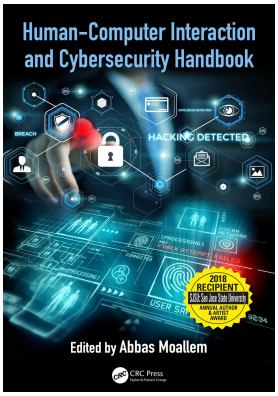

Human-Computer Interaction and Cybersecurity Handbook

Abbas Moallem

US government and law enforcement

Publication details
https://test.routledgehandbooks.com/doi/10.1201/b22142-17
Greg A. Ruppert
Published online on: 24 Oct 2018

chapter seventeen

US government and law enforcement

Greg A. Ruppert

Contents

17.1 Introduction

The complexity of cybersecurity in both scope and definition is evidenced in the real world by the myriad federal, state, local, and international agencies which play an integral role in the prevention, mitigation, and investigation of cyber-related incidents. Cyberadversaries range from nation states to organized crime groups to cyberhacktivists, all of which can vary their vectors of attack against a wide range of victims throughout the United States. Victims can include government sites, critical infrastructure, businesses, or individuals. Given the online and digital interactions between companies, systems, and customers, the ability to effectively fortify systems has become increasingly impossible. Adding to the complexity of defense are the complexity and size of the criminal adversaries. Nation states primarily engage in warfare, espionage, malicious attacks, and corporate theft. Organized crime groups engage in fraud, identity

theft, ransomware, and spear phishing campaigns for financial gain. Cyberhacktivists 7pursue a social agenda through a variety of cyberattacks designed to gain attention for their cause. As a result, the governmental reaction to cybersecurity has been to create or empower a panoply of agencies with authorities or jurisdiction, which was designed to provide the necessary response expertise to the evolving threat driven by the Internet and cyber-enabled enhancements to our global environment. However, this approach over time has led to confusion for the victims of cyberattacks as well as jurisdictional fighting among the many agencies. Thus, numerous legislative actions and executive orders have been enacted to define "the lanes in the road" for lead roles and to facilitate the coordination, outreach, and liaison between the agencies. This chapter will discuss the government and law enforcement agencies involved in cybersecurity, their roles, governing structures, and coordinating entities.

17.2 US governmental landscape

Cybersecurity has multiple facets that range from net defense to investigation to proactive activities to mitigation postattack. The US response has been historically divided into law enforcement, defense, and intelligence agencies. These were all developed agencies prior to the increased focus on cybersecurity. Thus, several departments and agencies have assumed or been given new or enhanced jurisdiction. This has resulted in an often confusing patchwork of agencies being involved in an investigation depending on the actor, cyberactivity, or government response. Under the US governmental landscape, this chapter will discuss the executive branch oversight and the coordination approach as well as the most prevalent federal agencies involved in the cybersecurity response in the US.

17.3 Overarching executive branch policy governance for a "whole-of-government" approach

Traditionally, the National Security Council (NSC) is the main policy development and coordination arm of the administration. President Obama prioritized the need to institutionalize policies to facilitate stronger cybersecurity and better protect the United States against cyberthreats [1]. Depending on the administration, the NSC appoints a high-ranking official to oversee the administration of the federal government of cybersecurity through the many departments and agencies and oversee a central interagency coordinating body related to cybersecurity. This interagency group will meet on a regular basis and as needed to provide operational coordination.

17.3.1 Cyber Unified Coordination Group

One of the more significant acts undertaken by the federal government was to outline the lanes in the road related to the federal government response to a cyberattack. This was accomplished through the creation of a Cyber Unified Coordination Group to coordinate the response to a significant cyberincident. Significant cyberincidents were defined as those that affect critical infrastructure owners and operators or cyberincidents that could have catastrophic regional or national effects on public health or safety, economic security, or national security.

