UDK 343.01(73)
343.2:004.7(73)
343.2:061.1(73)
336.745:004.3/.4(73)
343.359(73)
Received on 1 August 2022
Review

Thomas Dougherty *
Nevenka Lastrić Đurić **

THE UNITED STATES APPROACH TO THE INVESTIGATION AND PROSECUTION OF CYBERCRIME AND CRYPTOCURRENCY CRIME ***

This paper is primarily a compendium of various documents published by the United States (U.S.) Government and will provide an overview of the U.S. approach to the investigation and prosecution of cybercrime, i.e. those crimes that use or target computer networks, which we interchangeably refer to as computer crime. It should also be noted that this paper will address the approach to investigating and prosecuting cybercrime at the federal level and not the state or local level. The paper will first provide an overview of the several specialized investigation and prosecution units established within the U.S. that have been created or formed to address this issue. Next, it will provide an explanation to some of the specialized task forces and cybercrime programs established by the U.S. Government which aim to deliver training and technical assistance to foreign law enforcement, prosecuto-

* Thomas Dougherty is a Senior Trial Attorney with the U.S. Department of Justice (DOJ) and has been detailed from the Computer Crime and Intellectual Property Section (CCIPS) to the U.S. Embassy in Zagreb, Croatia, to serve as the International Computer Hacking and Intellectual Property (ICHIP) Attorney for Central, Eastern and Southern Europe. Prior to his assignment to Zagreb, he established the first ICHIP for Cybercrime office in Kuala Lumpur, Malaysia, in 2015. While serving as a Senior Trial Attorney at CCIPS from 2007 to 2014, he investigated and prosecuted numerous large-scale, multi-jurisdictional cybercrime cases in federal courts across the United States; doughertyts@state.gov.

** Nevenka Lastrić Đurić serves as the Legal Advisor to the International Computer Hacking and Intellectual Property (ICHIP) Attorney for Central, Eastern and Southern Europe at the U.S. Embassy in Zagreb, Croatia. She is a Croatian lawyer who holds an LL.M. degree in International Law from the Washington College of Law of the American University in Washington D.C.; duricn@state.gov; ORCID iD: https://orcid.org/0000-0001-5343-8426

*** The views expressed in this article do not necessarily represent the views of the United States Department of Justice or the United States. The contents of this paper do not purport to reflect the opinions or views of either of its authors. This paper is intended for informational and educational purposes only.

rial, and judicial partners to combat cybercrime activity. The primary U.S. cybercrime legislation will be summarized, including the laws governing the search and seizure of computers and obtaining electronic evidence in U.S. criminal investigations, the Stored Communications Act/Electronic Communications Privacy Act (SCA/ECPA), the U.S. Federal Rules of Evidence (FRE) 902 (13-14) and the Computer Fraud and Abuse Act (CFAA). Finally, the paper will cover the U.S. approach to cryptocurrency related crime and the U.S. Government's approach to seizure and forfeiture of digital assets and sentencing.

Keywords: *cybercrime, digital evidence, cryptocurrency, prosecution, investigation*

1. THE U.S. APPROACH TO INVESTIGATING AND PROSECUTING CYBERCRIME

1.1. Overview

The U.S. approach to deterring and combatting cybercrime and cyber-enabled crime consists of a variety of targeted federal criminal statutes, case law, specialized investigators and prosecutors, and an array of task forces, fusion centers, and complaint centers.

The U.S. takes a multiagency approach to investigating cybercrime and cryptocurrency crime. There are eight federal departments and numerous federal law enforcement agencies involved in cybercrime enforcement in the U.S. The DOJ leads much of the effort to prosecute cybercrime through its Criminal Division, National Security Division, and Office of the United States Attorneys. The DOJ also has cybercrime investigation functions through its law enforcement agencies such as the Federal Bureau of Investigation (FBI). The Department of Homeland Security's United States Secret Service and Homeland Security Investigations Department also play an active role in investigating cyber offenses. The Department of State funds cybercrime capacity building programs through the DOJ and other organizations to strengthen global capacity to investigate and prosecute cybercrimes, improve international cooperation on cybercrime investigations, and increase the sharing of digital evidence across international boundaries. State and local law enforcement agencies are also involved in many cybercrime investigations at the state and local level.

1.2. Specialized Investigation Units and Organizations

a. FBI Cyber Division

The FBI investigates computer crime as defined by the CFAA (18 U.S.C. § 1030 et seq). The CFAA defines a computer intrusion as an unauthorized access of a protected computer. A "protected computer" is defined as any computer connected to the internet or any computer connected to a network that is connected to the internet.[1] The FBI's Cyber Division has primary responsibility for the FBI's efforts to counter national security-related cyber intrusions.[2] The FBI combats cyber intrusion threats primarily through two operational components: the National Cyber investigative Joint Task Force (NCIJTF), an FBI-led multi-agency task force which serves as a national focal point for coordinating, integrating, and sharing pertinent information related to cyber threat investigations, and FBI cyber investigative squads located in each FBI field office in the United States.[3] Each of the 56 FBI field offices throughout the U.S. has at least one cyber squad consisting of special agents, intelligence analysts, and in some cases linguists and computer scientists.[4] The largest field offices have multiple cyber squads, with each squad responsible for investigating different types of cyber cases – such as national security intrusions, criminal intrusions, online child pornography, intellectual property rights, and internet fraud.[5] In the small to medium-size field offices, a single cyber squad may be responsible for investigating all types of cyber cases.[6]

b. Internet Crime Complaint Center

The FBI's Internet Crime Complaint Center (IC3) was founded in 2000 and has the mission to provide 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. Information is analyzed and disseminated for investigative and intelligence purposes to law enforcement and for public awareness.[7]

---

[1] The Federal Bureau of Investigation's Ability to Address the National Security Cyber Intrusion Threat, U.S. Department of Justice, Office of the Inspector General, Audit Division, Audit Report 11-22, April 2011, p. 2.

[2] *Id*., p. 2.

[3] *Id*., p. 2.

[4] *Id*., p. 3.

[5] *Id*., p. 3.

[6] *Id*., p. 3.

