.gov/sites/default/files/Section%20301%20FINAL.PDF (last accessed June 29, 2018).

[71] *Id.* at 153.

[72] *Id.* at 166.

[73] *Id.* at 168.

Chapter 4
Responding to Cyber Incidents

As discussed in Chapter 3, the Department's role in disrupting and preventing cyber threats not only embraces the traditional model of criminal law enforcement—which involves arresting suspected criminals and imprisoning offenders after they have been convicted—but also extends beyond that model to the use of non-criminal authorities and remedies.

In this chapter, we discuss other non-criminal, yet critically important, aspects of the Department's overall cyber mission: responding to, preventing, and managing cyber incidents.

Building Relationships and Sharing Cyber Threat Information

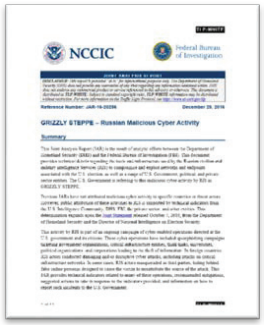
When responding to cyber incidents, preparation is key. Preparation will help victims of cyber attacks speed their response, lessen the effects of exploitation, and hasten recovery. In order to best assist potential victims of cyber threats, the Department needs to prepare, too. Our preparation efforts involve relationship building, routine information sharing, and engaging with organizations and sectors that are at particular risk. And when incidents do occur, open lines of communication enable reporting and facilitate response efforts.

1. Operational Engagement

In building relationships with potential victims of cyberattacks, the FBI employs "operational engagement"—that is, tailored and targeted outreach. Building trust is fundamental to this approach, which initially may seem difficult to achieve, given concerns about privacy, legal privileges, and the protection of sensitive information. To address these concerns, the FBI as a first step seeks to share its own information with industry, through a variety of outreach initiatives and information sharing programs.

The FBI disseminates numerous reports geared directly to the private sector regarding cyber threats. *See* **Fig. 1.** Common FBI-issued reports include Private Industry Notifications ("PINs"), which provide contextual information about ongoing or emerging cyber threats, and FBI Liaison Alert System ("FLASH") reports, which provide technical indicators gleaned through investigations or intelligence. These communication methods facilitate information sharing with either a broad or sector-specific audience, and provide recipients with actionable intelligence to protect against cyber threats and to detect ongoing exploitation. The FBI also often collaborates with other government agencies, including DHS, to release joint products, such as Joint Analysis Reports ("JARs") and Joint Technical Advisories ("JTAs").

Figure 1: FBI Product Lines



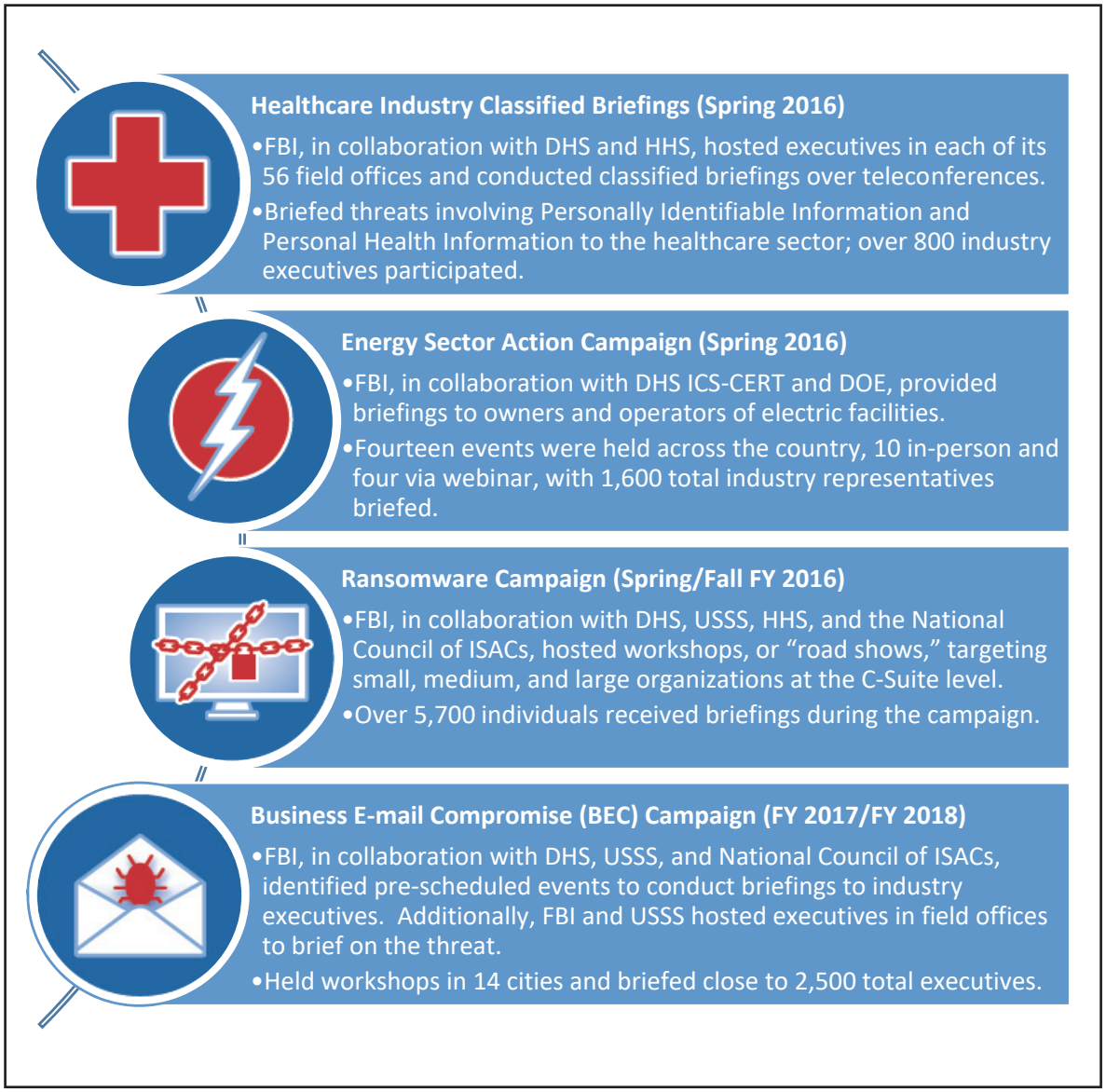
Product	**Private Industry Notification (PIN)**	**FBI Liaison Alert System (FLASH)**	**Public Service Announcement (PSA)**	**Joint Analysis Report/ Joint Technical Alert**
Author	FBI	FBI	FBI	FBI/DHS/Other Government Partners
Content	Provides contextual information about ongoing or emerging cyber threats	Provides technical indicators gleaned through investigations or intelligence	Provides information related to general cyber threats to the public	Provides technical details and indicators gleaned through joint analytic efforts.
Audience	Private Industry	Selected Partners/Target Industries	General Public	Private Industry

In certain circumstances, the FBI will join with sector-specific agencies[1] to execute an "action campaign" to quickly and efficiently advise a defined group of stakeholders of a particular cyber threat requiring their attention. *See* **Fig. 2.** These efforts serve a dual purpose of helping potentially targeted entities and advancing the FBI's cyber threat investigations.

The FBI also hosts targeted engagement events intended to bring together C-suite executives with government subject matter experts in order to build partnerships, encourage information sharing, and better understand the challenges the private sector faces in protecting against cyber threats.

In 2015, the FBI's Cyber Division began hosting a semi-annual Chief Information Security Officers ("CISO") Academy at the FBI Academy in Quantico, Virginia. The Academy seeks to enhance participants' understanding of the government and its functions by hosting approximately 30 CISOs representing key critical infrastructure sectors for a three-day training session. The event's sessions provide the latest information and intelligence on cyber threats, explain how the government interacts with private industry before, during, and after a cyberattack, explore investigative case studies, and engage participants in tabletop exercises. As of April 2018, the FBI had hosted four CISO Academies with over 120 total participants.

Figure 2: Recent FBI "action campaigns"



In addition, the FBI's Cyber Division, in collaboration with a host FBI field office and U.S. Attorney's Office, organizes one-day General Counsel Cyber Summits to bring corporate attorneys and CISOs together with Department personnel. At these summits, participants discuss how to overcome obstacles in information sharing and how best to work with the U.S. government when responding to a cyber incident. To date, the FBI has conducted four summits with over 500 total attendees.

2. *Enduring Partnerships*

The FBI has several established programs that enable connectivity, information sharing, and collaboration with the private sector on a range of hazards, including cyber threats. These programs include:

Domestic Security Alliance Council ("DSAC") was founded in 2006 as a national membership program to encourage public-private engagement between corporate chief security officers and the FBI on emerging threats facing the nation and economy. DHS was later added as a partner organization. With over 500 member companies, DSAC provides the FBI and DHS direct engagement with decision-makers in the U.S. economy's largest corporations and critical insight through the DSAC Executive Working Group.

InfraGard is a partnership between the FBI and members of the private sector for sharing information and promoting mutual learning relevant to the protection of the nation's critical infrastructure. In contrast to DSAC, InfraGard members join as individuals, not as corporations. There are over 50,000 vetted InfraGard members nationally, representing all critical infrastructure sectors, organized into 84 local chapters called "InfraGard Member Alliances." Each chapter is associated with its corresponding local FBI field office.

National Cyber-Forensics & Training Alliance ("NCFTA") was conceived in 1997 and the non-profit 501(c)(3) corporation was created in 2003. Headquartered in Pittsburgh, this organization has become an international model for joining law enforcement, private industry, and academia to build and share resources, strategic information, and cyber threat intelligence. Since its establishment, the NCFTA has evolved to keep up with the ever-changing cybercrime landscape. Today, the organization deals with threats from transnational criminal groups including spam, botnets, stock manipulation schemes, intellectual property theft, pharmaceutical fraud, telecommunication scams, and other financial fraud schemes that result in billions of dollars in losses to companies and consumers. The extensive knowledge base within the NCFTA has played a key role in some of the FBI's most significant cyber cases in the past several years.

National Domestic Communications Assistance Center ("NDCAC") is a national hub for technical knowledge management among law enforcement agencies that also strengthens law enforcement's relationships with the communications industry. Operated by the FBI's Operational Technology Division, the NDCAC leverages and shares law enforcement's collective technical knowledge and resources on issues involving real-time and stored communications to address challenges posed by advanced communications services and technologies. NDCAC develops and maintains relationships with industry to ensure law enforcement's understanding of new services and technologies, and it provides a venue to exchange information, streamline processes, and facilitate more efficient interaction between law enforcement and industry. NDCAC also educates industry on law enforcement's evidentiary processes and works with industry to verify that technical solutions work as expected.

Internet Crime Complaint Center ("IC3") provides the public with a reliable and convenient reporting mechanism to submit information to the FBI concerning suspected Internet-facilitated criminal activity and to develop effective alliances with law enforcement and industry partners. Since 2000, the IC3 has received complaints crossing the spectrum of cybercrime matters, to include online fraud in its many forms, including Intellectual Property Rights ("IPR") matters, computer intrusions, economic espionage, online extortion, identity theft and others. It is through this reporting that the program is able to analyze complaints for dissemination to the public, private industry, and for intelligence/investigative purposes for law enforcement.

3. *Reporting Cyber Incidents and Notifying Targeted Entities*

Through the numerous FBI and U.S. Attorneys' offices nationwide, the Department is uniquely positioned to interact with organizations that have experienced a cyber incident. The FBI has 56 field offices throughout the country, and has assisted victims of crime for over 100 years, including since the earliest days of computer crime. The FBI may learn through law enforcement or intelligence sources that a U.S. person or organization has suffered an incident or is the target of illicit cyber activity, and can proactively notify the targeted entity. Conversely, victims may be the first to detect the incident and then can notify the FBI. In either case, the Department stands ready to investigate the unauthorized activity and support victims.

Victim Notification

The Department identifies victims of cyber intrusion through a variety of means, such

as from the FBI's ongoing contact with victims, from investigations of threat actors, from other members of the U.S. Intelligence Community, and from foreign partners. This information may be highly classified or may carry special handling or sharing restrictions based on the sensitivity of the source and the information provided. The FBI takes all reasonable steps to identify the targeted individual or entity, determine if there was an actual compromise, and assess if there is actionable information it may share.

Depending upon the circumstances, the FBI can undertake direct or indirect notice to victims or potential victims. "Direct" notification is typically handled in-person through established liaison contacts, such as by notifying the representatives of an institutional victim. Larger scale data breaches involving thousands or millions of affected customers are more complicated. In such circumstances, the FBI relies on victimized institutions to provide notification to affected individuals. In those cases, the victimized institution may be better situated to notify its customers or members of a large-scale data breach.

Reporting Intrusions to the FBI

While law enforcement and intelligence agencies can sometimes uncover malicious cyber activity before a victim detects it on their networks, in other cases a targeted organization will be the first to detect anomalous activity. It is critically important to report incidents to law enforcement, as each incident potentially involves the commission of a federal crime and may warrant investigation. The FBI is uniquely positioned to investigate and attribute malicious cyber activity due to its dual criminal investigative and national security responsibilities.

While cyberattacks are typically conducted through technical means, behind the malicious activity is an actual individual or group perpetrating a crime. When the FBI is promptly notified, it can work to determine who caused the incident, link the incident to other incidents, maximize investigative opportunities, and potentially provide context regarding the actor, their tradecraft, and their motivations. Understanding who is targeting a victim's networks and for what purpose can inform defensive strategies and prevent future attacks. By notifying and assisting law enforcement, victims also help the FBI identify and pursue those responsible—which can help prevent future crimes against other victims. Such identification and pursuit is not limited to criminal response options. For example, attribution resulting from FBI investigative activities can support other U.S. government agencies' abilities to impose regulatory (e.g., sanctions), diplomatic, and technical costs upon those responsible for, or benefiting from, malicious cyber activities. Finally, notifying law enforcement may also place a victim company in a positive light with regulators, shareholders, and the public.

The Department encourages key organizations, particularly critical infrastructure owners and operators, to identify and form relationships with personnel in their local FBI field office, including through the partnerships detailed above, *before* an incident occurs. These pre-established relationships

and open lines of communication will speed reporting and response efforts.

The White House's Council of Economic Advisors recently observed that most data breaches are not reported to the U.S. government.[2] This reluctance may be driven by a fear of regulatory action, of reputational harm, or of an interruption to business operations. The reluctance of organizations and businesses to disclose that they have been attacked constitutes a major challenge for the U.S. government in its battle against cybercrime. Law enforcement cannot be effective without the cooperation of crime victims. A lack of cooperation may not only prevent discovery of evidence that could lead to identifying and holding the threat actors accountable, but also creates barriers to fully understanding the threat environment.