17.4 Department of Homeland Security

The Department of Homeland Security (DHS) has a number of agencies and offices responsible for multiple areas of cybersecurity. Under the National Protection and Programs Directorate, the DHS executes on multiple missions from the Office of Cybersecurity and Communications, Office of Cyber Infrastructure and Analysis, and the Office of Infrastructure and Protection. As a result of the combined effort, dozens of cybersecurity alerts to the private sector and general public related to cyberthreats are issued daily.

17.4.1 Office of Cybersecurity and Communications

The Office of Cybersecurity and Communications (CS&C), within the National Protection and Programs Directorate [2], is responsible for enhancing the security, resilience, and reliability of the cyberinfrastructure and communications infrastructure of the nation. CS&C works to prevent or minimize disruptions to critical information infrastructure in order to protect the public, the economy, and government services. CS&C leads efforts to protect the federal ".gov" domain of civilian government networks and to collaborate with the private sector—the ".com" domain—to increase the security of critical networks [3].

17.4.2 National Cybersecurity and Communications Integration Center

Additionally within CS&C, there is the National Cybersecurity and Communications Integration Center (NCCIC), which serves as a 24/7 cybermonitoring, incident response, and management center and as a national point of cyberincident and communications incident integration [4]. The NCCIC (pronounced "n-kick") is composed of four branches: NCCIC Operations and Integration, United States Computer Emergency Readiness Team (US-CERT) [5], Industrial Control Systems Cyber Emergency Response Team, and National Coordinating Center for Communications [4].

17.4.3 Office of Cyber and Infrastructure Analysis

The Office of Cyber and Infrastructure Analysis provides consolidated all-hazards consequence analysis, ensuring that there is an understanding and awareness of cybercritical and physical critical infrastructure interdependencies and the impact of a cyberthreat or incident to the critical infrastructure of the nation [6].

17.4.4 Office of Infrastructure Protection

The Office of Infrastructure Protection (leads the coordinated national effort to reduce the risk to US critical infrastructure posed by acts of terrorism. In doing so, the level of preparedness and the ability to respond and quickly recover in the event of an attack, natural disaster, or other emergency of the nation is increased [7].

17.4.5 US Cyber Emergency Response Team

As mentioned earlier, the DHS has the responsibility for the US Cyber Emergency Response Team. US-CERT provides a broad range of reporting and analysis to the government and private sector. US-CERT also exchanges information across a global Computer Security Incident Response Team community to improve the security of the

critical infrastructure and the systems and assets of the nation on which Americans depend. Partners with which US-CERT may share information include US federal agencies; private sector organizations; the research community; state, local, tribal and territorial governments; and international entities [8]. US-CERT is a member of the Forum for Incident Response and Security Teams [9]. US-CERT also provides a robust collection of reporting, analysis, and alerts valuable to the ongoing defenses needed for a robust cybersecurity program under their Cybersecurity Awareness System. As noted on their website, individuals can sign up to receive their four products that provide a range of information for users with varied technical or general expertise [10]. Those with more technical interest can read the *Alerts*, *Current Activity*, or *Bulletins*, while users looking for more general-interest pieces can read the *Tips* [10].

17.5 US law enforcement

In the United States, there are several different federal law enforcement agencies with overlapping jurisdictions to include the wide-ranging array of illegal activities connected to cybercrime. Cybercrimes include complex computer intrusions by nation states, hacktivism, and cyber-enabled criminal activity related to fraud and other financial scams. Also, the Internet and electronic communications are used in a multitude of other federal crimes such as terrorism, human trafficking, drug trafficking, and child pornography. In addition, there are state, local, tribal, and territorial law enforcement agencies which also have jurisdiction over cybercriminal activity. In 2016, the Presidential Policy Directive-41 [11] on US Cyber Incident Coordination Policy was released, setting forth principles governing the response of the federal government to cyberincidents. The policy designates certain federal agencies to take the lead in three different response areas—threat response, asset response, and intelligence support. Those agencies and their roles are as follows:

- The Department of Justice, acting through the Federal Bureau of Investigation (FBI) and the National Cyber Investigative Joint Task Force (NCIJTF), will be taking the lead on threat response activities.
- The DHS, acting through the NCCIC, will be the lead agency for asset response activities.
- The Office of the Director of National Intelligence, through its Cyber Threat Intelligence Integration Center, will be the lead agency for intelligence support and related activities [12].