[7] "*IC3 Mission Statement, Federal Bureau of Investigation, Internet Crime Complaint Center IC3*", https://www.ic3.gov/Home/About, accessed August 1, 2022.

c. The Virtual Currency Emerging Threats Working Group

The Virtual Currency Emerging Threats Working Group (VCET) was founded by the FBI in early 2012 to mitigate cross-programmatic threats arising from illicit actors' use of virtual currency systems.[8] The group leverages the collective subject matter expertise of its members to address issues arising from illicit actors' use of virtual currency, and deconflicts and shares information and concerns. VCET members represent an array of U.S. Government agencies, including, within the Department, the FBI, the Drug Enforcement Administration, multiple U.S. Attorney's Offices, and the Criminal Division's Asset Forfeiture and Money Laundering Section and Computer Crime and Intellectual Property Section.[9]

d. U.S. Department of Homeland Security Cyber Crimes Center

The U.S. Department of Homeland Security Cyber Crimes Center (HSI C3) supports the HSI's mission through the programmatic oversight and coordination of investigations of cyber-related criminal activity, and provides a range of forensic, intelligence and investigative support services across all HSI programmatic areas.[10] HSI C3 brings together highly technical assets dedicated to conducting trans-border criminal investigations of cyber-related crimes within the HSI portfolio of customs and immigration authorities.[11] It is responsible for identifying and targeting any cybercrime activity in which HSI has jurisdiction.[12] Transnational criminals, particularly sophisticated organizations with elevated technical expertise, have increasingly taken advantage of the anonymity afforded by the dark web and the use of cryptocurrencies to facilitate multiple forms of cross-border criminal activity.[13] To combat this threat, HSI seeks to identify and investigate criminals who use darknet marketplaces to engage in a wide array of crime, including the purchase, sale, and/or transfer of drugs, weapons, child pornography, fraudulent documents, counterfeit or unlicensed pharmaceuticals, and strategic technology.[14]

---

[8] "*Acting Assistant Attorney General Mythili Raman Testifies Before the Senate Committee on Homeland Security and Governmental Affairs, Justice News*", https://www.justice.gov/opa/speech/acting-assistant-attorney-general-mythili-raman-testifies-senate-committee-homeland, accessed August 1, 2022.

[9] *Id*.

[10] "*Cybercrime, Investigating Individuals and Networks Who Commit Online Criminal Activity,*" https://www.ice.gov/investigations/cybercrime-investigations, accessed August 1, 2022.

[11] *Id*.

[12] *Id*.

[13] *Id*.

[14] *Id*.

e. United States Secret Service

The United States Secret Service (USSS) is a federal law enforcement agency under the U.S. Department of Homeland Security. The USSS has two missions – criminal investigations and protection.[15] Criminal investigation activities include financial crimes, identity theft, counterfeiting, computer fraud, and computer-based attacks on the nation's financial, banking, and telecommunications infrastructure.[16] Cyber Fraud Task Forces (CFTFs), the focal point of the USSS's cyber investigative efforts, are a partnership between the Secret Service, other law enforcement agencies, prosecutors, private industry, and academia.[17] The strategically located CFTFs combat cybercrime through prevention, detection, mitigation, and investigation.[18]

1.3. Specialized Prosecution Units

a. Computer Crime and Intellectual Property Section (CCIPS)

The DOJ's Computer Crime and Intellectual Property Section (CCIPS) is responsible for investigating and prosecuting computer crime and intellectual property crime across the United States. Specifically, CCIPS pursues three overarching goals: to deter and disrupt computer and intellectual property crime by bringing and supporting key investigations and prosecutions; to guide the proper collection of electronic evidence by investigators and prosecutors; and to provide technical and legal advice and assistance to agents and prosecutors in the U.S. and around the world.[19] CCIPS executes this mission in a wide variety of ways, including (a) by identifying, supporting, and prosecuting high-impact, cutting-edge, and sensitive investigations and prosecutions; (b) by providing expert legal and technical advice, training, and support to the Department, investigative agencies, and other executive branch agencies; (c) promoting international policy that favors enforcement of computer crime and IP laws abroad, especially through building the capacity of foreign governments to investigate and prosecute; (d) by providing to prosecutors elite-level digital investigative analysis; (e) by advising on and litigating in support of the

[15] *The U.S. Secret Service: History and Missions*, Shaw Reese, Congressional Research Service, June 18, 2014, p. 1.

[16] *Id*., Summary Section.

[17] "*Cyber Investigations, United States Secret Service*", https://www.secretservice.gov/investigation/cyber, accessed August 1, 2022.

[18] *Id*.

[19] "*Computer Crime and Intellectual Property Section (CCIPS), About the Computer Crime & Intellectual Property Section*", https://www.justice.gov/criminal-ccips, accessed August 1, 2022.

lawful collection of electronic evidence; and (f) by developing and advocating for computer and intellectual property crime policies and legislation.[20]

CCIPS is also the U.S. point of contact for the Budapest Convention 24/7 digital evidence sharing network and the G724/7 High Tech Crime Network. Besides, CCIPS represents the U.S. Government at the Council of Europe in issues relating to the Budapest Convention, at UN Expert meetings and at the G7 High Tech Crime Working Group. Within CCIPS, there is an embedded digital forensic laboratory with 15 digital forensic analysts who provide forensic and technical consultation, research, and training.

b. CHIPs

In addition to the CCIPS, there are over 250 Computer Hacking and Intellectual Property (CHIP) prosecutors stationed with the 93 U.S. Attorney's Offices across the U.S. CHIP prosecutors are responsible for coordinating cybercrime and intellectual property prosecutions, training their fellow prosecutors on cybercrime, serving as points of contact for law enforcement concerning incident response and digital evidence search warrants, and providing outreach to the private sector and the public concerning cybercrime and intellectual property offenses.

1.4. Task Forces and International Cybercrime Programs

a. International Computer Hacking and Intellectual Property Attorney Advisor Program (ICHIP)

The U.S. Transnational and High-Tech Crime Global Law Enforcement (GLEN) program is the result of a partnership between the U.S. Department of State, Bureau of International Narcotics and Law Enforcement Affairs (DOS/INL) and CCIPS and Office of Overseas Prosecutorial Development, Assistance and Training (DOJ/OPDAT).[21]

GLEN is a worldwide law enforcement capacity building network of ICHIP attorney advisors, computer forensic analysts and federal law enforcement agents who deliver training and technical assistance to foreign law enforcement, prosecutorial, and judicial partners to combat intellectual property and cybercrime activity, as well as to assist in the collection and use of electron-

[20] *Id*.