Responding to Cyber Incidents and Managing Crisis

1. Policy Framework

Presidential Policy Directive ("PPD")-41, titled "United States Cyber Incident Coordination," defines the term "cyber incident,"[3] and describes cyber incident response in terms of three concurrent and mutually beneficial lines of effort: **threat response** (investigation, attribution, and threat pursuit); **asset response** (remediation and recovery); and **intelligence support**. It also refers to a fourth, unnamed line of effort that is best described as **"business response"** (ensuring business continuity, addressing legal and regulatory issues, and external affairs). In the context of a nationally significant cyber incident, these activities are carried out in a coordinated way by the affected entity, by its third-party cybersecurity providers (if any), and by relevant federal agencies.

PPD-41 designates the Department of Justice, through the FBI and the National Cyber Investigative Joint Task Force ("NCIJTF"), as the lead federal agency for threat response activities in the context of a significant cyber incident. Through evidence collection, technical analysis, and related investigative tools, the FBI works to quickly identify the source of a cyber incident, connect that incident with related incidents, and determine attribution.

In addition to the cyber incident response framework laid out in PPD-41, the federal government also has adopted a Cyber Incident Severity Schema,[4] a rubric for describing an incident's significance and improving the federal government's response. An *incident of national significance* is rated as a Level 3 "High" (Orange), or greater. While the FBI does not allocate resources based exclusively on the schema rating, the rating serves as an enabler to various multi-agency coordination procedures and incident response efforts.

Both PPD-41 and the severity schema recognize that not all cyber incidents are "significant" from a national perspective. Thus, the scale and speed of a federal response will vary based on the facts and circumstances of particular cases. The FBI has capability, plans, and procedures to manage routine incidents. It also is prepared to react to circumstances

requiring a more robust approach. Responses to both types of incidents are discussed below.

2. Routine Incident Response

The FBI's nationwide reach puts it in an optimal position to engage with potential victims. The FBI's field-centric model also allows it to respond quickly, and in-person, to cyber incidents—often in a matter of hours.

Each FBI field office houses a multi-agency Cyber Task Force ("CTF") modeled after the FBI's successful Joint Terrorism Task Force program. The task forces bring together cyber investigators, prosecutors, intelligence analysts, computer scientists, and digital forensic technicians from various federal, State, and local agencies present within the office's territory. The CTFs not only serve as a force multiplier, but also provide a forum for coordination amongst local partners for more effective incident response. This model also allows the FBI to draw on the relationships, expertise, authorities, and tools of the task force members.

In addition to these cyber-specific resources, the FBI has other technical assets it can use as needed to combat cyber threats. The FBI's Operational Technology Division develops and maintains a wide range of sophisticated equipment, capabilities, and tools to support investigations and to assist with technical operations. While every FBI field office has a computer forensics laboratory, certain field offices host a larger Regional Computer Forensic Laboratory. These resources can be leveraged throughout the FBI's response and investigative cycle to respond to cyber threats.

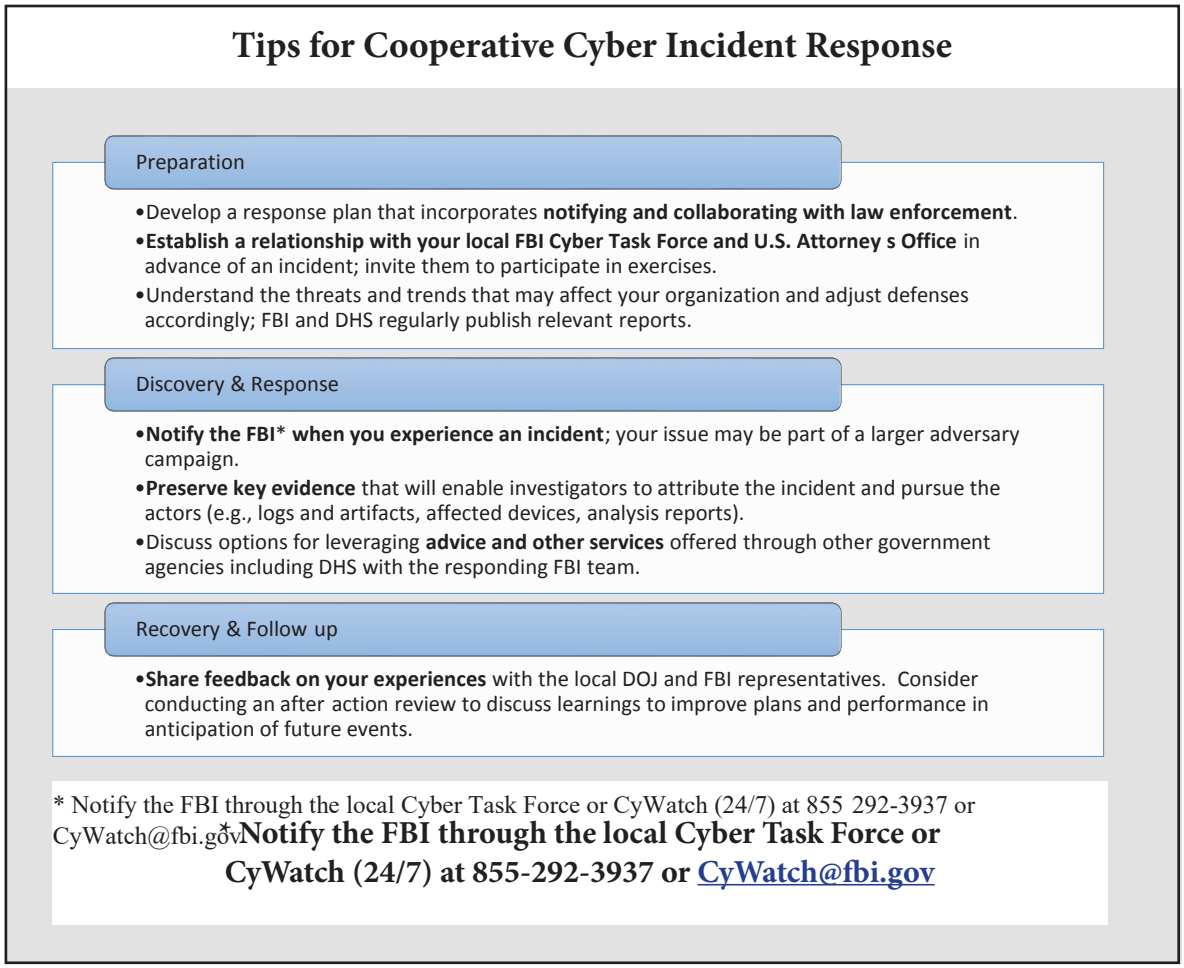
The FBI also has a strong international reach through a network of approximately 80 Legal Attaché offices throughout the world. It has supplemented 20 of these international offices with cyber-specific investigators to facilitate cooperation and information sharing to advance its cybercrime and national security investigations.

Because cyber threats and incidents occur around the clock, the FBI in 2014 established a steady-state, 24-hour watch capability called CyWatch. Housed at the NCIJTF, CyWatch is responsible for coordinating domestic law enforcement response to criminal and national security cyber intrusions, tracking victim notification, and partnering with the other federal cyber centers many times each day. CyWatch provides continuous connectivity to interagency partners to facilitate information sharing, and real-time incident management and tracking, as part of an effort to ensure that all relevant agencies are in communication.

3. Significant Incident Response

As directed by PPD-41, the FBI activates certain "enhanced coordination procedures" in the event of a "significant cyber incident."[5] These procedures include naming an accountable senior executive to manage the response and establishing a dedicated command center with a full array of communication capabilities.

Members of the local FBI Cyber Task Force will respond to the significant incident and a designated special agent will serve as the U.S. government's point of contact to the victim throughout the response. Nearby FBI field



offices can provide surge support and expertise as necessary, as each field office maintains personnel specifically trained on responding to incidents involving critical infrastructure and control systems. The response team may be further augmented by specialty support from FBI headquarters. For example, the FBI Cyber Action Team ("CAT") is the agency's elite rapid response force. On-call CAT members are prepared to deploy globally to bring their in-depth cyber intrusion expertise and specialized investigative skills to bear in response to significant cyber incidents. CAT's management and core team are based in the Washington, D.C. metro area and are supplemented by carefully selected and highly trained field personnel. The FBI also has technical analysis and operations units that directly support the response team through deep-dive malware analysis and digital forensics, and by implementing custom-built technical solutions to advance an investigation.

If a cyber incident generates physical impacts rising to the level of a crisis, the FBI has ex-

tensive crisis management capability. The FBI Crisis Management Unit coordinates the FBI's tactical and disaster relief efforts. The unit also provides the capability to activate command posts anywhere in the United States, and coordinates the FBI's vast investigative resources and infrastructure to support large-scale incidents regardless of type.

Finally, the FBI maintains a fleet of aircraft to support deployments when an immediate response is necessary, as well as command post vehicles to support on-scene operations.

Conclusion

The Department stands ready to assist victims of cyberattacks. By leveraging our field-centric model, investigative expertise, and partnerships at home and abroad, the Department works to pursue malicious cyber actors and to predict and prevent future attacks. We must continue to build trusting relationships and to work collaboratively to address the global cyber threat, and to impose costs on nation states, cybercriminals, and other malign cyber actors.

NOTES

[1] *See* "Sector Specific Agencies," U.S. Dept. of Homeland Security (July 11, 2017), available at: https://www.dhs.gov/sector-specific-agencies (last accessed June 29, 2018) (describing the "16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof," and listing the "Sector-Specific Agency" associated with each of these critical infrastructure sectors).

[2] "The Cost of Malicious Cyber Activity to the U.S. Economy," Council of Econ. Advisors, Exec. Office of the President, at 33 (Feb. 2018), available at: https://www.whitehouse.gov/wp-content/uploads/2018/02/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf (last accessed June 29, 2018).

[3] *See* "Presidential Policy Directive—United States Cyber Incident Coordination," The White House (July 26, 2016) ("PPD-41"), available at: https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident (last accessed June 29, 2018) (defining a "cyber incident" as "[a]n event occurring on or conducted through a computer network that actually or imminently jeopardizes the integrity, confidentiality, or availability of computers, information or communications systems or networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon. For purposes of [PPD-41], a cyber incident may include a vulnerability in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.").

[4] *See* "NCCIC Cyber Incident Scoring System," U.S. Computer Emergency Readiness Team, available at: https://www.us-cert.gov/NCCIC-Cyber-Incident-Scoring-System (last accessed June 29, 2018).

[5] A "significant" cyber incident is one "that is likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people." *See* PPD-41, *supra* note 3.

Chapter 5
Training and Managing Our Workforce

To appropriately identify, disrupt, dismantle, and deter computer intrusions and cyber-enabled crimes, the Department must develop and maintain a broad cadre of highly trained prosecutors, agents, and analysts. Whether identifying and locating cyber threat actors; collecting vital evidence through lawful process; or developing the latest tools to overcome sophisticated technologies criminals use to conceal their activities, Department personnel must understand how technology both facilitates criminal activity and can be used to detect, disrupt, and dismantle the same activity.

Investigators, for example, require advanced tools and resources to stay at least one step ahead of increasingly sophisticated anonymizing technologies that criminals and other adversaries exploit to avoid detection. Meanwhile, forensic analysts must possess the latest know-how to extract key evidence from sophisticated electronic media, such as encrypted cell phones and hard drives. Finally, prosecutors must tackle complex questions regarding legal authorities, jurisdiction, privacy, and other issues raised by investigating cybercrime and prosecuting those responsible for it.

The Department pursues two objectives in developing its workforce and specialized training initiatives. First, we seek to cultivate a multitude of attorneys who, in addition to superior legal skills, have the technological background and experience necessary to make appropriate decisions in technology cases. Second, we seek to retain a group of non-lawyer professionals whose primary expertise is technology. These computer scientists, engineers, and digital forensic investigators collaborate with attorneys and investigators, together forming a team with all necessary skills. Cultivating a workforce of technologically-savvy employees requires care in hiring and training, but also, crucially, requires that the Department make the right decisions about how it manages and organizes its employees.

How the Department internally organizes itself, and especially how it assigns cyber work, is a central part of the strategy to carry out its critical cyber mission and to recruit, train, and retain a technologically-expert workforce. In some respects, this challenge is not new. For example, prosecuting environmental crimes requires mastery both of a complex area of law and of relevant scientific facts; likewise, prosecuting antitrust and other complex business cases requires in-depth knowledge of how industries operate. The Department's solution to these challenges has been to build headquarters components and networks of attorneys and investigators that specialize in these technical areas of law enforcement. A similar strategy has worked well for cyber cases: the Department has concentrated its work of identifying, dismantling, disrupting, and

deterring computer intrusions and other cyber-enabled crimes into a select number of headquarters components and into networks of specialized attorneys and investigators. This method of organization yields at least three benefits for recruitment, training, and retention—which, in turn, benefits the investigation and prosecution of cyber cases.

First, despite ever-increasing competition in the technology job market, the Department can attract skilled prospects who are inspired by our mission. The Department now has employees who, in addition to being excellent lawyers or investigators, also have deep experience in network defense, computer forensics, and software engineering. These employees very often came to work at the Department precisely because they wanted to work on cyber cases. Offering prospective employees the chance to work exclusively (or near-exclusively) in the rewarding and challenging field of computer crime is a significant recruiting advantage. But making that promise is credible only if the Department can offer employment in specialized units, where cyber work has been concentrated.

Second, training employees in cyber cases requires far more than classroom instruction or reading from textbooks. Every seasoned attorney and investigator knows that the bulk of his or her expertise came from practical, on-the-job experience. Because the Department's specialized cyber units both at headquarters and in the field expose attorneys and investigators to cyber investigations, and do so repeatedly, they build skills and human capital much more effectively than if the work were dispersed indiscriminately around the Department.

Finally, the Department is constantly working to retain experienced attorneys and investigators in government employment. The skills of cyber investigators and attorneys are in heavy demand in the private sector, where salaries are much higher. The Department will lose this competition for talent if the only consideration is salary. Fortunately, that is not the only consideration for most employees. Only public service provides employees with so great an opportunity to protect and defend their country; in many ways, the work is itself a reward. To make maximum use of that reward, however, the Department's talented cyber workforce needs to be given regular opportunities to work on the cases and subject matter they feel most passionate about. Only an arrangement of specialized offices can offer that benefit.

In this spirit, the Department's criminal law enforcement entities, its United States Attorneys' Offices, and its relevant litigation divisions have dedicated workforce units and training initiatives that anchor the Department's broader strategy to recruit, train, and retain a technologically expert workforce in order to carry out its core cyber mission. These units and their specialized training initiatives are described below.