17.5.1 National Cyber Investigative Joint Task Force

The NCIJTF was created in 2008 to provide coordination among law enforcement and intelligence communities. The NCIJTF is composed of over 20 partnering agencies and has representatives who are colocated and jointly work to accomplish the mission of the organization from a whole-of-government perspective. As a unique multiagency cybercenter, the NCIJTF has the primary responsibility to coordinate, integrate, and share information to support cyberthreat investigations, supply and support intelligence analysis for community decision-makers, and provide value to other ongoing efforts in the fight against the cyberthreat to the nation [13]. The NCIJTF is managed by the FBI and led by an FBI senior executive as the director of the task force. Recent congressional legislation mandated the increased sharing of cyberthreat information, and the response of the government highlighted the role the NCIJTF.

17.5.2 FBI

The FBI is the lead federal agency for investigating cyberattacks by criminals, overseas adversaries, and terrorists. In fact, the majority of cybercrime is investigated by one of the FBI's 56 field offices' cyber task forces. These investigations are usually prioritized for larger intrusions or major attacks. They typically include massive distributed denial–of-service attacks, as well as Botnets and malware investigations. Efforts of the cyber task forces are overseen by the Cyber Division of the FBI within FBI headquarters. Unless the Internet merely facilitates the commission of the criminal activity (such as bank fraud or child sex trafficking), matters are assigned to the cyber task forces. Given the interplay between cyber-enabled crimes and the underlying type of crimes, often FBI squads will collaborate against a specific target [14]. The FBI Cyber Division in addition to overseeing and supporting field office efforts also manages several specialty units to facilitate the more robust engagement with the private sector, other governmental entities, and victims of cybercrimes.

17.5.2.1 FBI Internet Crime Complaint Center

The FBI Cyber Division also runs the Internet Crime Complaint Center (IC3) so the public can report information to the FBI regarding Internet-facilitated criminal activity. Reports are collected and disseminated to a variety law enforcement agencies for investigative and intelligence purposes. Reports are also created for public awareness [15]. Along with partner agencies, the IC3 participates in multiple initiatives targeting the following types of frauds:

- Charitable contributions fraud
- Counterfeit check fraud
- Identity theft task force
- International fraud
- Investment fraud
- Online pharmaceutical fraud
- Phishing
- Work-at-home scams [16]

17.5.2.2 FBI InfraGard

A partnership with members of the private sector, called InfraGard, is also overseen by the Cyber Division of the FBI. InfraGard is locally run by the FBI field offices. It has 84 chapters with more than 46,000 members nationwide, helping to protect and defend critical infrastructures [17]. The InfraGard program was designed to facilitate public–private collaboration between the private sector and the government [17].

17.5.3 DHS–US Secret Service

The Secret Service also engages in the investigation of cybercrime. It has developed an electronic crimes special agent program and established network of 46 financial crimes task forces and 39 electronic crimes task forces (ECTFs).

17.5.3.1 Electronic crimes task force

In 2001, the US PATRIOT Act mandated that the Secret Service establish a national network of ECTFs to prevent, detect, and investigate various forms of electronic crimes including

cybercrime [18]. Similar to the InraGard of the FBI, the ECTF model relies on partnerships between the law enforcement, the private sector, and academic community to share information and intelligence [18]. These ECTFs are a strategic alliance of over 4000 private sector partners; over 2500 international, federal, state, and local law enforcement partners; and over 350 academic partners [18].