[21] "*Global Cyber and Intellectual Property Crimes: U.S. Transnational and High-Tech Crime Global Law Enforcement Network (GLEN),* Updated April 29, 2022, https://www.justice.gov/criminal-opdat/global-cyber-and-intellectual-property-crimes , accessed August 1, 2022.

ic evidence to combat all types of crime, including transnational organized crime. The objective of GLEN is to promote the rule of law and to protect Americans from criminal threats emanating from abroad by delivering targeted training to encourage both immediate assistance as well as long-term institutional change. This assistance includes training workshops, legislative review, case-based mentoring, skills development, and promoting institutional reform, such as the formation of specialized units to address these criminal threats.[22]

The ICHIP program began in 2013 and since then funding has increased to include 12 attorney advisors, with a thirteenth to be deployed in 2022, two global cyber forensic advisors or GCFAs, and two investigators.[23] The current ICHIP Attorney Advisors are located in Sao Paulo, Panama City, Bucharest, The Hague, Zagreb, Abuja, Addis Ababa, Hong Kong, Kuala Lumpur, Bangkok and two global subject matter experts based in Washington, DC.[24]

The mission of the ICHIP program is to assess the capacity of law enforcement authorities throughout the region to enforce intellectual property rights (IPR) and combat cybercrime; develop and deliver training designed to enhance the capacity of justice sector personnel to enforce IPR and combat cybercrime; assist in developing or strengthening institutions dedicated to enforcing IPR and combatting cybercrime; monitor regional trends in IPR protection and computer crimes; and provide expert assistance in support of the United States' IPR and cybercrime policies and initiatives in the region.[25]

b. FBI Cyber Assistant Legal Attachés

Another way that the U.S. is combatting cyber threat is by placing FBI cyber experts in FBI legal attaché (LEGAT) offices in strategic locations around the globe.[26] These experts are called Cyber Assistant Legal Attachés, or Cyber ALATs, and they work on a daily basis with law enforcement in host countries, sharing information, cooperating on investigations, and enhancing our relationships overall.[27] Sometimes, they even work in the same physical space alongside their foreign counterparts.[28] The Cyber ALAT program began in

[22] *Id*.

[23] *Id*.

[24] *Id*.

[25] "*Overseas Work: International Computer Hacking and Intellectual Property (ICHIP) Network*", May 2, 2022, https://www.justice.gov/criminal-ccips/overseas-work, accessed August 1, 2022.

[26] "*National Cyber Security Awareness Month: FBI Deploys Cyber Experts to Work Directly with Foreign Partners*", October 26, 2016, https://www.fbi.gov/news/stories/fbi-deploys-cyber-experts-to-work-directly-with-foreign-partners, accessed August 1, 2022.

[27] *Id*.

[28] *Id*.

2011, when several FBI Cyber Division personnel were deployed to a handful of LEGAT offices to address significant cyber threats in those regions impacting U.S. interests and FBI investigations.[29] The host nation also benefits from the presence of a cyber ALAT in the way of technical assistance offered in support of cyber investigations as well as information-sharing efforts that often eliminate the duplication of resources expended to investigate the same threat actor groups.[30] Cyber ALATs also facilitate requests from foreign partners for cyber training.[31]

c. National Cryptocurrency Enforcement Team

One of the more recent efforts to address the challenges of cryptocurrencies and digital assets was the establishment of the National Cryptocurrency Enforcement Team (NCET) within the U.S. DOJ in 2021. The role of NCET is to tackle complex investigations and prosecutions of criminal misuses of cryptocurrency, particularly crimes committed by virtual currency exchanges, mixing and tumbling services, and money laundering infrastructure actors.[32] NCET also assists in the tracing and recovery of assets lost to fraud and extortion, including cryptocurrency payments to ransomware groups. The NCET team is comprised of federal prosecutors from a variety of specialized units, including the Money Laundering and Asset Recovery Section (MLARS), CCIPS and other detailees to the Criminal Division from various U.S. Attorney's Offices across the U.S.[33]

d. Ransomware Task Force

Shortly after the Colonial Pipeline ransomware attack, the DOJ launched the Ransomware and Digital Extortion Task Force (Task Force).[34] A central goal of the Task Force is to ensure that the efforts in combating ransomware and digital extortion are focused, coordinated and appropriately resourced.[35] The Task Force includes, but is not limited to, the United States Attorneys'

[29] *Id*.

[30] *Id*.

[31] *Id*.

[32] "*Deputy Attorney General Lisa O. Monaco Announces National Cryptocurrency Enforcement Team*", October 6, 2021, https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-national-cryptocurrency-enforcement-team, accessed August 1, 2022.

[33] *Id*.

[34] Memorandum For Heads of Department Litigating Components, All United States Attorneys, Federal Bureau of Investigation, Office of the Deputy Attorney General, U.S. Department of Justice, April 20, 2021, accessed at: DOJ.Memo_.Taskforce/042021 on August 1, 2022.

[35] Memorandum For All Prosecutors, Office of the Deputy Attorney General, U.S. Department of Justice, June 3, 2021, accessed at: Guidance Regarding Investigations and Cases Related to Ransomware and Digital Extortion.

Offices, CCIPS, MLARS, NSD, and FBI and is responsible for coordinating and tracking any ransomware investigations as outlined by the Deputy Attorney General in a Memorandum of the Deputy Attorney General published in June 2021.[36]

e. National Cyber-Forensics and Training Alliance

The National Cyber-Forensics and Training Alliance (NCFTA) was established in 2002 as a non-profit partnership between private industry, government, and academia for the sole purpose of providing a neutral, trusted environment that enables two-way collaboration and cooperation to identify, mitigate, and disrupt cybercrime.[37] NCFTA provides insight into the scope and impact of the threat to law enforcement and shares critical and real-time information. From the period of 2015 to 2021, NCFTA has prevented financial losses in the amount of $12.25 billion, enabled $178 million seizures by law enforcement, produced 26,945 intelligence reports, referred 4,184 cases to law enforcement, and contributed to 1,179 law enforcement arrests.[38]

f. The National Center for Missing and Exploited Children

The National Center for Missing and Exploited Children's (NCMEC) CyberTipline is the nation's centralized reporting system for the online exploitation of children. It was founded in 1998. The public and electronic service providers can make reports of suspected online enticement of children for sexual acts, child sexual molestation, child sexual abuse material, child sex tourism, child sex trafficking, unsolicited obscene materials sent to a child, misleading domain names, and misleading words or digital images on the internet.[39] NCMEC staff review each tip and work to find a potential location for the incident reported so that it may be made available to the appropriate law-enforcement agency for possible investigation.[40]

In 2021, NCMEC's CyberTipline received 29.3 million reports of suspected child sexual exploitation, an increase of 35% from 2020. In 2020, there were 21,751,085 reports, increasing in 2021 to 29,397,681. Reports to the CyberTipline included 85 million files, out of which 44,856,209 were video, 39,393,298 images and 196,228 others. NCMEC alerted law enforcement to over 4,260 potential new child victims. Reports regarding CSAM, legally referred to as child pornog-

[36] *Id*.