1. Federal Bureau of Investigation

As described in Chapter 4, the FBI is often a "first responder" to a cyber incident. With Cyber Task Forces located in each of its 56

field offices across the country, the FBI is prepared to respond to and investigate cyberattacks and intrusions wherever they may occur. Its agents serve both as investigators and high-tech specialists, capable of applying the most current technological know-how to collect evidence at the scene of a cyberattack or intrusion, analyze data forensically, and trace a cybercrime to its origins. Through its Cyber Division located at FBI headquarters in Washington, D.C., and the Operational Technology Division located at Quantico, Virginia, the FBI provides leadership to its global efforts to investigate cyber threats, whether they stem from criminal or national security actors. The Cyber Division has organized itself, both at headquarters and in FBI field offices, to focus its investigations and operations exclusively on computer intrusions and attacks, and related online threats.

The FBI is also responsible for the operation of the National Cyber Investigative Joint Task Force ("NCIJTF"), a multi-agency cyber center that serves as the national focal point for coordinating cyber investigations across government agencies. The NCIJTF is comprised of 30 plus partnering agencies from across law enforcement, the intelligence community, and the Department of Defense, with representatives who are co-located and work jointly to accomplish the organization's mission from a whole-of-government perspective. Members have access to and analyze data that provides a unique, comprehensive view of the Nation's cyber threat while working together in a collaborative environment in which they maintain the authorities and responsibilities of their home agencies. The NCIJTF coordinates, integrates, and shares cyber threat information to support investigations and operations for the intelligence community, law enforcement, military, policy makers, and trusted foreign partners in the fight against cyber threats. The NCIJTF is responsible for coordinating whole-of-government cyber campaigns, integrating domestic cyber data, and sharing domestic cyber threat information.

The FBI Criminal Investigative Division has created the Hi-Tech Organized Crime Unit ("HTOCU") to launch a long term, proactive strategy to target transnational organized crime groups using advanced technology to conduct large scale computer-enabled and computer-facilitated crime. HTOCU works to bring traditional organized crime techniques, tradecraft, and strategies to bear on transnational criminal enterprises that use high technology to perpetrate criminal activity. HTOCU, in coordination with the FBI's Cyber Division and the Money Laundering Unit, has developed and implemented strategies to dismantle transnational criminal enterprises engaged in large-scale fraudulent activity. Furthermore, HTOCU works to identify new sources, technical vulnerabilities, collection opportunities, and emerging trends in cyber-enabled transnational organized criminal activity.

The Joint Criminal Opioid Darknet Enforcement ("J-CODE") Team is a new FBI initiative, announced by Attorney General Sessions in January 2018, to target drug trafficking—especially fentanyl and other opioids—on the Dark Web. Building on the work that

began with the government's dismantling of Silk Road and AlphaBay, the FBI is bringing together agents, analysts, and professional staff with expertise in drugs, gangs, health care fraud and more, as well as federal, State, and local law enforcement partners from across the U.S. government, to focus on disrupting the sale of illegal drugs via the Dark Web and dismantling criminal enterprises that facilitate this trafficking. The J-CODE will create a formalized process to prioritize dark markets, vendors, and administrators for strategic targeting; to develop strategies to undermine confidence in the Dark Web; and to formulate de-confliction and operational requirements with other domestic and international partners.

In accordance with the requirements set forth in the Federal Cybersecurity Workforce Assessment Act of 2015, the Department, including the FBI, is identifying and coding federal positions that perform information technology, cybersecurity, and other cyber-related functions based on the work roles described in the National Initiative for Cybersecurity Education Framework.[1] This analysis will underpin an effort to prioritize areas of critical need within the workforce, and support possible recommendations for introducing new job roles that will improve the FBI's ability to respond to Internet-enabled crimes and technologically advanced threat actors.

With respect to training, the FBI has a number of programs to ensure its workforce possesses the key cyber skills and tools to succeed in their investigations, especially as the technological landscape rapidly evolves. For instance, the FBI is implementing the "Cyber Certified" training and certification program for investigators, intelligence analysts, technical specialists, and attorneys, whether currently in the Cyber Program or working in other mission areas. These employees will be observed for future training and development activities.

In an attempt to rapidly increase the level of cyber knowledge shared throughout the organization, and in an effort to infuse cyber knowledge into traditionally non-cyber programs, the FBI has also created the Workforce Training Initiative ("WTI"). The WTI is designed to increase the number of employees who are capable of responding to, investigating, and analyzing a variety of cyber-related cross-programmatic matters, and its courses cover the breadth of cyber-related topics.

The On the Job Training ("OJT") initiative is a combination of classes and real world experiences encountered daily on a cyber squad. The OJT program takes place over a six-month period and requires a full-time commitment from participants. The participants are reassigned to a cyber squad and are expected to work cyber cases under the mentorship of cyber-skilled professionals. At the conclusion of the six-month program, participants return to their original squads with enhanced cyber skills to address cyber threats within that program and to share their knowledge. Upon completion of this program, participants will be designated Cyber Certified.

The FBI Digital Forensics program offers digital evidence related training and certifications to personnel dedicated to managing digital evidence challenges, and also offers technical training to the broader FBI workforce which familiarizes them with the challenges of properly preserving and handling digital evidence. The Forensic Examiner certification program includes over ten weeks of total training, practical exercises, mentorship, and a moot court which includes Department attorneys and senior examiners.

The FBI's Cyber Executive Certification Program provides high-level cyber training and prepares executives for their role in the cyber investigation process. Participants have the opportunity to obtain two industry standard certifications, in addition to the internal FBI certificate. Additionally, the digital evidence program offers advanced training to personnel supervisors of digital evidence workforce, preparing them to ensure the technical requirements of FBI investigation are met by the digital evidence staff.

Finally, FBI-led cyber training takes place at Cyber Academy campuses located at different points in the country, while digital evidence training occurs at Regional Computer Forensics Laboratories, and at FBI headquarters. Cyber training ranges from the Cyber Basic School, a two-week curriculum designed to instill cybersecurity fundamentals in all employees, to advanced training for seasoned cyber investigators. Digital evidence training includes guidance in analysis of Windows, Macintosh, UNIX, and mobile operating systems, Internet artifacts, secure device access, vehicle forensics, and Internet of Things related challenges.

2. The Criminal Division

Computer Crime and Intellectual Property Section

In 1996, the Department consolidated the Criminal Division's expertise in computer crime matters into a single office called the Computer Crime and Intellectual Property Section ("CCIPS"), with prosecutors devoted to pursuing computer crime prosecutions fulltime. Over the years, CCIPS's mission has grown beyond prosecution to include spearheading cyber policy and legislative initiatives, training and support, public outreach, and cybersecurity guidance. CCIPS consists of a team of specially trained attorneys dedicated to investigating and prosecuting high-tech crimes and violations of intellectual property laws, and to advising on legal issues concerning the lawful collection of electronic evidence.

Today, CCIPS is responsible for implementing the Department's national strategies to combat computer and intellectual property crimes worldwide by working with other Department components and government agencies, the private sector, academic institutions, and foreign counterparts, among others. Section attorneys work to improve the domestic and international legal, technological, and operational legal infrastructure to pursue network criminals most effective-

ly. Working in support of and alongside the 94 U.S. Attorneys' Offices ("USAOs"), CCIPS prosecutes violations of federal law involving computer intrusions and attacks. CCIPS has also worked with the Treasury Department's Office of Foreign Asset Control to use new authorities under Executive Order 13694 to bring sanctions against foreign nationals for malicious cyber-enabled criminal activities. In conjunction with the Executive Office for United States Attorneys ("EOUSA"), described below, CCIPS conducts at least four multi-day in-person trainings and up to twelve webinars a year. It also maintains an internal website with information available to all Department components that is visited more than 90,000 times a year, and has a rotating daily duty-attorney system that responds to approximately 2,000 calls for advice a year.

In addition, the Criminal Division established the Computer Hacking and Intellectual Property ("CHIP") coordinator program in 1995 to ensure that each USAO and litigating division has at least one prosecutor who is specially trained on cyber threats, electronic evidence collection, and technological trends that criminals exploit. The CHIP network now includes approximately 270 prosecutors from USAOs and Main Justice, and aids in the coordination of multi-district prosecutions involving cyber threats. Specialized CHIP units exist in 25 designated USAOs. CHIP Assistant U.S. Attorneys (AUSAs) work with law enforcement partners from multiple law enforcement agencies at the outset of an investigation, often in consultation with CCIPS, to provide legal guidance, help craft an investigative plan, obtain necessary search warrants and court orders, collect electronic evidence, and ultimately, build a criminal case. Pursuant to departmental regulation, U.S. Attorneys are responsible for ensuring that experienced and technically-qualified AUSAs serve as the district's CHIP prosecutors; ensuring that CHIP resources are dedicated to CHIP program objectives; ensuring that the USAO notifies, consults, and coordinates with CCIPS and other USAOs; and promoting and ensuring effective interaction with law enforcement, industry representatives, and the public in matters relating to computer and intellectual property crime.

Money Laundering and Asset Recovery Section

The Criminal Division's Money Laundering and Asset Recovery Section ("MLARS") leads the Department's asset forfeiture and anti-money laundering enforcement efforts. MLARS is responsible for, among other things, coordinating complex, sensitive, multi-district, and international money laundering and asset forfeiture investigations and cases; providing legal and policy assistance and training to federal, State, and local prosecutors and law enforcement personnel; and assisting Departmental and interagency policymakers by developing and reviewing legislative, regulatory, and policy initiatives.

With respect to cyber-enabled threats in particular, MLARS has established a Digital Currency Initiative that focuses on providing support and guidance to investigators, prosecutors, and other government agencies on cryptocurrency prosecutions and forfei-

tures. The Digital Currency Initiative will expand and implement cryptocurrency-related training to encourage and enable more investigators, prosecutors, and Department components to pursue such cases, while developing and disseminating policy guidance on various aspects of cryptocurrency, including seizure and forfeiture. Through the Initiative, MLARS will also advise AUSAs and federal agents on complex questions of law related to cryptocurrency to inform charging decisions and other prosecutorial strategies.

Office of Enforcement Operations, Electronic Surveillance Unit

Electronic surveillance is one of the most effective law enforcement tools for investigating many types of criminal enterprises, including cyber-based criminal enterprises that use electronic media and Internet-based technologies to perpetrate their crimes. The Electronic Surveillance Unit ("ESU") in the Criminal Division's Office of Enforcement Operations is responsible for reviewing all federal requests to conduct interceptions of wire, electronic, or oral communications pursuant to the Wiretap Act. ESU's specialized attorneys provide suggested revisions and offer guidance to ensure that electronic surveillance applications meet all constitutional, statutory, and Department policy requirements. Every federal wiretap application must be approved by a senior Department of Justice official before it is submitted to a court, and ESU makes recommendations to those officials based on its review. Additionally, ESU attorneys regularly conduct webinars and in-person trainings, and provide legal advice to federal prosecutors and law enforcement agencies on the use of electronic surveillance. They also assist in developing Department policy on emerging technology and telecommunications issues.

Office of International Affairs

The Criminal Division's Office of International Affairs ("OIA") returns fugitives to face justice, and obtains essential evidence for criminal investigations and prosecutions worldwide by working with domestic partners and foreign counterparts to facilitate the cooperation necessary to enforce the law, advance public safety, and achieve justice. Drawing upon a vast network of international agreements and its expertise in extradition and mutual legal assistance, OIA in recent years has worked with domestic and foreign law enforcement to hold cybercriminals accountable in U.S. courts and obtain the evidence needed to untangle complex transnational cybercrime schemes.

In addition to its work supporting investigations and prosecutions of cybercriminals, OIA uses mutual legal assistance to obtain electronic evidence for foreign and domestic law enforcement personnel. As the need to obtain electronic evidence in virtually every type of criminal case has burgeoned, OIA has worked to modernize its practice in this area by creating a team of attorneys and support personnel specially trained in obtaining electronic evidence, and by implementing process efficiencies to ensure swift attention to requests from prosecutors and police. OIA is also actively engaged in the policy, legislative, and multilateral arenas in which topics concerning access to electronic evi-

dence and law enforcement cooperation are discussed and debated to ensure that the Department's mission is advanced and that our law enforcement personnel get the tools they need to keep pace with ever-evolving threats. Consistent with these goals, OIA conducts regular training for U.S. prosecutors on the tools available to them to obtain evidence located overseas and to secure the return of fugitives. OIA also provides frequent regional and bilateral trainings to our foreign partners to bolster their ability to stop criminal activity before it reaches our shores.

3. The National Security Division

The investigation, disruption, and deterrence of national security cyber threats are among the highest priorities of the Department's National Security Division ("NSD"). These priorities come from a recognition that network defense alone is not enough to counter the threat. To the contrary, we must also impose costs on our adversaries using all of the U.S. government's lawfully available tools. This "all-tools" approach informs NSD's efforts to combat cyber threats to our national security, with the goal of deterring and disrupting cyber-based intrusions and attacks. In this context, national security cyber cases are those perpetrated by nation states, terrorists, or their agents or proxies, or cases involving the targeting of information that is controlled for national security purposes.

All NSD attorneys must take a cyber course within two years of joining the division. NSD also conducts annually a one-day cyber training in-house for all NSD employees, which is taught by NSD and CCIPS attorneys.

In addition, in 2012, NSD launched the National Security Cyber Specialist ("NSCS") network to equip USAOs around the Nation with prosecutors trained on national security cyber threats, such as nation-state cyber espionage activities and terrorists' use of technology to plot attacks. NSCS-Main is comprised of lawyers and other experts drawn from NSD's component sections and offices, as well as from CCIPS and ESU in the Criminal Division. NSCS-Main also coordinates as needed with other Department headquarters components, including the Civil Division, the Antitrust Division, the Office of Legal Policy, and the Office of Legal Counsel, and works closely with the Department's investigative components, including the FBI.

The NSCS Network also includes AUSAs in each of the USAOs; these AUSAs serve as their offices' primary points of entry for cases involving cyber threats to the national security and coordinate closely with NSCS-Main. NSD and CCIPS, in conjunction with EOUSA, provides annual training for NSCS members. The NSCS training covers a number of national security cyber topics to enhance the education of the prosecutors who handle these matters. In addition, through the National Security/Anti-Terrorism Advisory Council, there are approximately seven training courses conducted annually for national security prosecutors. Those trainings generally include a number of cyber-related sessions for national security prosecutors.