17.6 State and local law enforcement efforts

The United States consists of tens of thousands of state-level and local-level law enforcement agencies. These agencies have differing geographic as well as state and local law jurisdictions. In addition, the agencies can greatly vary in size such as major large city departments with over 40,000 sworn officers to small departments consisting of as few as two deputies. As a result, the cyber-related expertise greatly varies. While the FBI has management responsibilities over several national databases such as fingerprint records* or the National Crime Information Center,† there are no standardized cyber-related databases. Additionally, many state and local departments do not possess the equipment, expertise, or related resources to conduct cyber-enabled or cyber-related investigations. Some states also vary with the degrees of criminal legislation related to cyberattacks. Additionally, most agencies lack the ability to efficiently investigate criminal activity, which crosses state lines, let alone national borders. Thus, given the speed and distance in which cybercrimes occur, the methods of state and local law enforcement investigation, which was designed around protecting the local community from criminal activity occurring in that area by actors also located in the same area, have not kept pace with technological advancements.

17.6.1 FBI regional computer forensic laboratories

In an effort to assist state and local law enforcements, the FBI established regional cyber forensic laboratories (RCFLs) to provide technical assistance, develope new digital

* In July 1999, the fingerprint identification function was automated in the Integrated Automated Fingerprint Identification System (IAFIS). This national, computerized system for storing, comparing, and exchanging fingerprint data in a digital format permits comparisons of fingerprints in a faster and more accurate manner. It is located in, and operated by, the Criminal Justice Information Services Division of the FBI in Clarksburg, West Virginia. IAFIS provides three major services to its customers. First, it is a repository of criminal history information, fingerprints, criminal subject photographs, as well as information regarding military and civilian federal employees and other individuals as authorized by Congress. Second, it provides positive identification of individuals based on fingerprint submissions (both through 10 print fingerprints and latent fingerprints). Third, it provides tentative identification of individuals based on descriptive information such as a name, date of birth, distinctive body markings, and identification numbers. The primary function of IAFIS is to provide the FBI a fully automated fingerprint identification and criminal history reporting system. Additionally, IAFIS has made several other accomplishments. It has improved latent fingerprint identification services to the law enforcement community, and it has helped develop uniform biometric standards. These improvements have eliminated the need to process and retain paper fingerprint cards and has thereby accelerated the identification process. Another benefit has been the development of improved digital image quality. See FBI [19].

† The National Crime Information Center, or NCIC, has been called the lifeline of law enforcement—an electronic clearinghouse of crime data that can be tapped into by virtually every criminal justice agency nationwide, 24 hours a day, 365 days a year. It helps criminal justice professionals apprehend fugitives, locate missing persons, recover stolen property, and identify terrorists. It also assists law enforcement officers in performing their duties more safely and provides information necessary to protect the public. NCIC was launched on January 27, 1967 with five files and 356,784 records. By the end of 2015, NCIC contained 12 million active records in 21 files. During 2015, NCIC averaged 12.6 million transactions per day. See FBI [20].

evidence forensics tools, and create training programs for digital evidence examiners and law enforcement officers [21].

As a result, the FBI has created 15 RCFLs to serve as a forensics laboratory and training center for the examination of digital evidence in support of all types of criminal investigations. A typical midsize RCFL consists of 15 people whose responsibilities range from crime scene-based digital evidence collection to computer evidence examinations as well as related testimony before a court or grand jury. These RCFLs provide much needed expertise to smaller departments throughout the United States [21].

17.7 Conclusion

The speed of which cybercrime has grown from a mechanism to cause mayhem and engage in small cyber-enabled fraud into a worldwide epidemic has not allowed law enforcement to keep pace with the threats. The international scope of the infrastructure used and the speed at which an attack can be carried out make it nearly impossible to prevent criminal, nation state, or terrorism attacks, and the established mechanisms built over centuries to investigate and bring criminals to justice are oftentimes efforts of futility. Adding to the complexity is that the victims are often private sector companies with no interest in coming forward to report a massive intrusion as such a pronouncement will result in damage to their brand, civil lawsuits, executive dismissals, and loss of revenues. As a result, the cooperation between the primary victim of the crime is filtered through law firms and often delayed. The ultimate victims are often the clients or customers of the company that suffered the initial cyberattack and their interests are sometimes only a secondary concern to the companies they once entrusted with their information. Further complicating law enforcement efforts is the traditional methodology of investigating crimes where they occur through regional offices connected to the community. The ability for cybercrimes and attacks, which primarily emanate from overseas locations and strike multiple US victims in differing locations in rapid succession, requires a centralized investigative division in order to collect all the threat intelligence and evidence and then conduct truly holistic investigations. A centralized program would serve as a primary hub of all collection and investigation, thereby possessing the ability to fully comprehend the attack and facilitate the full-range response actions and preventative measures which only the whole-of-government approach has to offer. Unfortunately, such a massive shift in established bureaucratic structures to accomplish this centralization would require a level of leadership in the political structures of Washington, DC, that is unprecedented in recent history.