[37] "*The National Cyber-Forensics and Training Alliance (NCFTA)*", https://www.ncfta.net/, accessed August 1, 2022.

[38] *Id*. *Id*.

[39] "*Overview: National Center for Missing & Exploited Children, CyberTipline*", https://www.missingkids.org/gethelpnow/cybertipline, accessed August 1, 2022.

[40] *Id*.

raphy, make up the largest reporting category. Over 99% of the reports received by the CyberTipline in 2021 regarded incidents of suspected CSAM.[41]

2. SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS

2.1. Federal Rule of Criminal Procedure 41(e)(2)(B)

The Federal Rules of Criminal Procedure (Fed.R.Crim.Pro.) govern how federal criminal prosecutions are conducted in U.S. District Courts, which are the general trial courts at the federal level.

Rule 41(e)(2)(B) governing the issuing of a search warrant stipulates that this type of warrant enables the seizure of electronic storage media or the seizure or copying of electronically stored information. Additionally, unless otherwise specified, a search warrant issued under this rule specifically authorizes law enforcement to review seized data at a later stage under the condition that it is consistent with the warrant. However, the execution of the warrant itself refers to the seizure or on-site copying of the media or information, and not to any later off-site copying or review.

In other words, computers and other electronic storage media commonly contain such large amounts of information that it is often impractical for law enforcement to review all the information during execution of the warrant at the search location.[42] This rule acknowledges the need for a two-step process: officers may seize or copy the entire storage medium and review it later to determine what electronically stored information falls within the scope of the warrant.[43]

2.2. The Stored Communications Act and the Electronic Communications Privacy Act

The Electronic Communications Privacy Act and the Stored Wire Electronic Communications Act are commonly referred to together as the Electronic Communications Privacy Act (ECPA) of 1986.[44] ECPA, as amended,

[41] *Id*.

[42] *Advisory Committee on Rules of Criminal Procedure*, Washington D.C., April 6-7, 2009, p. 114., available at: https://www.uscourts.gov/rules-policies/archives/agenda-books/advisory-committee-rules-criminal-procedure-april-2009, accessed August 1, 2022.

[43] *Id*.

[44] 18 U.S.C. §§ 2510-2523, Electronic Communications Privacy Act.

protects wire, oral, and electronic communications while those communications are being made, while they are in transit, and when they are stored on computers. The Act applies to email, telephone conversations, and data stored electronically.

The ECPA has three titles. Title I of the ECPA, which is often referred to as the Wiretap Act, prohibits intentional actual or attempted interception, use, disclosure, or "procure[ment] [of] any other person to intercept or endeavor to intercept any wire, oral, or electronic communication". Title I also prohibits the use of illegally obtained communications as evidence.[45] Title II of the ECPA, which is called the Stored Communications Act (SCA), protects the privacy of the contents of files stored by service providers and of records held about the subscriber by service providers, such as subscriber name, billing records, or IP addresses.[46] Title III of the ECPA, which addresses pen register and trap and trace devices, requires government entities to obtain a court order authorizing the installation and use of a pen register (a device that captures the dialed numbers and related information to which outgoing calls or communications are made by the subject) and/or a trap and trace (a device that captures the numbers and related information from which incoming calls and communications coming to the subject have originated).[47]

2.3. Obtaining Subscriber, Traffic and Content Data

Specifically, §§2701-2712 of the ECPA regulate how the government can obtain stored account information from network service providers such as ISPs.[48] Whenever agents or prosecutors seek stored email, account records, or subscriber information from a network service provider, they must comply with the ECPA.[49] § 2703 creates a code of criminal procedure that federal and state law enforcement officers must follow to compel disclosure of stored communications from network service providers.[50] § 2702 regulates voluntary disclosure by network service providers of customer communications and records, both to government and non-government entities.[51] §2701 prohibits unlawful access to certain stored communications; anyone who obtains, alters,

[45] 18 U.S.C. § 2515.

[46] 18 U.S.C. §§ 2701-12.

[47] 18 U.S.C. §§ 3121 – 3127.

[48] *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*; Computer Crime and Intellectual Property Section (CCIPS), Office of Legal Education, Executive Office for United States Attorneys, 2009., p. 115.

[49] *Id.*

[50] *Id.*

[51] *Id.*

or prevents authorized access to those communications is subject to criminal penalties.[52]

When agents and prosecutors wish to obtain information relating to an individual customer or subscriber, they must be able to classify these types of information using the language of the SCA.[53] The SCA breaks the information down into three categories: (1) contents; (2) non-content records and other information pertaining to a subscriber or customer; and (3) basic subscriber and session information, which is a subset of non-content records and is specifically enumerated in 18 U.S.C. § 2703(c)(2). [54]

Section 2703(c)(2) lists the categories of basic subscriber and session information: (A) name; (B) address; (C) local and long distance telephone connection records, or records of session times and durations; (D) length of service (including start date) and types of service utilized; (E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and (F) means and source of payment for such service (including any credit card or bank account number). In general, the items in this list relate to the identity of a subscriber, his relationship with his service provider, and his basic session connection records.[55]

Section 2703(c)(1) covers a second type of information: "a record or other information pertaining to a subscriber or to a customer of such service (not including the contents of communications". This is a catch-all category that includes all records that are not contents, including basic subscriber and session information described in the previous section.[56] As one court explained, "a record means something stored or archived. The term information is synonymous with data".[57] Common examples of "record[s] . . . pertaining to a subscriber" include transactional records, such as account logs that record account usage; cell-site data for cellular telephone calls; and email addresses of other individuals with whom the account holder has corresponded.[58]

The contents of a network account are the actual files (including email) stored in the account.[59] Pursuant to 18 U.S.C. § 2510(8), "contents", when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication.[60] For example, stored emails or voice mails are "contents", as are word