Finally, this year, for the first time, NSD is offering a Cyber Fellowship for those selected attorneys who applied to further their education on technology-related issues. Five attorneys were selected to participate in 2018 and have been attending a series of trainings offered by the FBI, the CIA, Carnegie Mellon University, and the SANS Institute. Those selected have also agreed to assist with training and other cyber initiatives at NSD.

4. United States Attorney's Offices / Executive Office for United States Attorneys

The United States Attorneys serve as the nation's principal litigators, under the direction of the Attorney General. There are 93 United States Attorneys stationed throughout the United States, Puerto Rico, the Virgin Islands, Guam, and the Northern Mariana Islands.[2] Each United States Attorney is the chief federal law enforcement officer of the United States within his or her particular jurisdiction. United States Attorneys conduct most of the trial work in which the United States is a party. Although the distribution of caseloads varies between districts, each USAO deals with every category of cases, including cybercrime prosecutions. As referenced above, the role of the CHIP AUSA was established to ensure that each USAO has personnel trained on cyber threats, electronic evidence collection, and technological trends exploited by criminals. Similarly, the NSCS program discussed above was designed to equip USAOs around the nation with prosecutors specially trained on national security cyber threats, such as nation state cyber espionage activities and terrorists' use of technology to plan attacks. The USAOs also coordinate as needed with Department headquarters components, such as the Criminal and National Security Divisions, in a further effort to ensure the effectiveness of such cyber-oriented investigations and prosecutions.

EOUSA provides executive and administrative support for the 93 United States Attorneys. Such support includes legal education, administrative oversight, technical support, and the creation of uniform policies, among other responsibilities.

The National Advocacy Center, which EOUSA operates, provides numerous courses every year addressing a wide variety of cyber-related topics. These courses are attended by prosecutors from across the country and are tailored to address the training needs of attorneys with varying levels of experience handling cyber matters. Working with CCIPS and the National Security Division's Counterterrorism and Counterespionage sections, these cybercrime courses range from introductory to advanced level and have included training addressing the nature of computer forensics, the investigation of computer intrusions, and the use of electronic evidence, among other related topics. In short, each year, the Department trains hundreds of federal prosecutors in cybercrime and national security cyber matters.

In addition to these in-person training programs, EOUSA, through the Office of Legal and Victim Programs and the Office of Legal Education ("OLE"), sponsors additional cyber training, including webinars that are

broadcast nationwide. These webinars allow the Department to provide supplemental cutting-edge training and allow prosecutors to view these presentations from their own offices, while still enabling them to remotely ask the presenters questions and download related materials. For example, EOUSA sponsored a webinar discussing new provisions of a Federal Rule of Evidence relating to electronic evidence, immediately after those provisions became effective. Almost 1,000 Department employees viewed that program. Working closely with CCIPS and OEO, additional notable webinars have included programs addressing legal standards for obtaining cell phone location information, searching and seizing computers and other digital devices, cryptocurrency, and social media and online investigations, to name just a few.

OLE, working with CCIPS, has also issued standalone written materials that prosecutors can use for training and law enforcement purposes.

5. Drug Enforcement Administration

The DEA enforces the Nation's controlled substance laws and regulations. Through its participation in J-CODE and beyond, DEA is developing its expertise in Dark Market investigations. DEA's Operational Support Unit ("STSO") serves as the point of contact between DEA offices and the technology and communications industry, in order to identify, address, and resolve subpoena and related compliance issues, as well as other legal and regulatory issues. STSO also disseminates to the field guidance relating to these issues. STSO is attempting to bring DEA employees into a more advanced awareness of today's cyber world, so they can adapt to that environment while performing the daily tasks of Internet research and investigations.

6. INTERPOL

The mission of INTERPOL Washington (United States National Central Bureau), is to advance the law enforcement interests of the United States as the official representative to the International Criminal Police Organization (INTERPOL); to share criminal justice, humanitarian, and public safety information between our Nation's law enforcement community and its foreign counterparts; and to facilitate transnational investigative efforts that enhance the safety and security of our Nation.

INTERPOL Washington leverages a network of 192 countries connected by a secure communications platform to share information for the purpose of enhancing international cooperation in all areas of criminal investigation, including cybercrime investigations. INTERPOL Washington maintains an office dedicated to advancing the cybercrime investigations of U.S. law enforcement by establishing and maintaining relationships with the heads of cybercrime units of other countries; sharing information through the secure communications platform to assist cybercrime investigations conducted by the agencies of the Department of Justice and the Department of Homeland Security; and

providing support to other federal, State, local, and tribal law enforcement agencies.

7. Foreign Government Training Initiatives

In addition to training its own personnel, the Department also provides training and technical assistance to foreign governments to ensure that they are equipped to address their own domestic cyber threats. As countries develop their own capacity to address cyber issues, they are also better equipped to assist the United States in investigations involving criminal conduct emanating from within their own borders. The Department has maintained a robust program for encouraging foreign governments to develop their criminal and procedural laws to address emerging cybercrime threats and capabilities, consistent with the Budapest Convention on Cybercrime. As discussed in Chapter 3, the Budapest Convention—which the United States ratified over ten years ago—provides a legal framework for criminalizing key types of cybercrime, developing the tools necessary to investigate such crime, and establishing the network for rapid international cooperation that must exist to investigate and prosecute cyber actors wherever they are located.

Using a balanced approach of frank policy discussions with countries that have technical capabilities similar to our own, combined with multilateral training initiatives aimed at countries whose legal infrastructure for addressing cyber threats is in earlier stages of development, the Department has continued to improve the capacity of other countries to address cyber threats around the world, thereby also increasing our own capacity to thwart cyber threats.

8. Department-Wide Cybersecurity Awareness Training

In addition to the specialized units and training described above, the Department recognizes that cybersecurity effectiveness depends on everyone in the organization. Users are still one of the most attacked entities in the organization. Social engineering attacks (described in more detail in Chapter 2) come in many forms, are still effective, and can target anyone in the Department. As such, all Department employees must have a basic understanding of their responsibilities when handling the Department's information and accessing its information system, while being held accountable for abusing those responsibilities.

All Department personnel receive annual cybersecurity awareness training. In addition, all employees and contractors must sign the "Department of Justice Cybersecurity and Privacy Rules of Behavior (ROB) for General Users" agreement, which confirms that the employee or contractor completed the training and understands the applicable cybersecurity requirements and responsibilities. As the agreement makes clear, "each [Department] user is responsible for the security and privacy of [Department] information systems and their data."

Adequate training ensures that everyone within the Department has a basic understanding of the relevant threats, their role in protecting our information and information

systems, and how to detect and respond to cybersecurity events. Typical web-based training is most common; however, many training delivery mechanisms are used to get the broadest penetration of the material. For example, phishing exercises are conducted throughout the year, and in-person briefings and topic-specific training sessions are offered for special audiences and material.

Finally, the Department has also hosted a number of Department-wide trainings and awareness campaigns to educate the Department's workforce on privacy and cybersecurity. The Office of Privacy and Civil Liberties organizes an annual Privacy Forum, which gathers the Department's privacy officials to discuss current privacy and civil liberties issues. In addition, the Department's Office of the Chief Information Officer hosts an annual Cybersecurity Symposium, which provides a forum for employees to gain an understanding of the latest trends in cybersecurity from federal and industry leaders. These events help educate the Department's workforce on the most current trends in information security and privacy.

While the Department employs a robust training program, we can do more to carry the Department into the future. Training can reinforce best practices, enable advanced threat detection, and improve security and safety across the Department as we all work to carry out its critical cyber mission.

NOTES

[1] *See* National Institute for Standards and Technology, Special Publication 800-181, *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework* (Aug. 2017), available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf (last accessed June 29, 2018).

[2] One United States Attorney is assigned to each of the 94 judicial districts, with the exception of Guam and the Northern Mariana Islands, where a single United States Attorney serves in both districts.

Chapter 6
Looking Ahead

This report describes the most significant cyber threats our Nation faces, and catalogs the ways in which the Department confronts and combats those threats. As the discussion in previous chapters reveals, the Department has had many successes. At the same time, we face a number of challenges.

In this chapter, we further explore those challenges and identify specific areas for additional inquiry. We also outline eight key areas of future effort that will define the Department's work in the months ahead.

Specific Challenges

Each part of the Department's efforts to confront cyber threats—(1) preventing and responding to cyber incidents (Chapter 4); (2) investigating and prosecuting cyber-related crimes (Chapter 2); and (3) dismantling, disrupting, and detering malicious cyber threats (Chapter 3)—bears its own unique challenges.[1]

Here, we describe those challenges and, where applicable, discuss how the Department has begun addressing the challenge or what actions we may yet take to sharpen our efforts. Where appropriate, we also highlight issues that require further consideration and development due to the complex or evolving nature of the threat.

1. Challenges in Preventing and Responding to Cyber Incidents

Working with the Private Sector

Virtually every instance of cyber-related crime implicates the private sector in some way, whether the private sector is the target of malicious cyber activity, the provider of technology or services through which cybercrimes are committed or concealed, or the repository of evidence (such as communications) relating to cyber-enabled criminal activity. As such, the relationship that the Department, including the FBI, builds and maintains with the private sector is critical to our efforts to combat cybercrime. Fortunately, the Department and the private sector already have engaged in numerous formal and informal collaborations. Even so, the Department must deepen these relationships, particularly as technology evolves and the cast of service providers and technology manufacturers continues to change.

a. The Computer Security Research Community

The computer security research community—which is comprised of not only computer security companies but also individuals and organizations with expertise in computer security—has made valuable contributions to combating cyber threats by discovering

significant exploitable vulnerabilities affecting, among other things, the confidentiality of data, the safety of Internet-connected devices, and the security of automobiles. Some security researchers have also been allies in law enforcement efforts to dismantle cyber threats. For example, assistance with malware analysis and mitigation techniques has helped law enforcement conduct operations against various cybercriminals, including through botnet takedowns.

Even so, some in the computer security research community harbor concerns that law enforcement may misconstrue as criminal activity their methods of searching for and analyzing vulnerabilities. Some researchers have even expressed anxiety that such concerns have chilled legitimate security research.

To ensure the Department maintains and fosters a positive, collaborative working relationship with computer security researchers, the Department should consider potential legal options to encourage and protect legitimate computer security research. For instance, a three-year exemption to the Digital Millennium Copyright Act ("DMCA")[2]—the result of rulemaking by the U.S. Copyright Office[3]—has allowed researchers to conduct vulnerability research on consumer products, including Internet of Things ("IoT") devices. IoT devices are prime targets of cybercriminals for use in illicit activities like distributed denial of service attacks. Finding and repairing vulnerabilities in consumer devices is important and will likely become even more important as IoT devices proliferate, perform more household tasks, and collect more data capable of being monetized by criminals.

The Copyright Office has initiated its next rulemaking process to evaluate extending the DMCA exemptions. The Department has submitted input to the Copyright Office in support of extending and expanding the current security research exemption, with caveats intended to protect public safety and avoid confusion over legal research activities.[4] At the same time, the Department should continue evaluating existing laws and regulations to identify other opportunities to support and encourage legitimate computer security research. Finally, the Criminal Division's Cybersecurity Unit should conduct additional outreach to the computer security community. In doing so, the Unit should seek out opportunities to: (1) explain how the Department's policies and practices address concerns about unwarranted prosecutions for legitimate security research; and (2) better educate the computer security research community about the federal criminal laws implicated by computer security activities.

b. Encouraging Private Sector Reporting of Cyber Incidents

Another important component of the Department's collaboration with the private sector is the public-private work on information sharing and threat assessment. As discussed in Chapter 4, the FBI disseminates numerous reports directly to members of

the private sector to inform them of cyber threats. This information sharing provides the private sector with actionable intelligence that enables them to take appropriate precautions.

Information sharing, however, is most effective when it flows two ways. When a private sector entity reports a breach or attempted intrusion, the Department gains valuable insights into threat activity that can help direct, in real time, law enforcement efforts to investigate and disrupt the malicious activity. Prompt reporting also provides information that officials can accumulate and share with other private sector entities to facilitate appropriate security measures. Indeed, efforts by the Department and FBI to help manage cyber incidents and, later, to bring perpetrators to justice through prosecution are best accomplished when the victim—who may be the first to discover an incident—reports the incident or intrusion in a timely manner.

Unfortunately, many cyber incidents in the United States are never reported to law enforcement. Victims—especially businesses—often decide not to report cyber incidents for a variety of reasons, including concerns about publicity and potential harm to the company's reputation or profits, and even concerns of retaliation by a nation state where they wish to do business. Some victims may simply not know how to report the incident to appropriate authorities. And still others, particularly larger companies, may try to act on their own to pursue, confront, or disrupt the perpetrator, though doing so may trigger civil or even criminal liability, or may impact U.S. foreign relations. Regardless of the reason, lack of reporting is a significant impediment to the Department's efforts to thwart cybercriminals and to address threats to national security—particularly when new threats are emerging.

Encouraging reporting from private sector victims is thus critical to enhancing the Department's ability to prevent, deter, investigate, and prosecute (or otherwise disrupt) cybercrimes. To facilitate reporting, the Department should consider not only how to build deeper trust with the private sector, but also understand and address the private sector's needs and concerns related to reporting. This assessment should include understanding how best to incentivize reporting as well as how to eliminate obstacles or barriers. The Department should also continue its outreach to the private sector to identify additional areas for collaboration, especially with respect to reporting and information sharing. In the past, such outreach has resulted in industry-targeted guidance such as the Criminal Division Cybersecurity Unit's *Best Practices for Victim Reporting and Responding to Cyber Incidents*.[5]

The Department must also consider the role that DHS and other government agencies play in working with the private sector to ensure federal agencies' efforts are complementary and cooperative. In addition to DHS and other federal partners, the Department should continue to work with the agencies that regulate the private sector to evaluate

expectations and encourage clear thresholds for reporting.

The Department's additional efforts on private sector reporting should also include attention to statutory data breach notification requirements. Currently, all 50 States have enacted separate notification laws setting standards governing notification by private entities when a data breach occurs, but there is no federal reporting requirement or standard. As such, companies must navigate and comply with the varying requirements in 50 State jurisdictions.[6] In the wake of recent high-profile data breaches exposing Americans' personal information, Congress has a revived interest in national notification requirements. A national data breach standard could increase federal law enforcement's effectiveness to pursue hackers and prevent data breaches.

c. Reviewing Guidance on Victim Notification

In 2012, the Attorney General issued General Guidelines for Victim and Witness Assistance ("AG Victim Guidelines" or "guidelines") that, among other things, discussed two statutes—the Victims' Rights and Restitution Act, 42 U.S.C. § 10607, and the Crime Victims' Rights Act, 18 U.S.C. § 3771—which accord certain rights to individuals who meet the statutory definition of "victim." The AG Victim Guidelines also address when FBI notification to victims and witnesses is appropriate and warranted. Given the evolving nature of cyber-enabled crimes—including the fact that it is not always easy to identify a cybercrime "victim" or the extent or nature of the harm—the Department should review the AG Victim Guidelines to ensure, among other things, that the guidelines, and any related victim notification policies and practices, appropriately account for the unique and often nuanced nature of cybercrime.