References

1. *Fact Sheet: The Administration's Cybersecurity Accomplishments*, The White House, Washington, DC, https://obamawhitehouse.archives.gov/sites/default/files/fact_sheet-administration_cybersecurity_accomplishments.pdf, May 19, 2018.
2. *National Protection and Programs Directorate*, Department of Homeland Security, Washington, DC, https://www.dhs.gov/national-protection-and-programs-directorate, May 19, 2018.
3. *Office of Cybersecurity and Communications*, Department of Homeland Security, Washington, DC, https://www.dhs.gov/office-cybersecurity-and-communications, May 19, 2018.
4. *National Cybersecurity and Communications Integration Center*, Department of Homeland Security, Washington, DC, https://www.dhs.gov/national-cybersecurity-and-communications-integration-center, May 19, 2018.
5. *US-CERT*, https://www.us-cert.gov/, May 19, 2018.

6. *Office of Cyber and Infrastructure Analysis*, Department of Homeland Security, Washington, DC, https://www.dhs.gov/office-cyber-infrastructure-analysis, May 19, 2018.
7. *Office of Infrastructure Protection*, Department of Homeland Security, Washington, DC, https://www.dhs.gov/office-infrastructure-protection, May 19, 2018.
8. US-CERT (United States Computer Emergency Readiness Team). *About Us*, US-CERT, Washington, DC, https://www.us-cert.gov/about-us, May 19, 2018.
9. *FIRST*, https://www.first.org/, May 19, 2018.
10. *National Cyber Awareness System*, US-CERT, Washington, DC, https://www.us-cert.gov/ncas, May 19, 2018.
11. *Presidential Policy Directive—United States Cyber Incident Coordination*, The White House, Washington, DC, https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident, May 19, 2018.
12. *Countering the Cyber Threat*, Federal Bureau of Investigation, Washington, DC, https://www.fbi.gov/news/stories/new-us-cyber-security-policy-codifies-agency-role, May 19, 2018.
13. *National Cyber Investigative Joint Task Force*, Federal Bureau of Investigation, Washington, DC, https://www.fbi.gov/investigate/cyber/national-cyber-investigative-joint-task-force, May 19, 2018.
14. *FBI-Cyber*, Federal Bureau of Investigation, Washington, DC, https://www.fbi.gov/investigate/cyber, May 19, 2018.
15. *FBI, IC3*, Internet Crime Complaint Center, Clarksburg, West Virginia, https://www.ic3.gov/about/default.aspx, May 19, 2018.
16. *FBI, IC3—Brochure*, Internet Crime Complaint Center, Clarksburg, West Virginia, https://www.ic3.gov/media/IC3-Brochure.pdf, May 19, 2018.
17. *FBI, InfraGard*, https://www.infragard.org, May 19, 2018.
18. *USSS—Cyber ECTF Brochure*, US Secret Service, Washington, DC, https://www.secretservice.gov/data/investigation/USSS-Cyber-Investigations-Flyer.pdf, May 19, 2018.
19. *Criminal Justice Information Services (CJIS)*, Federal Bureau of Investigation, Washington, DC, https://www.fbi.gov/services/cjis
20. *National Crime Information Center*, Federal Bureau of Investigation, Washington, DC, https://fbi.gov/services/cjis/ncic, May 19, 2018.
21. *Regional Computer Forensic Laboratory*, https://www.rcfl.gov/, May 19, 2018.