[52] *Id*.
[53] *Supra* note 48, p. 121.
[54] *Id*.
[55] *Id*.
[56] *Supra* note 48, p. 122.
[57] *In re United States,* 509 F. Supp. 2d 76, 80 (D. Mass. 2007).
[58] *Supra* note 48, p. 122.
[59] *Id*.
[60] *Supra* note 48, p. 123.

processing files stored in employee network accounts. The subject lines of emails are also contents.[61]

Moreover, Section 2703 articulates the steps that the government must take to compel providers to disclose the contents of stored wire or electronic communications (including email and voice mail) and other information such as account records and basic subscriber and session information.[62] Section 2703 offers five mechanisms that a "government entity" can use to compel a provider to disclose certain kinds of information. The five mechanisms are as follows: subpoena; subpoena with prior notice to the subscriber or customer; § 2703(d) court order; § 2703(d) court order with prior notice to the subscriber or customer; and a search warrant.[63] Finally, providers of services not available "to the public" may freely disclose both contents and other records relating to stored communications.[64]

2.4. Federal Rules of Evidence 902 (13-14) and 1001(d)

2.4.1. Federal Rules of Evidence

The Federal Rules of Evidence (FRE) are a set of rules that governs the introduction of evidence at civil and criminal trials in federal courts.[65] On December 1, 2017, the FRE was amended to provide two new rules to clarify the procedures for authenticating electronic evidence in federal courts and to provide new procedures to save time and money for the parties when there is no dispute about authenticity. Specifically, FRE 902(13) and (14) read as follows:

> "**Rule 902(13): Certified Records Generated by an Electronic Process or System**. A record generated by an electronic process or system that produces an accurate result, as shown by a certification of a qualified person that complies with the certification requirements of Rule 902(11) or (12). The proponent must also meet the notice requirements of Rule 902(11)."[66]
> "**Rule 902(14): Certified Data Copied from an Electronic Device, Storage Medium, or File.** Data copied from an electronic device, storage medium, or file, if authenticated by a process of digital identification, as shown by a certification of a qualified person that complies with the certification

[61] *Id*.
[62] *Supra* note 48, p. 127.
[63] *Id*.
[64] *Supra* note 48, p. 135.
[65] Fed. R. Evid., 2022 Edition. Available at: https://www.rulesofevidence.org.
[66] Fed. R. Evid. 902(13).

requirements of Rule 902(11) or (12). The proponent also must meet the notice requirements of Rule 902(11)."[67]

The first provision allows self-authentication of machine-generated information, upon the submission of a certificate prepared by a qualified person,[68] such as the contents of a website or data generate by an app. The second rule provides a similar certification procedure for a copy of data taken from an electronic device, media or file,[69] such as a mobile phone or hard drive. Without 902(14), the government would usually have to call two witnesses – first, the technician who made the forensic copy of a phone who would need to testify about making it and the methodology he used to verify that the copy was an exact copy of information inside the phone, and second, the technician who then performed the forensic examination of the copy itself. With Rule 902(14), the government now needs only to obtain the first technician's certification of the facts establishing how he copied the information and verified that the copy was true and accurate and then call the other technician who performed the forensic examination.[70]

3. PROSECUTING COMPUTER CRIMES

3.1. Computer Fraud and Abuse Act

The Computer Fraud and Abuse Act (CFAA) was enacted in 1986, as an amendment to the first federal computer fraud law, to address criminal computer intrusions. In addition to amending a number of the provisions in the original section 1030, the CFAA also criminalized additional computer-related acts. Congress addressed federalism concerns in the CFAA by limiting federal jurisdiction to cases with a compelling federal interest – i.e. where computers of the federal government or certain financial institution are involved or where the crime itself is interstate in nature.[71]

[67] Fed. R. Evid. 902(14).

[68] EV2015-04, Advisory Committee on Evidence Rules, Minutes of the Meeting of April 17, 2015, New York, New York, p. 8., accessed August 1, 2022.

[69] *Id*.

[70] "*How Two New Rules for Self-Authentication Will Save You Time and Money*", John M. Haried, Duke University School of Law, p. 39, available at: https://judicature.duke.edu/articles/how-two-new-rules-for-self-authentication-will-save-you-time-and-money/

[71] *Prosecuting Computer Crimes Manual*; Computer Crime and Intellectual Property Section (CCIPS), Criminal Division, Office of Legal Education, Executive Office for United States Attorneys, 2010.

The current version of the CFAA includes seven types of criminal activity: obtaining national security information, accessing a computer and obtaining information, trespassing in a government computer, accessing a computer to defraud and obtain value, intentionally damaging by knowing transmission, recklessly damaging by intentional access, negligently causing damage and loss by intentional access, trafficking in passwords and extortion involving computers.[72] The law prohibits accessing a computer without authorization, or in excess of authorization. The only computers, in theory, covered by the CFAA are defined as "protected computers". They are defined under section 18 U.S.C. § 1030(e)(2) to mean a computer. Two terms are thus key: "protected computer" and "authorization".

The term "protected computer", 18 U.S.C. § 1030(e)(2), is a statutory term of art that has nothing to do with the security of the computer. In a nutshell, "protected computer" covers computers used in or affecting interstate or foreign commerce and computers used by the federal government and financial institutions. Several of the criminal offenses in the CFAA require that the defendant access a computer "without authorization". Others require that the defendant "exceeds authorized access". The term "without authorization" is not defined by the CFAA. The legislative history of the CFAA reflects an expectation that persons who exceed authorized access will be insiders, while persons who access a computer without authorization will typically be outsiders. However, insiders who are authorized to access a computer face criminal charges only if they intend to cause damage to the computer and not for recklessly or negligently causing damage. In contrast, outside intruders who break into a computer could be punished for any intentional, reckless, or other damage they cause by their trespass.

3.2. Other Network Crime Statutes

Other Network Crime Statues include Unlawful Access to Stored Communications: 18 U.S.C. §2701, Identity Theft: 18 U.S.C. §1028(a)(7), Aggravated Identity Theft: 18 U.S.C. §1028A, Access Device Fraud: 18 U.S.C. §1029, CAN-SPAM Act: 18 U.S.C. §1037, Wire Fraud: 18 U.S.C. §1343 and Communication Interference: 18 U.S.C. §1362.