Preventing Cyber-Related Vulnerabilities in Connection with Foreign Investment and Supply Chains

As part of its efforts to prevent cybercrime, the Department is concerned with mitigating vulnerabilities that threaten national security. Such areas concern foreign investment in domestic assets and foreign supply chains.

For example, a March 22, 2018 Presidential Memorandum observed that "China directs and facilitates the systematic investment in, and acquisition of, U.S. companies and assets by Chinese companies to obtain cutting-edge technologies and intellectual property and to generate large-scale technology transfer in industries deemed important by Chinese government industrial plans."[7] Under ambitious industrial policies, China aims to use foreign investment as a means of dominating cutting-edge technologies like advanced microchips, artificial intelligence, and electric cars, among others.

Currently, the Department responds to threats posed by foreign investment in the United States and the export of sensitive technology by enforcing U.S. export controls and through the Committee on Foreign Investment in the United States ("CFIUS"), a statutorily-established body that has au-

thority to review transactions that could result in control of a U.S. business by a foreign person. As the March 22, 2018 Presidential Memorandum indicates, further coordination through CFIUS, enforcement of existing technology transfer controls, and other interagency efforts will be necessary to tackle risks from foreign investment in sensitive industries and technologies.

In addition to foreign investment, the Department is generally concerned with hardening supply chains. Technology supply chains are especially vulnerable, because the hardware components and software code that go into technology products often come from foreign sources, including developers in Russia and China.[8] To address these concerns, the Department coordinates with other government agencies and the private sector to effectively manage and mitigate cybersecurity risks in U.S. supply chains.

For example, the Department contributes to Team Telecom, an ad hoc interagency working group that considers the law enforcement, national security, and public safety implications of applications for licenses from the Federal Communications Commission involving a threshold percentage of foreign ownership or control. Moving forward, the Department should continue to engage with these and other interagency efforts to determine the best ways to strengthen defenses against national security risks.

2. Challenges in Investigating and Prosecuting Computer Crime

Accessing Data in the United States

Data not only is key to understanding the nature of cybercrime and the identity of perpetrators, but also is a primary source of evidence for prosecution. Unfortunately, the relevant data is often hard to reach, hidden on computers in different States or even in countries half a world away, lurking on dark markets, or protected by anonymized host servers or encryption. Recognizing that accessing data is the starting point and often the cornerstone of computer crime investigations and prosecutions, the Department has made concerted efforts to improve its ability to collect data related to criminal activity. However, several challenges to accessing data remain and require further collaboration with federal, State, and private sector partners.

One such challenge is the reality that cybercrime often does not take place in one identifiable, physical location. Sophisticated cybercriminals can control botnets spread throughout several States or countries and can hide their illegal activities on proxy networks. The rules governing law enforcement efforts, however, have largely not kept pace with these criminal realities. For this reason, the Department proactively engaged with the Federal Rules Committee and on December 1, 2016, an amended version of Rule 41 of the Federal Rules of Criminal Procedure went into effect. (That new Rule is discussed in detail in Chapter 3.)

The circumstances that the amendments to Rule 41 address are important, but they do not cover all instances where data related to criminal activity are stored in varying or unknown locations within the United States. The Department should identify any additional common or recurring circumstances where current legal authorities fall short of providing law enforcement with the tools necessary to access relevant data within the United States and determine whether changes similar to the recent Rule 41 amendments would be effective.

Accessing Data Abroad

The Department faces similar challenges in accessing data located outside the United States. As with the Rule 41 amendments in the domestic context, the Department recently engaged with partners to enhance our investigative authority in such circumstances. In particular, as the result of a joint effort between the private sector and the Department to bring clarity to investigative demands for data stored overseas, the Clarifying Lawful Overseas Use of Data Act ("CLOUD Act") became law on March 23, 2018. (The CLOUD Act is also discussed in Chapter 3.)

Passage of the CLOUD Act institutes a framework for technology companies to comply with investigative demands for data stored outside of the requesting country's territory, and creates processes to resolve thorny conflict of laws problems. The Act clarifies that the U.S. government's traditional authority in this area remains in force: communications service providers must disclose information subject to a court order that is within their "possession, custody, or control," even if the electronic servers containing that information are located overseas. The CLOUD Act also authorizes our government to enter into formal agreements with other nations that remove legal barriers that would otherwise create conflict of laws problems where a provider is subject to a foreign court order to produce data stored in that other country. The Act requires both governments to "certify" that the laws and practices of the other country provide adequate protections for human rights and personal privacy. The agreements must also implement transparency measures and periodic reviews to ensure ongoing compliance. The Department is currently considering how it should implement such agreements.

Challenges remain, however, when investigating computer crimes that extend overseas, particularly because the CLOUD Act addresses only those instances where the relevant overseas data is possessed or controlled by an entity subject to U.S. jurisdiction. Many types of evidence fall outside those criteria, and traditional mutual legal assistance treaty ("MLAT") procedures may also fall short.

For those reasons, the Department continually aims to improve its international outreach efforts and to engage with international Internet governance bodies to encourage them not to apply rules that unreasonably restrict or interfere with valid investigations. For example, the Department is currently monitoring and assessing the impact of the European Union's sweeping General Data

Protection Regulation ("GDPR"), which went into effect on May 25, 2018.

Broadly speaking, the GDPR regulates how private companies and governments process, store, and transfer data concerning E.U. residents, including how such data and information is handled and transferred into and out of the E.U. Violators could be subject to fines up to 4% of their gross revenue worldwide or 20 million Euros, whichever is greater, creating a serious financial incentive for covered entities not to violate the new regulation. Exceptions written into the GDPR should ensure that it does not affect the ability of U.S. law enforcement to obtain evidence through MLATs. Also, law enforcement-to-law enforcement sharing is covered by a separate directive and is thus outside of the scope of the GDPR. Still, significant questions and uncertainties exist about the GDPR, which could negatively affect law enforcement, including by impeding information sharing.

For example, some interpret the GDPR to require that the publicly-available WHOIS system remove information about the registrants of Internet domain names from public access, thereby necessitating the building and maintenance of secured law enforcement portals to access that information. As described in Chapter 3, prosecutors and law enforcement agencies around the world use the WHOIS system thousands of times a day to investigate crimes ranging from botnets to online fraud. The registrant data in WHOIS can create crucial leads to targets' identities, locations, and other pieces of their criminal infrastructure. This data can also help identify additional victims. Due to the significant risk associated with noncompliance with the GDPR, however, the private organization responsible for maintaining WHOIS has decided to remove much of the registrant data from the publicly-available segments of the system while the organization works with stakeholders, including the Department, to develop a GDPR-compliant system.

This is only one example of how the GDPR may be interpreted to impede the ability of law enforcement authorities to obtain data critical for their authorized criminal and civil law enforcement activities. Uncertainty about the GDPR also has placed in question not only voluntary disclosures of information about criminal activity—*e.g.*, by their employees, contractors, or customers—to U.S. law enforcement agencies, but also may cause companies with a significant E.U. presence to become reluctant to comply even with disclosures required by legal process, such as warrants and subpoenas, for fear that such a disclosure would be in violation of the GDPR. Absent official guidance, companies with significant E.U. business may become reluctant to participate in mandatory data transfers to U.S. law enforcement and regulatory authorities, which would impede effective tax collection, limit the ability of agencies to stop anti-competitive business practices, impair the work of public health and safety agencies, and undermine the integrity of global banking, securities, and commodities markets. This could also undercut the Department's mitigation programs for businesses and individuals that wish to cooperate in areas such as fraud, bribery, money laundering, sanctions violations, and antitrust matters—programs that yield information

that often results in criminal referrals, and thus relate to the Department's core mission.

In short, given the uncertainty that the GDPR presents in certain key areas, the Department (as well as the U.S. government as a whole) must continue to collaborate with European authorities and stakeholders to carefully monitor the GDPR's impacts.

The "Going Dark" Problem

One of the most significant challenges to the Department's ability to access investigative data is the "Going Dark" problem. "Going Dark" describes circumstances where the government is unable to obtain critical information in an intelligible and usable form (or at all), despite having a court order authorizing the government's access to that information. The problem impacts a range of issues, including data retention;[9] anonymization; provider compliance (or absence thereof); foreign-stored data; data localization laws; tool development and perishability; and other similar issues. The challenges posed by the Going Dark issue have achieved greatest prominence in the context of encryption.

These challenges have significantly grown in recent years as the sophistication of encryption has increased. In the past, only the most sophisticated criminals encrypted their communications and data storage; today the average consumer has access to better technology than sophisticated criminals had twenty years ago. Previously, providers used encryption of some sort but generally retained a way of accessing the unencrypted data if necessary or desired, including to comply with law enforcement search warrants or wiretap orders. In the past several years, the Department has seen the proliferation of default encryption where the only person who can access the unencrypted information is the end user. The advent of such widespread and increasingly sophisticated encryption technologies that prevent lawful access poses a significant impediment to the investigation of most types of criminal activity, including violent crime, drug trafficking, child exploitation, cybercrime, money laundering (including through cryptocurrencies), and domestic and international terrorism.

Faced with the challenges posed by encrypted information, investigative agencies have sometimes looked to other sources of information and evidence, which can be costly to procure and maintain. While these efforts have occasionally been successful, evidence and information lost to encryption often cannot be replaced solely by pursuing other sources of evidence. For example, communications metadata, such as non-content information about who contacts whom in phone records, can be helpful in putting the pieces together, but it provides less information than the content of data and communications—a difference that can prove outcome-determinative in the context of a criminal investigation, where prosecutors must prove guilt beyond a reasonable doubt. Moreover, metadata is also often simply unavailable because there is no mandate for providers to be able to access it. Relatedly, in the context of a judicial order authorizing the real-time interception of communications, the court must find, by law, that alternate sources of data do not exist or are insufficient to meet the investigation's goals.

Going Dark

Warrant-proof encryption poses a serious challenge to effective law enforcement.

"To those of us charged with the protection of public safety and national security, encryption technology and its application…will become a matter of life and death which will directly impact our safety and freedoms."

– FBI Director Louis Freeh
July 9, 1997

1997

"We have engaged the tech community aggressively to help solve this problem. You cannot take an absolutist view on this. So if your argument is strong encryption, no matter what, and we can and should, in fact, create black boxes, then that I think does not strike the kind of balance that we have lived with for 200, 300 years."

– President Barack Obama
March 11, 2016

2016

"While convinced of the problem, I'm open to all constructive solutions, solutions that take the public safety issue seriously. We need a thoughtful and sensible approach, one that may vary across business models and technologies, but . . . we need to work fast."

– FBI Director Christopher Wray
March 7, 2018

2018

"To be very clear — the [U.K.] government supports strong encryption and has no intention of banning end-to-end encryption. But **the inability to gain access to encrypted data in specific and targeted instances is right now severely limiting our agencies' ability to stop terrorist attacks and bring criminals to justice."**

– U.K. Home Secretary Amber Rudd
August 1, 2017

"Few issues have vexed law enforcement agencies more than this one. They can't get access to the data they need to stop crime and hold criminals to account. **95 per cent of [our intelligence organization's] most dangerous counter-terrorism targets actively use encrypted messages to conceal their communications.** We need access to digital networks and devices, and to the data on them, when there are reasonable grounds to do so. These powers must extend beyond traditional interception if our agencies are to remain effective and pre-empt and hold to account criminal activity. There will also need to be obligations on industry – telecommunications and technology service providers – to cooperate with agencies to get access to that data . . . . "

– Australian Minister for Law Enforcement & Cybersecurity Angus Taylor
June 6, 2018

Exploiting software vulnerabilities can be another way to access encrypted (or otherwise inaccessible) data on a phone or other device. The Department has, in some instances, lawfully exploited security flaws to access electronic data, including data stored on smartphones. This is a promising technique, and the Department should expand its use in criminal investigations. However, so-called "engineered access" is not a replacement for all the evidence, including evidence subject to a court order, that is lost. Moreover, expanding the government's exploitation of vulnerabilities for law enforcement purposes will likely require significantly higher expenditures—and in the end it may not be a scalable solution. All vulnerabilities have a limited lifespan and may have a limited scope of applicability. Software developers may discover and fix vulnerabilities in the normal course of business, or the government's use of a vulnerability could alert developers to its existence. Finally, each vulnerability might have very limited applications—limited, for example, to a particular combination of phone model and operating system.

"Responsible encryption is achievable. Responsible encryption can involve effective, secure encryption that allows access only with judicial authorization. Such encryption already exists. Examples include the central management of security keys and operating system updates…"

—Deputy Attorney General Rod Rosenstein, October 10, 2017

The challenges posed by the Going Dark problem are among law enforcement's most vexing. To address these challenges, the Department's efforts should include: (1) considering whether legislation to address encryption (and all related service provider access) challenges should be pursued; (2) coordinating with international law enforcement counterparts to better understand the international legal, operational, and technical challenges of encryption; (3) collecting accurate metrics and case examples that demonstrate the scope and impact of the problem; (4) working to use technical tools more robustly in criminal investigations; (5) insisting that providers comply with their legal obligations to produce all information in their possession called for by compulsory process, and holding them accountable when they do not; (6) working with State and local partners to understand the challenge from their perspective and to assist them technologically in significant cases; and (7) reaching out to academics, industry, and technologists to fully understand the implications and possibilities for lawful access solutions.

Additional Investigative Authorities

The Department has identified at least two additional legal authorities it needs to support cyber-related investigations. First, exceptions to the court order requirements of the Pen Register statute, 18 U.S.C. § 3121, are unnecessarily narrow. That statute governs the real-time collection of non-content "dialing, routing, addressing, or signaling information" associated with wire or electronic communications. This information includes phone numbers dialed as well as the "to" and "from" fields of e-mail. In general, the statute requires a court order authorizing collection of such information on a prospective basis unless the collection falls within a statutory exception. The exceptions to the Pen Register statute, however, are not coextensive with the exceptions to the Wiretap Act, codified at 18 U.S.C. § 2511 *et seq*, which generally governs wiretaps to obtain the content of wire or electronic communications. This results in the illogical situation where non-content information associated with a communication is subject to more extensive protection than the content of the communication itself. Moreover, the Pen Register statute's consent provision could be clarified to allow users to provide direct, express consent for implementation of a pen/trap device by the government to facilitate cooperative investigation efforts. The Department stands ready to assist Congress in developing legislation to implement this needed improvement.