Section 2701 focuses on protecting email and voicemail from unauthorized access and thereby protects the confidentiality, integrity, and availability of these communications stored by providers of electronic communications

[72] *Id*., p. 3.

services pending the ultimate delivery to their intended recipients.[73] Section 1028A applies when a defendant knowingly transfers, possesses or uses without lawful authority a means of identification of another person during and in relation to any felony violation of certain enumerated federal offenses. In other words, this section is often applicable in the context of computer crime. 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 emails, often violate Section 1029, a predicate crime for a section 1028A charge. Prosecutors commonly bring charges under Section 1029 in many types of phishing cases, where a defendant uses fraudulent emails to obtain bank account numbers and passwords, and "carding" cases, where a defendant purchases, sells or transfers stolen bank account, credit card, or debit card information. Penalties for violations of Section 1029 range from a maximum of 10 or 15 years of imprisonment depending on the subsection violated.

The CAN-SPAM Act of 2003 also provides a means for prosecuting those responsible for sending large amounts of unsolicited commercial email (a.k.a. spam), 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. Another particularly powerful and commonly applicable charge in network crime cases is wire fraud under Section 1343. This section is also a predicate for RICO and money laundering charges. Finally, Section 13622 which prescribes communication interference can provide an alternative charge where a compromised computer is owned or used by the United States for communication purposes.

3.3. Cryptocurrency Related Crime and Seizure of Cryptocurrency

3.3.1. Cryptocurrencies

On June 6, 2022, the DOJ issued a report on cryptocurrencies.[74] The report focuses on the criminal misuse of digital assets, the most common of which are cryptocurrencies, the challenges arising in the international investigation of crimes related to digital assets and recommendations to improve international cooperation in detecting, investigating, and prosecuting criminal activity related to digital assets. Digital assets are used to further a variety of

[73] *Supra* note 71, p. 89.

[74] The Report of the Attorney General Pursuant to Section 8(b)(iv) of Executive Order 14067: How to Strengthen International Law Enforcement Cooperation For Detecting, Investigating And Prosecuting Criminal Activity Related to Digital Assets; Office of the Attorney General, Department of Justice, Washington D.C., 2022.

different types of criminal activity, which include, but are not limited to, the following types of crime: money laundering, ransomware, fraud and theft, narcotics trafficking, human trafficking, terrorism trafficking, sanctions evasion and tax evasion.

U.S. law enforcement and regulatory agencies have taken steps to address the challenges posed by this new technology, including the development and sharing of expertise with foreign counterparts, participation in international standard-setting for a, and other U.S. government efforts to combat illicit use of digital assets.[75]

The DOJ has also had some notable successes in disrupting ransomware activities over the last year, including the recovery of approximately $2.3 million in cryptocurrency paid as ransom by those responsible for the DarkSide ransomware incident targeting Colonial Pipeline.[76] The DOJ also announced charges against individuals suspected of deploying Sodinokibi/REvil ransomware against victim companies, including the arrest of the individual charged with the ransomware attack against Kaseya, a multinational information technology software company, as well as the seizure of $6.1 million in cryptocurrency paid in ransom to the group.[77] The largest financial seizure of the DOJ ever was earlier this year in the Bitfinex Hack case of 2016, when two individuals were arrested for alleged conspiracy to launder $4.5 billion in stolen cryptocurrency. The DOJ seized over $3.6 billion worth of stolen Bitcon (94,000 Bitcoins). It is the DOJ's biggest seizure of cryptocurrency ever and the largest single financial seizure in the department's history.

Furthermore, digital assets and the exchanges trading them can offer opportunities for criminals to launder their illicit proceeds.[78] The 2022 Crypto Crime Report from Chainalysis estimates that cybercriminals have laundered over $33 billion worth of cryptocurrency since 2017.[79] Even more, narcotics trafficking and other controlled substances remain available at the darknet marketplaces, whereby the most popular payment medium of exchange is cryptocurrency. Human traffickers have also increasingly turned to cryptocurrency to promote illegal sex services and to launder their profits, although cryptocurrency is one of several payment options. The financing of terrorism

[75] *Id*., p. 9.

[76] "*Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside*", Press Release, June 7, 2021, https://www.justice.gov/opa/pr/departmentjustice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside, accessed August 1, 2022.

[77] "*Ukrainian Arrested and Charged with Ransomware Attack on Kaseya*", Press Release, November 8, 2021, https://www.justice.gov/opa/pr/ukrainian-arrested-and-charged-ransomware-attack-kaseya, accessed August 1, 2022.

[78] *Supra* note 74, p. 21.

[79] Chainalysis, The 2022 Crypto Crime Report, Feb. 2022, p. 11.

is not immune to crypto as well. The global and distributed nature of digital asset platforms has also enabled terrorists to make peer-to-peer transfers to members of their organizations, circumventing the AML/CFT controls found in more traditional payment methods. Finally, the rise in the use of cryptocurrencies has provided additional avenues for tax evasion. Individuals and businesses are required by U.S. law to report income received in cryptocurrency on their tax returns. Criminals are also increasingly using cryptocurrencies to hide the profits of their criminal schemes from tax authorities.[80]

3.3.2. Seizure and Forfeiture

Seizure and forfeiture of criminal proceeds in the form of cryptocurrencies is a powerful tool and advances the government's mission to help restore property to victims, punish and deter wrongdoers, and deprive illicit organizations of their ill-gotten gains.[81]

Overall, there are three forms of forfeiture under U.S. law – administrative, criminal judicial, and civil judicial.[82] The forfeiture of any asset, including cryptocurrency, must be authorized under a federal statute; there is no common law of forfeiture.[83] There is no single statute or place in the federal code that authorizes all forfeitures.[84] Rather, forfeiture law is a patchwork of numerous and often interdependent provisions.[85] Fortunately, the crimes that prosecutors are likely to encounter in cases involving cryptocurrency offer powerful forfeiture authority. These include wire and mail fraud, which allows the forfeiture of the "proceeds" of the crime; drug trafficking, which allows the forfeiture of the proceeds and property that facilitated the crime; and money laundering, which allows the forfeiture of all property "involved in" the crime.[86] Thus, though prosecutors may be aware of the different manners in which various governmental entities classify cryptocurrency –such as a "commodity" or "security" – those distinctions should have no bearing on the forfeitability of cryptocurrency *per se*.

Specifically with regards to seizure, investigators may seize cryptocurrency with a search warrant that provides authority to seize cryptocurrency, a for-

[80] Supra note 74, p. 24.

[81] *Forfeiting Cryptocurrency: Decrypting the Challenges of a Modern Asset*; Neal B. Christiansen and Julia E. Jarrett, Asset Forfeiture and Money Laundering, Department of Justice, Journal of Federal Law and Practice, Volume 67, 2019, p. 156.

[82] *Id*., p. 161.

[83] *Id*., p. 160.

[84] *Id*., p. 160.

[85] *Supra* note 81, p. 160.

[86] *Supra* note 81, p. 160.

feiture seizure warrant, or another method that otherwise comports with the government's obligations under the Fourth Amendment (for example, seizing cryptocurrency with the owner's consent).[87] When seizing cryptocurrency via a search warrant, the supporting affidavit should establish probable cause that the cryptocurrency is located at the place to be searched and has the requisite nexus to the relevant criminal activity.[88] Attachments must provide explicit authority for the United States to transfer seized cryptocurrency to a government-controlled wallet.[89] It is the location of the cryptocurrency that will determine the seizure method. Cryptocurrency can be held in three ways: locally, i.e. a target stores their private keys on paper or hardware in their possession; in a wallet hosted by a U.S. registered exchange and, finally, in a wallet that is hosted, or whose private keys are otherwise located outside the U.S.

In advance of seizure, seizing agencies have already set up wallets for the storage of seized cryptocurrency and they typically set up one or more wallet for each seizure.[90] Regardless of the cryptocurrency wallet type, upon seizure the cryptocurrency should be immediately transferred to the agency-controlled wallet. It is best practice to conduct the transfers using a clean computer, meaning a dedicated, password-protected computer that has not been connected to the DOJ or agency networks. The cryptocurrency should be held in "cold storage" wallets – that is, wallets that are not connected to the internet, for example an encrypted, offline device – until it is transferred to a U.S. Marshals Service (USMS)-controlled wallet.[91] The USMS provides cryptocurrency storage and disposition services for all federal agencies – including those who do not participate in the Asset Forfeiture Fund and therefore typically store and dispose of assets independently. Finally, it is important to mention that the policy of the DOJ is to keep the assets in the same form as they were at seizure and not liquidate them until a final order of forfeiture is entered or an administrative forfeiture is complete.[92] However, there exists an exception to the rule, and that is the possibility of a so-called "interlocutory order", whereby a prosecutor files a motion with the court to allow early sale under the Federal Rules of Criminal Procedure 32.2(b)(7), if all parties with a potential ownership interest in the cryptocurrency agree to sell seized cryptocurrency while awaiting trial or sentencing.[93]

[87] Asset Forfeiture Policy Manual (2021), Chapter 2, Section V.B.
[88] *Supra* note 81, p. 171.
[89] *Supra* note 81, p. 171.
[90] *Supra* note 81, p. 177.
[91] *Supra* note 81, p. 178.
[92] *Supra* note 87.
[93] *Supra* note 81, p. 178.

3.4. Sentencing

The United States Sentencing Guidelines (Guidelines) are used by federal judges to craft consistent and appropriate sentences as they are only advisory rather than mandatory.[94]

The Guidelines treat many cyber-enabled crimes such as ransomware, business email compromise fraud, and other computer-enabled frauds as basic economic offenses for which U.S.S.G. § 2B1.1 determines an offender's sentence.[95] An offense sentenced under this section is usually assigned a base offense level of six. After determining the base offense level, prosecutors must determine whether any specific offense characteristics and adjustments may apply.[96] The base offense level is increased based on the level of monetary loss the defendant caused according to a specifically prescribed loss table. For example, if the defendants caused the loss of (in other words stole) more than $200,000, the increase will be to 12. If the defendant is found responsible for more than $5,000 of economic damage, the increase will be 2. The government bears the burden of proving the amount of loss by a preponderance of evidence.[97] Courts are not required to precisely determine the amount of loss attributable to a defendant. Rather, the court need only make a reasonable estimate of the loss. [98]

Furthermore, section 2B1.1 imposes a graduated increase in offense level based on the number of victims that suffered actual loss as a result of the offense. If the offense causes loss to ten or more victims, the offense level is increased by two and if it causes loss to 250 or more victims, the offense level is increased by six. This specific offense characteristic may be particularly important in network crimes, such as the propagation of worms or viruses, crimes that, by their very nature, involve a large number of victims.[99] It is also worth mentioning that extraterritorial conduct is a base for an increase, which means that if a substantial part of a fraudulent scheme was committed from outside the United States, the sentencing court should increase the base offense level by two levels or if such an increase does not result in an offense level of at least twelve to twelve. The use of sophisticated means, trafficking in access devices, the risk of death or injury, the intent to obtain private information, intentional damage, and violations that involve critical infrastructure also result in an increase in the defendant's offense level.[100]

---

[94] *Supra* note 71, p. 131.

[95] *Supra* note 71, p. 131.

[96] *Supra* note 71, p. 132.

[97] *United States v. Jackson*, 155 F.3d 942, 948 (8th Cir. 1998).

[98] 4th Cir. U.S.S.G. § 2B1.1, cmt.n.3(C); *Elliott v United States*, 332 F.3d 753, 766 (4th Cir. 2003).

[99] *Supra* note 71, p. 136.

[100] *Supra* note 71, p. 132-142.

For example, if a violation of 18 U.S.C. §1030(a)(3) occurs, i.e. an intrusion into a computer, the application of sentencing Guideline §2B2.3 which governs trespass would apply. Namely, 18 U.S.C. §1030(a)(3) defines that whoever intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency which is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States, and such conduct affects that use by or for the Government of the United States. The maximum punishment under the statute is imprisonment for not more than ten years.[101]

Specifically, Guideline §2B2.3 governs trespass where the base offense level is 4 (four). The offense level is increased by two if the trespass occurred on a computer system used to maintain or operate a critical infrastructure, or by or for a government entity in furtherance of the administration of justice, national defense, or national security.[102]

4. CONCLUSION

As the U.S. law enforcement community and the U.S. Department of Justice evolve to meet cyber threats, it cannot and does not want to fight these threats alone, as cyber threats do not respect borders.[103] Evolving to match the cyber threats does not only mean new tools and teams within the U.S. Department of Justice — it means finding innovative ways to work with our international partners.[104] Over the last decade, the U.S. has seen a growing threat to government and commercial entities alike in the form of cyber-attacks originating from a wide array of players: foreign intelligence services, criminal groups, hacktivists, and insider threats.[105] The attacks have grown in sophistication, ranging from exploiting systemic weaknesses in authentication architecture,

[101] 18 U.S. Code § 1030 - Fraud and Related Activity in Connection with Computers.