Second, the Department faces similar problems in obtaining electronic communication transactional records ("ECTRs")—the e-mail equivalent of toll billing records for telephone calls[10]—in national security investigations. ECTRs do not include the content of communications, but they can provide crucial evidence early in national security investigations, when investigators do not yet have a clear indication of a subject's network of contacts. Information obtained from ECTRs, such as e-mail addresses, can help establish the probable cause necessary to get a Foreign Intelligence Surveillance Act order or search warrant to allow the FBI to obtain the content of stored communications, identify a potential confidential human source who may be able to provide valuable intelligence, or help eliminate a subject from suspicion. As electronic networks increasingly have supplanted telephone networks as the means for terrorists and foreign agents to communicate, the ability to access these records efficiently has become even more important to the FBI's work.

Under 18 U.S.C. § 2709, electronic communication service providers are obliged to provide ECTRs in response to certain requests—sometimes called National Security Letters ("NSLs")—made in connection with qualifying national security investigations. Companies, however, have invoked an omission in section 2709 to refuse to provide ECTRs in response to NSLs. The statute states in paragraph (a) that wire or electronic communication service providers have a duty to provide ECTRs in response to a request made by the Director of the FBI under paragraph (b). But paragraph (b) fails expressly to include ECTRs in the categories of information the Director may request, even though paragraph (a) explicitly references ECTRs.

Clarifying the statutory authority would strengthen the Department's ability to conduct counterintelligence investigations and to identify and disrupt terrorist plots in the United States. Law enforcement has obtained equivalent telephone records with a simple subpoena for decades, and the courts have held that non-content metadata of this kind, held by third-party service providers, is not protected by the Fourth Amendment.[11] A proposal to clarify that the FBI may obtain ECTRs by issuing NSLs would reaffirm a similar type of authority to the equivalent type of electronic communications information.

Apprehending Criminals Located Abroad

Even when accessible data allows law enforcement to understand the nature of the crime, to identify potential perpetrators, and to build a case for prosecution, holding the guilty party or parties accountable can still be a challenge. While the Department has made several advances to enhance its ability to prosecute sophisticated cybercriminals, difficulties apprehending criminal suspects, as well as the need for additional prosecutorial authorities, continue to hinder our efforts to bring malicious cyber actors to justice.

For example, as with our successful effort to amend Rule 41, the Department worked with the Federal Rules Committee to tackle the problem of serving criminal defendants accused of committing computer crimes. Rule 4 governs the service of criminal process upon individuals and organizations—essentially the process by which prosecutors give notice of charges to, and initiate court proceedings against, a criminal defendant. Prior to the amendment, Rule 4 did not explicitly provide a method to serve process on an organization with no physical presence in the United States, an artifact of the pre-cyber era when organizations could hardly commit crimes in the United States without having a physical presence here. As discussed in Chapters 2 and 3, today, technology allows foreign actors to commit intellectual property and computer crimes in the United States from virtually anywhere in the world.

Rule 4, amended as of December 1, 2016, now provides prosecutors with a "non-exhaustive list of methods" for serving "an organization not within a judicial district of the United States." Most importantly, the amended Rule 4 allows the government to serve a foreign organization "by any . . . means that gives notice." For example, the government has relied on the amended Rule 4 to serve foreign organizations by mailing and e-mailing process to the foreign organization's U.S.-based defense counsel. The government has also served foreign organizations by mailing process to the registered agent for a recently dissolved U.S. subsidiary of the foreign organization or, in another case, by personally serving process on the president of a U.S. organization that shared a common "parent" organization with the subject of the summons. This change is particularly important in situations where a state-owned enterprise is charged with a crime but the foreign jurisdiction is unwilling to assist with efforts to serve process.

Service, however, is only one facet of the problem that the Department faces in at-

tempting to hold sophisticated cybercriminals accountable. As noted throughout this report, attributing a cyber-incident to an individual or group of actors is difficult due to anonymizing technologies and encryption techniques that allow cybercriminals to remain hidden from law enforcement. Additionally, there are cybercriminals who, though identified, manage to remain beyond the reach of U.S. law enforcement, especially when they are located abroad. While the Department has several mechanisms to bring cybercriminals to the United States to face trial, including extradition treaties and collaborative relationships with other countries (*see* Chapter 3), these efforts are not always successful. Some foreign sovereigns choose not to cooperate or will do so only after imposing unreasonable limitations on law enforcement. Other countries may not punish perpetrators for the specific computer crime the United States is seeking to prosecute or may lack sophisticated domestic cybercrime law enforcement capabilities. In addition to continuing to build strong relationships with other countries and assisting their efforts to meet the requirements to join the Budapest Convention (also discussed in Chapter 3), the Department should continue to identify necessary additional authorities and potential mechanisms for bringing foreign-based cybercriminals to justice.

Additional Criminal Prohibitions

Once malicious cyber actors are identified, it is important for the Department to have the authorities necessary to prosecute those individuals for the illicit activity. Additional criminal prohibitions would help the Department prosecute and deter malicious cyber activity.

a. Protecting Election Computers from Attack

The principal statute used to prosecute hackers—the Computer Fraud and Abuse Act ("CFAA")—currently does not prohibit the act of hacking a voting machine in many common situations. In general, the CFAA only prohibits hacking computers that are connected to the Internet (or that meet other narrow criteria for protection). In many conceivable situations, electronic voting machines will not meet those criteria, as they are typically kept off the Internet. Consequently, should hacking of a voting machine occur, the government would not, in many conceivable circumstances, be able to use the CFAA to prosecute the hackers. (The conduct could, however, potentially violate other criminal statutes.)

*b. Insider Threat/*Nosal *Fix*

Until recently, the Department regularly used the CFAA's prohibition on "exceeding authorized access" to prosecute insider threats—in particular, employees who abused permitted access to their employers' systems by stealing proprietary information or accessing information for their own illicit purposes and gain. The Department, for example, prosecuted police officers who sold their access to confidential criminal records databases, government employees who accessed private tax and passport records without authority, and bank employees who abused access to steal customers' identities. These employees had

some right to access those computers, but their conduct was a crime under the CFAA because they intentionally exceeded their employer's computer use rules.

Decisions in the Second, Fourth, and Ninth Circuit Courts of Appeals, however, have limited the definition of "exceeds authorized access" in section 1030(e)(6) of the CFAA. In *United States* v. *Nosal*, 676 F.3d 854 (9th Cir. 2012) (en banc), the Ninth Circuit held that an indictment did not state a violation of the CFAA when it alleged that a former employee had asked current employees to access information in a proprietary database to aid him in starting a new firm. The company had computer policies that limited employee access to legitimate work purposes. Although the employees' efforts to access information for the benefit of the former employee's new firm violated the company's policies, the court held such an activity did not violate federal criminal law. According to the *Nosal* court, the definition of "exceeds authorized access" in section 1030(e)(6) "is limited to violations of restrictions on access to information, and not restrictions on its use." *Id*. at 863-64.[12]

Such decisions have caused grave damage to the government's ability to prosecute and protect against serious insider threats. If the CFAA can be used only against outsiders with no right at all to access computers, many insider threats—including those in the intelligence and law enforcement communities with access to extremely sensitive information—may go unpunished. Prosecutors should have adequate statutory authority to pursue insiders who abuse their computer access for illicit means. Any such authority should also ensure appropriate consideration and treatment of legitimate privacy-related concerns.

c. CFAA as RICO Predicate

As discussed in Chapter 3, the Racketeer Influenced and Corrupt Organizations Act ("RICO") is an important prosecutorial tool for charging organizations engaged in a pattern of criminal activity because RICO violations carry substantial sentencing penalties as well as the ability for the government to seize assets of the criminal organization. RICO requires proof of, among other things, a pattern of "racketeering activity," which is defined as violations of two or more qualifying predicate criminal acts.

Currently, computer fraud under the CFAA does not qualify as a predicate act under the RICO statute, whereas similar conduct, such as wire fraud and mail fraud, does qualify. Adding the CFAA as a predicate offense for RICO purposes could increase our ability to fight cybercrime and take down criminal organizations engaged in such activities.

d. Combating Sextortion

"Sextortion" and related offenses are discussed in Chapter 2. Although such conduct may implicate certain existing criminal laws, there are no federal criminal statutes specifically addressing sextortion and non-consensual pornography. Additionally, while stalking, bullying, and harassment have more commonly been dealt with by local law enforcement or outside the criminal justice

system, the use of computers and mobile networks has turned many such crimes into multi-jurisdictional and even multi-national offenses.[13] The increasingly expansive nature of these crimes, in addition to the use of new technologies, may merit a federal response. New federal criminal offenses specifically targeting sextortion and non-consensual pornography, as well as possible new sentencing enhancements for such offenses under existing authorities, could have merit.

3. Challenges in Connection with Other Legal Actions to Dismantling, Disrupting, and Deterring Malicious Cyber Conduct

As described in Chapter 3, in addition to traditional investigation and prosecution, the Department has an array of other techniques and tools to dismantle, disrupt, and deter cyber threats, including a blend of civil, criminal, and administrative powers. The Department has employed these tools to disable botnets, disrupt dark markets, and pursue sanctions against specified malicious actors. As with our investigation and prosecution activities, however, the Department needs additional tools and authorities to maximize effectiveness.

Tackling Tor/Dark Markets

The Department cannot disrupt cyber activity that it cannot find. This makes Tor and the existence of dark markets one of the greatest impediments to our efforts. As discussed in detail in Chapter 2, Tor provides anonymity in two ways—first, by anonymizing communications sent from computers running Tor, and second, by allowing individuals to operate websites on the Dark Web called Tor "Hidden Services" without divulging location information of the websites' servers.

While sometimes used for innocuous and even beneficial purposes, the anonymity afforded by Tor also poses a unique and significant threat to public safety. The anonymizing technology is effective, making it difficult to identify the physical location of dark market websites either to shut them down or to identify who is administering them. The result is that law enforcement investigators can observe and document the fact that disturbing criminal activity is occurring, but they cannot use the sort of investigative steps that ordinarily would allow them to determine who is perpetrating the crimes.

Combating criminals' abuse of Tor and their exploitation of dark markets requires a concerted effort. The Department should work with partners to develop new technological tools that will enable law enforcement to identify the true location of Hidden Services websites engaged in criminal activity. Effective development and use of these tools will enable law enforcement to locate and lawfully seize servers hosting such sites, and to identify the administrators, vendors, buyers, and participants who use them. In addition, the federal government should carefully evaluate its role in funding these anonymizing technologies, as currently the U.S. government is the primary source of funding for the Tor Project, the organization responsible for maintaining the Tor software.

Enhancing Our Ability to Disrupt Botnets

On May 22, 2018, DHS and the Department of Commerce released a joint report titled, "A Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats."[14] The report encourages collaboration between the government and private industry, recognizing that addressing the global botnet problem requires further discussions on market incentives and on securing products at all stages of their life cycle. The Department should play an active role in these efforts.

Despite being the principal law enforcement agency tasked with disrupting and dismantling botnets, the Department's current statutory authority is limited. As it stands today, the law gives federal courts the authority to issue injunctions to stop the ongoing commission of specified fraud crimes or illegal wiretapping through the use of botnets, by authorizing actions that prevent a continuing and substantial injury. The Department used this authority effectively in its successful disruption of the Coreflood botnet in 2011 and of the Gameover Zeus botnet in 2014. *See* Appendix 2. Because the criminals behind these particular botnets used them to intercept communications containing online financial account information and, with that information, committed fraud, the existing law allowed us to obtain court authority to disrupt the botnets by stopping the criminals' commands from reaching the infected computers.

Unfortunately, botnets can be and often are used for many other types of illegal activity beyond fraud or illegal wiretapping. As explained in Chapter 2, for example, malicious actors can employ botnets to steal sensitive corporate information, to harvest e-mail account addresses, to hack other computers, or to execute DDoS attacks against websites or other computers. When these crimes do not involve fraud or illegal wiretapping, courts may lack the statutory authority to issue an injunction to disrupt the botnet. The Department should evaluate the merits of creating a more comprehensive authority for courts to address all types of illegal botnets.

Advancing a CFAA Forfeiture Fix

As discussed in Chapter 3, the Department in recent years has regularly used civil forfeiture authorities to disrupt cybercriminal groups by seizing valuable assets such as computer servers and domain names used to operate botnets, as well as profits derived from illegal activity.[15] These actions are permissible even when it is not yet possible to arrest the offenders. Expanding forfeiture authority to CFAA offences could enhance the Department's capacity to dismantle, disrupt, and deter cyber threats by targeting the instruments of, and profits from, cybercrime.

Issues for Further Evaluation

In addition to helping facilitate action on the specific recommendations made above and elsewhere in this report, the Department should initiate a deeper evaluation of several key areas where strategic coordination is

especially important. Some of these evaluations are already underway; others will be part of the Department's ongoing efforts to evaluate its authorities, practices, and resources.

The eight non-exclusive areas for deeper evaluation include:

1. Strengthening Our Own Defenses: Consistent with the President's May 2017 Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure,[16] the Department is continually reassessing how best to defend its networks and reduce vulnerabilities. The Department should consider next steps and a longer-term strategy to maintain the security of its own defenses.

2. Enhancing Effective Collaboration with the Private Sector: The Department's ability to work collaboratively and effectively with the private sector will continue to be one of the most critical elements of our strategy to fight cybercrime. In the coming months, the Department should engage in a more extensive evaluation of our work with the private sector by seeking specific input from private sector participants. Where appropriate, we will make recommendations to enhance these collaborative efforts, including with regard to information-sharing, threat and incident notification, data breach notification standards, and frameworks for joint disruptive efforts, such as botnet takedowns.

3. Addressing Encryption and Anonymity (the Going Dark Array of Issues): Addressing the complex issues raised by the legal and technical barriers that prevent law enforcement from obtaining information in electronic form is another Department priority. As discussed above, it is critical that the Department maintain the ability to identify those who employ technology for illicit means and, with appropriate legal authority, to obtain evidence to bring criminals to justice. The Department should continue to develop a framework to ensure that these public safety and national security objectives can be met even as encryption and anonymizing technologies continue to evolve. In addition, the Department should explore and, as appropriate, adopt new investigative methods to replace the investigative opportunities that have been lost.

4. Addressing Malign Foreign Influence Operations: As discussed in Chapter 1, hostile foreign actors exploit the Internet and social media platforms to conduct influence operations against our Nation, including by spreading disinformation and propaganda online on a scale greater than has ever been observed before. In addition to implementing the disclosure policy discussed in Chapter 1, the Department should consider additional ways to improve our ability to respond to malign foreign influence operations, including whether new criminal statutes aimed directly at this threat are needed, and whether there are new ways we can work with the private sector in this area. Because this problem requires a whole-of-government solution, the Department should also consider how best to use existing or additional interagency coordination mechanisms to address the threat.