[102] United States Sentencing Commission, Guidelines Manual, §3E1.1 (Nov. 2011), Chapter Two, Part B-Basic Economic Offenses, 2. Burglary and Trespass, §2B2.3 – TRESPASS, available at: https://guidelines.ussc.gov/gl/%C2%A72B2.3.

[103] "Deputy Attorney General Lisa O. Monaco Delivers Remarks at Annual Munich Cyber Security Conference: Remarks as Delivered", February 17, 2022, https://www.justice.gov/opa/speech/deputy-attorney-general-lisa-o-monaco-delivers-remarks-annual-munich-cyber-security, accessed August 1, 2022.

[104] *Id*.

[105] U.S. Department of Justice Information Technology Strategic Plan for Fiscal Years 2022-2024, U.S. Department of Justice, Office of the Chief Information Officer, June 2022, p. 2-3.

ransomware attacks, social media misinformation, to attacks on supply chains and industrial controls.[106]

To conclude, combating cybercrime and cyber-enabled threats remains among the DOJ's highest priorities as part of its mission to ensure public safety against foreign and domestic threats, and to provide federal leadership in preventing and controlling crime.[107] Looking ahead, the focus is to expand and reinforce a resilient enterprise that is both well-protected from threats and has the mechanisms to rapidly recover from attacks with minimal disruption to mission operations.[108]

REFERENCES

1. *Prosecuting Computer Crimes Manual*; Computer Crime and Intellectual Property Section (CCIPS), Criminal Division, Office of Legal Education, Executive Office for United States Attorneys, 2010.
2. *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*; Computer Crime and Intellectual Property Section (CCIPS), Office of Legal Education, Executive Office for United States Attorneys, 2009.
3. *Report of the Attorney General Pursuant to Section 8(b)(iv) of Executive Order 14067: How To Strengthen International Law Enforcement Cooperation For Detecting, Investigating And Prosecuting Criminal Activity Related To Digital Assets*; Office of the Attorney General, Department of Justice, Washington D.C., 2022.
4. *Forfeiting Cryptocurrency: Decrypting the Challenges of a Modern Asset*; Neal B. Christiansen and Julia E. Jarrett, Asset Forfeiture and Money Laundering, Department of Justice, Journal of Federal Law and Practice, Volume 67, 2019.
5. *Federal Bureau of Investigation's Ability to Address the National Security Cyber Intrusion Threat*; U.S. Department of Justice, Office of the Inspector General, Audit Division, Audit Report 11-22, April 2011.
6. *Report of the Attorney General's Cyber Digital Task Force, Cryptocurrency Enforcement Framework*, Department of Justice, Office of the Deputy Attorney General, October 2020.
7. *Advisory Committee on Rules of Evidence*, New York, NY, April 17, 2015.
8. *2022 Crypto Crime Report*, Chainalysis, February 2022.
9. United States Sentencing Commission, Guidelines Manual, §3E1.1 (Nov. 2011).
10. Asset Forfeiture Policy Manual (2021), Chapter 2, Section V.B.

[106] *Id*.
[107] *Id*.
[108] *Id*.

Sažetak

Thomas Dougherty *
Nevenka Lastrić Đurić **

PRISTUP SJEDINJENIH AMERIČKIH DRŽAVA ISTRAZI I PROGONU KIBERNETIČKOG KRIMINALA I KRIMINALA POVEZANOG S KRIPTOVALUTAMA

Ovaj je rad prije svega sažetak različitih dokumenata koje je objavila Vlada Sjedinjenih Američkih Država (SAD) i pružit će pregled načina na koji SAD pristupa istrazi i progonu kibernetičkog kriminala, tj. onim kaznenim djelima koja se koriste računalnim mrežama ili su usmjerena protiv njih, a koja još nazivamo i računalnim kriminalom. Rad je pritom usmjeren na objašnjavanje istrage i progona kibernetičkog kriminala na federalnoj razini u SAD-u, a ne na državnoj ili lokalnoj. Najprije će biti iznesen pregled nekoliko specijaliziranih istražnih i tužiteljskih jedinica u SAD-u koje su uspostavljene upravo u svrhu borbe protiv kibernetičkog kriminala. Nadalje će biti objašnjene neke od specijaliziranih operativnih skupina i programa vezanih uz kibernetički kriminal koje je uspostavila Vlada SAD-a, a cilj im je pružanje obuke i tehničke pomoći međunarodnim partnerima u pravosudnom sustavu radi jačanja zajedničke borbe protiv kibernetičkog kriminala. U radu će također biti izloženo najvažnije zakonodavstvo SAD-a u području kibernetičkog kriminala, uključujući i zakone koji uređuju pretragu i oduzimanje računala, pribavljanje digitalnih dokaza u kaznenim istragama SAD-a, odredbe Zakona o pohrani komunikacija/Zakona o privatnosti elektroničkih komunikacija, Federalna pravila SAD-a o dokazima te Zakon o računalnoj prijevari i zlouporabi. Konačno, rad će pokriti i pristup SAD-a istrazi i progonu kriminala povezanog s kriptovalutama, kao i pristup Vlade SAD-a oduzimanju kriptovaluta te načinu određivanja kazne u kaznenom postupku.

Ključne riječi: kibernetički kriminal, digitalni dokazi, kriptovalute, progon, istraga

* Thomas Dougherty savezni je tužitelj u Ministarstvu pravosuđa SAD-a i trenutačno služi mandat kao regionalni pravni savjetnik Ureda za međunarodno računalno hakiranje i intelektualno vlasništvo (ICHIP) za srednju, istočnu i južnu Europu u Veleposlanstvu SAD-a u Zagrebu. Prije svog mandata u Zagrebu g. Dougherty osnovao je 2015. prvi ured ICHIP-a za kibernetički kriminal u Kuala Lumpuru u Maleziji. Dok je bik federalni tužitelj u SAD-u od 2007. do 2014., g. Dougherty radio je na brojnim slučajevima kibernetičkog kriminala na federalnim sudovima diljem SAD-a. doughertyts@state.gov

** Nevenka Lastrić Đurić radi kao pravna savjetnica Ministarstva pravosuđa Sjedinjenih Američkih Država pri Veleposlanstvu SAD-a u Zagrebu. Magistrirala je na Pravnom fakultetu u Zagrebu, a nakon toga je završila i poslijediplomski studij međunarodnog prava (LL. M.) u Washingtonu, D.C., na American University, Washington College of Law. duricn@state.gov; ORCID iD: https://orcid.org/0000-0001-5343-8426