5. Addressing the Global Nature of Cyber-Enabled Crime: A hallmark of technology-enabled crime is that it increasingly cuts across international boundaries, even when less sophisticated actors are behind the malicious activity. As discussed above, the global nature of cybercrime carries with it numerous impediments—both technological and arising out of foreign laws and international agreements—to the Department's ability to identify and locate malicious actors and bring them to justice. These impediments bear no easy solutions and may only grow as technology continues to evolve. The Department should continue evaluating this set of challenges and make additional recommendations to improve its global investigative and prosecutorial reach.

6. Preparing for Emerging and Future Technology: The technology behind current cyber-enabled threats will continue to evolve. The Department must ensure that its continued recalibration of efforts and resources not only aims at the major threats of today, but also prepares it for the emerging threats of tomorrow. The Department should continue to evaluate how its investigative and prosecutorial abilities can keep pace with, and even stay ahead of, the evolving technological threat. For example, the Department should continue evaluating the emerging threats posed by rapidly developing cryptocurrencies that malicious cyber actors often use, and autonomous vehicle technology, which has both ground and aerial applications (*e.g.*, unmanned aircraft systems).

7. Sharpening Departmental and Interagency Organization of Efforts to Fight Cyber-Enabled Crime: The Department's cyber-related mission requires effort and expertise from many components. Similarly, the Department's efforts make up just one part of the U.S. government's approach to cyber issues. As such, the Department must continuously review its internal coordination approach and resources, as well as how it interacts with its interagency partners, to determine if any improvements or adjustments are needed. Relatedly, the Department should continue evaluating how most effectively to recruit and retain attorneys, investigators, and professional staff with the necessary skills and mission-oriented mindset to ensure it has the human capital it needs to confront evolving cyber threats.

8. Strengthening the Department's Tools and Authorities: This report has described numerous additional recommendations to strengthen the Department's tools and authorities. Where such improvements are already known, the Department should seek ways to advance those improvements, including by seeking interagency approval to advocate for legislation, where appropriate.

In each of these key areas, the Department should not be merely reactive to known challenges and obstacles, but rather should pursue a strategic and forward-looking approach.

NOTES

[1] Challenges specific to foreign influence operations are discussed in detail in Chapter 1 and so are not repeated here.

[2] The Digital Millennium Copyright Act, codified at 17 U.S.C. § 1201, prohibits the circumvention of technological controls, such as encryption and password protocols, that protect copyrighted works. Section 1201 also includes a rulemaking process that recognizes that, in some cases, exceptions to the general prohibition may be justified. Section 1201 requires the Copyright Office to conduct a rulemaking every three years to evaluate proposed exemptions proposed by the public to the anti-circumvention provision and to recommend appropriate proposals for adoption by the Librarian of Congress. The exemptions last only three years unless they are renewed in a subsequent proceeding.

[3] The last rulemaking process conducted in 2016 resulted, *inter alia*, in a three-year exemption for "security research" conducted on particular categories of devices, including machines designed for use by individual consumers, motorized land vehicles, and certain medical devices. Security research included "good faith testing for and the identification, disclosure and correction of malfunctions, security flaws and vulnerabilities in computer programs." *See generally* U.S. Copyright Office, "Section 1201 Rulemaking: Sixth Triennial Proceeding to Determine Exemptions to the Prohibition on Circumvention," (Oct. 2015), available at: https://www.copyright.gov/1201/2015/registers-recommendation.pdf (last accessed June 29, 2018).

[4] *See* John T. Lynch, Jr., Chief, Department of Justice Computer Crime and Intellectual Property Section, to Regan Smith, General Counsel and Associate Register of Copyrights, Library of Congress (June 28, 2018), available at: https://www.justice.gov/criminal-ccips/page/file/1075496/download (last accessed June 29, 2018). To date, the Department is unaware of any claims that the current security research exemption has thwarted or interfered with criminal investigations or prosecutions.

[5] Available at: https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/04/30/04272015reporting-cyber-incidents-final.pdf (last accessed June 29, 2018).

[6] *See* "Alabama Rolls with Tide as Last State to Adapt Breach Notification Law," Taft Stettinius & Hollister LLP (Apr. 30, 2018), available at: https://www.lexology.com/library/detail.aspx?g=cc0e9bb3-fe24-4211-b9dc-1fbfd350637f (last accessed June 29, 2018).

[7] "Presidential Memorandum on the Actions by the United States Related to the Section 301 Investigation," The White House (March 22, 2018), available at: https://www.whitehouse.gov/presidential-actions/presidential-memorandum-actions-united-states-related-section-301-investigation/ (last accessed June 29, 2018).

[8] For example, due to such concerns, DHS in September 2017 issued a directive requiring federal agencies to remove and discontinue use of antivirus software provided by Moscow-based Kaspersky Lab. Several months later, Congress enacted a government-wide ban on Kaspersky products and services that exceeded the scope of the DHS prohibition. Both measures came in response to growing national security concerns presented by the presence of Kaspersky products on U.S. information systems. Kaspersky challenged both measures in court, and both suits

were dismissed at the pleading stage. Litigation continues in the court of appeals. Also in 2017, Congress amended 10 U.S.C. § 491 to restrict Department of Defense procurement of certain telecommunications equipment or services with particular Chinese or Russian origins.

[9] Accessing data is further complicated in some circumstances by the lack of any uniform data retention standards or requirements for service providers. Without such requirements, data that is potentially critical to law enforcement investigations is simply not retained or in some cases is not retained long enough to be useful.

[10] Telephone toll billing records include the originating phone number, the phone number called, and the date, time, and length of the call. ECTRs for e-mail show the sending e-mail address, the e-mail recipients, and the date, time, and size of the e-mail message.

[11] *See, e.g.*, *United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008) (holding that e-mail and Internet users have no reasonable expectation of privacy in to/from addresses of their messages or in IP addresses of websites visited).

[12] *See also WEC Carolina Energy Solutions LLC v. Miller*, 687 F.3d 199, 207 (4th Cir. 2012) ("[W]e reject an interpretation of the CFAA that imposes liability on employees who violate a use policy[.]"); *United States v. Valle,* 807 F.3d 508 511 (2d Cir. 2015) (an individual "'exceeds authorized access' only when he obtains or alters information that he does not have authorization to access for any purpose which is located on a computer that he is otherwise authorized to access").

[13] For instance, a criminal in one State can easily disseminate graphic images and personally-identifying information of his victim in another State or around the world. He can store the images and information on servers in unfriendly foreign jurisdictions, using proxy technology to conceal his true location. He can threaten and extort the victim using end-to-end encrypted communication applications that store little or no information about subscribers. Without leaving home, the perpetrator can commit an elaborate and hard-to-trace scheme using technology easily accessible to anyone. Worse, someone with no technical sophistication at all can hire someone to do the harassment for him from a dark market online.

[14] "A Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats," U.S. Dept. of Commerce & U.S. Dept. of Homeland Security (May 22, 2018), available at: https://www.commerce.gov/sites/commerce.gov/files/media/files/2018/eo_13800_botnet_report_-_finalv2.pdf (last accessed June 29, 2018).

[15] 18 U.S.C. §§ 981-83.

[16] Exec. Order No. 13,800, 82 Fed. Reg. 22391 (May 16, 2017).

Office of the Attorney General
Washington, D. C. 20530

February 16, 2018

MEMORANDUM FOR HEADS OF DEPARTMENT COMPONENTS

FROM: THE ATTORNEY GENERAL

SUBJECT: Cyber-Digital Task Force

The malicious use of technology poses an unprecedented threat against our nation. While computers, smart devices, and other chip-enabled machines—as well as the networks that connect them—have enriched our lives and have driven our economy, the malign use of these technologies harms our government, victimizes consumers and businesses, and endangers public safety and national security. Indeed, the scale of this cyber threat, and the range of actors that use cyber intrusions and attacks to achieve their objectives, have grown in alarming ways.

The Department of Justice remains committed to confronting cyber threats by detecting, deterring, and disrupting malicious cyber activity through the enforcement of federal law. Therefore, today, I am establishing the Department's Cyber-Digital Task Force (the Task Force). This Task Force not only will canvass the many ways that the Department already combats the global cyber threat, but also will identify how federal law enforcement can more effectively accomplish its mission in this vital and evolving area.

The Task Force shall be chaired by a senior Department official appointed by the Deputy Attorney General and shall consist of representatives from the Criminal Division; the National Security Division; the United States Attorney's Office community; the Office of Legal Policy; the Office of Privacy and Civil Liberties; the Office of the Chief Information Officer; the Bureau of Alcohol, Tobacco, Firearms and Explosives; the Drug Enforcement Administration; the Federal Bureau of Investigation; and the United States Marshals Service. The Deputy Attorney General may invite representatives from other Department components, and from other federal agencies, to participate in the Task Force as appropriate, and may establish subcommittees to focus the Task Force's efforts.

Many of the most pressing cyber threats that our nation faces transcend easy categorization. These threats include: efforts to interfere with, or disable, our critical infrastructure; efforts to interfere with our elections; use of the Internet to spread violent ideologies and to recruit followers; theft of corporate, governmental, and private information on a mass scale; use of technology to avoid or frustrate law enforcement, or to mask criminal activity; and the mass exploitation of computers, along with the weaponizing of everyday consumer devices (as well as of the very architecture of the Internet itself) to launch attacks on American citizens and businesses. Evaluating these threats, and formulating a strategy to combat them, should be among the Task Force's highest priorities.

I have asked for an initial report from the Task Force describing the Department's current cyber-related activities and offering initial recommendations by no later than June 30, 2018.

The Internet has transformed our lives. We must ensure that Internet-based technologies remain sources of enrichment, rather than becoming forces of destruction and vectors of chaos. I look forward to our continued work together in support of a prosperous and safe America.

Appendix 2
Recent Successful Botnet Disruptions

VPNFilter

In May 2018, the Department took steps to disrupt the operation of a global botnet of hundreds of thousands of infected home and office ("SOHO") routers and other networked devices under the control of a group of actors known as the "Sofacy Group" (also known as "apt28," "sandworm," "x-agent," "pawn storm," "fancy bear" and "sednit").[1] The botnet, which the FBI and cybersecurity researchers called "VPNFilter," targets SOHO routers and network-access storage devices. In order to identify infected devices and facilitate their remediation, the U.S. Attorney's Office for the Western District of Pennsylvania applied for and obtained court orders authorizing the FBI to seize a domain that is part of the malware's command-and-control infrastructure. The FBI also put out a public service announcement urging individuals and organizations to reset their routers.[2]

The cumulative effect of these actions would be to purge parts of the malware from the routers that were reset, and to direct attempts by the remaining malware to reinfect the device to an FBI-controlled server, which captured the Internet Protocol ("IP") address of infected devices. A non-profit partner organization agreed to disseminate the IP addresses to those who can assist with remediating the botnet, including foreign CERTs and Internet service providers.

Although the devices would remain vulnerable to reinfection while connected to the Internet, these efforts maximized opportunities to identify and remediate the infection worldwide in the time available before Sofacy actors learned of the vulnerability in their command-and-control infrastructure.

Kelihos

On April 10, 2017, the Department announced an extensive effort to disrupt and dismantle the Kelihos botnet—a global network of tens of thousands of computers infected with the Kelihos malware.[3] Under the control of a cybercriminal, Peter Levashov, that botnet facilitated a range of malicious activities, including harvesting login credentials, distributing hundreds of millions of spam e-mails, and installing ransomware and other malicious software. The enormous volume of unsolicited spam e-mails sent by the botnet advertised counterfeit drugs, work-at-home scams, and a variety of other frauds, including deceptively promoted stocks in order to fraudulently increase their price (so-called "pump-and-dump" stock fraud schemes).

To liberate the victim computers from the botnet, the Department obtained civil and criminal court orders that authorized measures to neutralize the Kelihos botnet by (1) seizing domain names that the botnet used to communicate with the command-and-control servers, (2) establishing substitute servers that received the automated requests for instructions so that infected computers no longer communicated with the criminal operator, and (3) blocking any commands sent from the criminal operator attempting to regain control of the infected computers. As described in Chapter 3, Levashov was arrested in Spain and extradited to the U.S. to face justice.

Avalanche

On November 30, 2016, the Department, in coordination with German state and federal police, Europol, and various other countries and entities, conducted a takedown operation against

the Avalanche malware infrastructure. This takedown led to the disabling of seven botnets that relied on this infrastructure and impacted approximately 10 different malware families that had utilized the Avalanche network.

The Avalanche network offered cybercriminals a secure infrastructure, designed to stand in the way of detection by law enforcement and cyber security experts, over which the criminals conducted malware campaigns as well as money laundering schemes known as "money mule" schemes. Access to the Avalanche network was offered to the cybercriminals through postings on exclusive underground online criminal forums. In these schemes, highly organized networks of "mules" purchased goods with stolen funds, enabling cybercriminals to launder the money they acquired through malware attacks or other illegal means.

The types of malware and money mule schemes operating over this network varied. Ransomware, such as Nymain, encrypted victims' computer files until the victim paid a ransom (typically in a form of electronic currency) to the cybercriminal. Other malware, such as GozNym, was designed to steal victims' sensitive banking credentials, which were directed through the intricate network of Avalanche servers to backend servers controlled by the cybercriminals and used to initiate fraudulent wire transfers.

The Avalanche network, which had been operating since at least 2010, was estimated to involve hundreds of thousands of infected computers worldwide. The monetary losses associated with malware attacks conducted over the Avalanche network were estimated to be in the hundreds of millions of dollars worldwide, although exact calculations are difficult due to the high number of malware families present on the network.

This operation required an unprecedented level of international coordination to seize, block, and sinkhole over 800,000 malicious domains associated with the Avalanche network. These domains had been used to send commands to infected devices, pass banking credentials to cyber criminals, and obfuscate efforts by law enforcement to investigate this conspiracy. The USAO for the Western District of Pennsylvania and the Computer Crime and Intellectual Property Section obtained a temporary restraining order which greatly assisted in this effort. The Department continues to build on the success of this operation, using information obtained through seized infrastructure to identify and arrest criminals responsible for the creation of the malware distributed via Avalanche.

Gameover Zeus & Cryptolocker

In 2014, the Department led a coalition of nearly a dozen foreign countries and a group of elite computer security firms to disrupt and dismantle the highly-sophisticated "Gameover Zeus botnet."4 At its peak, that botnet consisted of a global network of between 500,000 and 1 million computers infected malware that used keystroke logging to collect online financial account information and, in turn, inflicted more than $100 million of losses to individuals in the United States. The Gameover Zeus network was also used to spread the Cryptolocker ransomware, which used cryptographic key pairs to encrypt the computer files of its victims and often left victims with no choice but to pay hundreds of dollars to obtain the decryption keys needed to unlock their files. As of April 2014, security researchers estimated that Cryptolocker had infected more than 234,000 computers and, according to one estimate, caused more than $27 million in ransom payments in its first two months in circulation.

To disrupt both the Gameover Zeus botnet and the Cryptolocker malware, the Department deployed a combination of criminal and civil tools available to law enforcement. As an initial matter, a federal grand jury indicated a key administrator of the botnet (Evgeniy Bogachev) with a 14-count indictment, and the Department filed a separate civil injunction against Bogachev as the leader of a tightly-knit gang of cyber criminals based in Russia and Ukraine responsible for both the Gameover Zeus and Cryptolocker schemes. Further, as in Kelihos, the Department obtained civil and criminal court orders authorizing measures to redirect requests for instructions by computers victimized by the two schemes away from the criminal operators to substitute servers established pursuant to court order. The FBI was also authorized to obtain the IP addresses of the victim computers reaching out to the substitute servers, and to provide that information to DHS's Computer Emergency Readiness Team (US-CERT) to help victims remove the Gameover Zeus malware from their computers.[5]

To identify servers as command-and-control hubs for the Gameover Zeus botnet and Cryptolocker malware, and to subsequently facilitate victims' efforts to remediate the damage to their computers, the Department also enlisted the assistance of numerous computer security firms and leading universities.

Coreflood

In 2011, the Department disrupted and disabled the decade-old "Coreflood" botnet through a civil complaint, search warrants, a criminal seizure warrant, and a temporary restraining order.[6]

This botnet was a global network of 100,000 computers infected with a particularly harmful type of malware named Coreflood, which could be controlled remotely to steal private personal and financial information from unsuspecting computer users. The botnet's administrators, in turn, used the stolen information for a variety of criminal purposes, including stealing funds from the compromised accounts. In one example described in court filings, for instance, Coreflood leveraged information gleaned through illegal monitoring of Internet communications between a user and the user's bank to take over an online banking session and cause the fraudulent transfer of funds to a foreign account.

The Department employed a multi-prong enforcement strategy to dismantle the Coreflood botnet. It obtained search warrants to seize five command-and-control servers that remotely controlled hundreds of thousands of infected computers, and a seizure warrant to secure 29 domain names that the botnet used to communicate with the command-and-control servers. Federal authorities also obtained a temporary restraining order that authorized the government to replace the illegal command-and-control servers with substitute servers. To prevent the defendants from reconstituting the botnet through new servers, domains, and updated software, the TRO also authorized the government to respond to routine requests for direction from the infected computers in the United States with a command that temporarily stopped the Coreflood malware from running on the infected computers. By limiting the defendants' ability to control the botnet, computer security providers and victims were given the time and opportunity to remove the malware from infected computers. The Department also filed a civil complaint against 13 "John Doe" defendants associated with the botnet.

NOTES

[1] Press Release, "Justice Department Announces Actions to Disrupt Advanced Persistent Threat 28 Botnet of Infected Routers and Network Storage Devices," U.S. Dept. of Justice (May 23, 2018), available at: https://www.justice.gov/opa/pr/justice-department-announces-actions-disrupt-advanced-persistent-threat-28-botnet-infected (last accessed June 29, 2018).

[2] Federal Bureau of Investigation, "Foreign Cyber Actors Target Home and Office Routers and Networked Devices Worldwide" (May 25, 2018), available at: https://www.ic3.gov/media/2018/180525.aspx (last accessed June 29, 2018).

[3] Press Release, "Justice Department Announces Actions to Dismantle Kelihos Botnet," U.S. Dept. of Justice (Apr. 10, 2017), available at: https://www.justice.gov/opa/pr/justice-department-announces-actions-dismantle-kelihos-botnet-0 (last accessed June 29, 2018).

[4] Press Release, "U.S. Leads Multi-National Action Against "Gameover Zeus" Botnet and "Cryptolocker" Ransomware, Charges Botnet Administrator," U.S. Dept. of Justice (June 2, 2014), available at: https://www.justice.gov/opa/pr/us-leads-multi-national-action-against-gameover-zeus-botnet-and-cryptolocker-ransomware (last accessed June 29, 2018).

[5] At no point during the operation did the FBI or law enforcement access the content of any of the victims' computers or electronic communications.

[6] Press Release, "Department of Justice Takes Action to Disable International Botnet," U.S. Dept. of Justice (Apr. 13, 2011), available at: https://www.justice.gov/opa/pr/department-justice-takes-action-disable-international-botnet (last accessed June 29, 2018).

Appendix 3
Recent Successful Dark Web Disruptions

AlphaBay & Hansa

On July 20, 2017, the Department announced the seizure of AlphaBay, an online criminal marketplace that had operated for over two years on the dark web and facilitated the sale throughout the world of deadly illegal drugs, stolen and fraudulent identification documents and access devices, counterfeit goods, malware and other computer hacking tools, firearms, and toxic chemicals. Around the time of its takedown, AlphaBay was the largest criminal marketplace on the Internet. Indeed, prior to the site's disruption, one AlphaBay staff member claimed that it serviced over 200,000 users and 40,000 vendors. AlphaBay operated as a hidden service on the "Tor" network, and used cryptocurrencies including Bitcoin, Monero, and Ethereum in order to hide the locations of its underlying servers and the identities of its administrators, moderators, and users. Based on law enforcement's investigation of AlphaBay, authorities believe the site was also used to launder hundreds of millions of dollars deriving from illegal transactions on the website.

The operation to seize the AlphaBay site coincided with efforts by Dutch law enforcement to investigate and take down the Hansa Market, another prominent dark web market. Like AlphaBay, Hansa Market was used to facilitate the sale of illegal drugs, toxic chemicals, malware, counterfeit identification documents, and illegal services. To maximize the disruptive impact of the joint takedowns, Dutch authorities took covert control over the Hansa Market during the period when AlphaBay was shutdown. That covert control not only allowed Dutch police to identify and disrupt the regular criminal activity on Hansa, but then also allowed the authorities to sweep up all those new users who were displaced from AlphaBay and needed a new trading platform. The success of this joint operation stands out as yet another example of what international law enforcement can accomplish when working closely together to neutralize a cybercrime marketplace.

Silk Road

In late 2013, the Department joined with various law enforcement partners across the government to disrupt the hidden "Silk Road" website, and to prosecute its creator and owner, Ross Ulbricht.[1]

For the two years leading up to the Department's actions, Silk Road stood out as the most sophisticated and extensive criminal marketplace on the Internet, serving as a sprawling black-market bazaar where unlawful goods and services, including illegal drugs of virtually all varieties, were regularly bought and sold. At its height, several thousand drug dealers and other unlawful vendors used the site to distribute hundreds of kilograms of illegal drugs and other unlawful goods and services to well over 100,000 buyers, and to launder hundreds of millions of dollars deriving from these unlawful transactions.

To remain outside the reach of law enforcement, Silk Road's administrators anonymized the site's transactions by operating it on the Tor network and including a Bitcoin-based payment system designed to conceal its users' identities and locations. Despite these efforts, law enforcement ultimately pierced Silk Road's cloak of anonymity and seized control of the website, its domain, its servers, and 29,655 Bitcoins residing on those servers (worth approximately $28 million at the

time of seizure). The creator and administrator of Silk Road, Ross Ulbricht, was also arrested and ultimately convicted of seven charges relating to money laundering and computer hacking, among others, and sentenced to life in federal prison. The government seized an additional 144,336 Bitcoins from Ulbricht's computer hard drive (worth approximately $130 million at the time of seizure).

Operation Onymous

Building on the success of the Silk Road takedown, in November 2014, U.S. and European authorities took joint action against the underground website known as "Silk Road 2.0," as well as dozens of additional dark market websites that were facilitating the sale of an astonishing range of illegal goods and services on hidden services within the Tor network, including weapons, drugs, murder-for-hire services, stolen identification data, money laundering, hacking services, and others.[2] Silk Road 2.0 was created in November 2013 to fill the void left by the government's seizure of the Silk Road website in October 2013. As with Silk Road, the Department used civil forfeiture authorities to seize control over 400 Tor website addresses known as ".onion" addresses, as well as the servers hosting them. Administrators associated with these Dark Web markets were criminally prosecuted.

Darkode

On July 15, 2015, the Department announced the dismantling of a computer hacking forum known as "Darkode" as part of a coordinated law enforcement action across 20 countries that led to the search, arrest, or charging of 70 Darkode members and associates.[3]

At the time of its takedown, the Darkode forum represented a uniquely grave threat to the integrity of data on computers because it provided a platform where highly-sophisticated cybercriminals congregated to buy, sell, and trade malware, botnets, and PII used to steal from U.S. citizens and individuals around the world. Before becoming a member of Darkode, prospective members were allegedly vetted through a process in which an existing member invited a prospective member to the forum for the purpose of presenting the skills or products that he or she could bring to the group. As part of Operation Shrouded Horizon, the FBI was able to disrupt and dismantle Darkode by infiltrating the forum's membership.

NOTES

[1] Press Release, "Manhattan U.S. Attorney Announces Seizure of Additional $28 Million Worth of Bitcoins Belonging to Ross William Ulbricht, Alleged Owner and Operator of "Silk Road" Website," Federal Bureau of Investigation (Oct. 25, 2013), available at: https://archives.fbi.gov/archives/newyork/press-releases/2013/manhattan-u.s.-attorney-announces-seizure-of-additional-28-million-worth-of-bitcoins-belonging-to-ross-william-ulbricht-alleged-owner-and-operator-of-silk-road-website (last accessed June 29, 2018).

[2] Press Release, "Dozens of Online 'Dark Markets' Seized Pursuant to Forfeiture Complaint Filed in Manhattan Federal Court in Conjunction with the Arrest of the Operator of Silk Road 2.0," Federal Bureau of Investigation (Nov. 7, 2014), available at: https://www.fbi.gov/contact-us/field-offices/newyork/news/press-releases/dozens-of-online-dark-markets-seized-pursuant-to-forfeiture-complaint-filed-in-manhattan-federal-court-in-conjunction-with-the-arrest-of-the-operator-of-silk-road-2.0 (last accessed June 29, 2018).

[3] Press Release, "Major Computing Hacking Forum Dismantled," U.S. Dept. of Justice (July 15, 2015), available at: https://www.justice.gov/opa/pr/major-computer-hacking-forum-dismantled (last accessed June 29, 2018).

Appendix 4
Glossary of Key Terms

Acronym	Meaning
AECA	Arms Export Control Act
AUSA	Assistant United States Attorney
BEC	Business Email Compromise
Boyusec	Guangzhou Bo Yu Information Technology Company Limited
C&C	Command-and-Control
C.F.R.	Code of Federal Regulations
C2	Command and Control
CAATSA	Countering America's Adversaries Through Sanctions Act
CAN-SPAM	Controlling the Assault of Non-Solicited Pornography and Marketing
CAT	Cyber Action Team
CCIPS	Computer Crime and Intellectual Property Section
CFAA	Computer Fraud and Abuse Act
CHIP	Computer Hacking and Intellectual Property
CFIUS	Committee on Foreign Investment in the United States
CISO	Chief Information Security Officer
CLOUD	Clarifying Lawful Overseas Use of Data
CNN	Cable News Network
CTF	Cyber Task Force, Federal Bureau of Investigation
DDoS	Distributed Denial of Service
DEA	Drug Enforcement Administration
DHS	Department of Homeland Security
DMCA	Digital Millennium Copyright Act
DOJ	Department of Justice
DSAC	Domestic Security Alliance Council

Acronym	Meaning
EAR	Export Administration Regulations
ECPA	Electronic Communications Privacy Act
ECTR	Electronic Communication Transactional Record
EEA	Economic Espionage Act
EOUSA	Executive Office for United States Attorneys
ESU	Electronic Surveillance Unit
FBI	Federal Bureau of Investigation
FinCEN	Financial Crimes Enforcement Network
FISA	Foreign Intelligence Surveillance Act
FLASH	FBI Liaison Alert System
FSB	Russian Federal Security Service
GDPR	General Data Protection Regulation
HTOCU	Hi-Tech Organized Crime Unit
IC3	The Internet Crime Complaint Center
IEEPA	International Emergency Economic Powers Act
INTERPOL	International Criminal Police Organization
IoT	Internet of hings
IP (address)	Internet Protocol
IPR	Intellectual Property Rights
IRS	Internal Revenue Service
ISIL	Islamic State of Iraq and the Levant
ISP	Internet Service Provider
JAR	Joint Analysis Report
J-CODE	Joint Criminal Opioid Darknet Enforcement
JITs	Joint Investigative Teams
JTA	Joint Technical Advisory
KAT	Kickass orrents

Acronym	Meaning
MLARS	Money Laundering and Asset Recovery Section, Criminal ivision
MLAT	Mutual Legal Assistance Treaty
MUCD	Military Unit Cover esignator
NCCIC	National Cybersecurity and Communications Integration Center
NCFTA	National Cyber-Forensics and Training Alliance
NCIJTF	National Cyber Investigative Joint Task Force
NDCAC	National Domestic Communications Assistance Center
NICE	National Initiative for Cybersecurity Education
NITs	Network Investigative Techniques
NSCS	National Security Cyber Specialists
NSD	National Security Division
NSL	National Security Letter
OFAC	Office of Foreign Assets Control
OIA	Office of International Affairs, Criminal ivision
OJT	On the Job Training
OLE	Office of Legal Education
P2P	Peer-to-Peer
PII	Personally Identifiable Information
PINs	Private Industry Notifications
PLA	People's Liberation Army
PPD	Presidential PolicyD irective
PRC	People's Republic of China
PRTT	Pen Register and Trap and Trace
PSA	Public Service Announcement
RICO	Racketeer Influenced and Corrupt Organizations Act
ROB	Rules of Behavior
SCADA	Supervisory Control and Data Acquisition

Acronym	Meaning
SPE	Sony Pictures Entertainment
STSO	Operational Support Unit (Drug Enforcement Administration)
SUA	Specified Unlawful ctivity
Tor	The Onion Router
TRO	Temporary Restraining Order
USAO	United States ttorney's Office
USNCB	United States National Central Bureau (INTERPOL)
US-CERT	United States Computer Emergency Readiness Team
USTR	United States Trade Representative
RRA	Victims' Rights and Restitution ct
WTI	Workforce Training Initiative