The CYBERSECURITY LAW REPORT

www.cslawreport.com Volume 3, Number 15 July 26, 2017

CYBER THREAT TYPES

International Law Playing Cybersecurity Catch-Up (Part Two of Two)

By Seth D. Rothman and Andreas S. Baum
Hughes Hubbard & Reed LLP

Cybersecurity is a pressing concern for nation states around the globe, as well as for the private and public entities within them. International law has been slow to keep pace and is only just starting to specifically address cybersecurity. To fill the void, governments have been trying to apply existing laws to cover cybersecurity, specifically in the areas of (1) cyberwarfare; (2) laws relating to cyber crimes; and (3) laws that regulate business. This is a challenge, especially as the threats and technology continue to evolve. And within certain jurisdictions, the E.U., for example, transformative legislation covering privacy and security is being implemented.

See also "Prosecuting Borderless Cyber Crime Through Proactive Law Enforcement and Private Sector Cooperation" (Mar. 2, 2016).

Cyber Crime

Although there is no agreed-upon definition of cyber crime, it generally refers to any criminal activity that involves a computer or a digital network. The computer or the network may be used to commit the crime or may be the target of the crime. INTERPOL, the international police organization, distinguishes between "advanced cybercrime," sophisticated attacks against computer hardware and software, and "cyber-enabled crime," traditional crimes that have "taken a new turn with the advent of the internet, such as crimes against children, financial crimes and even terrorism."[1]

However it is defined, cyber crime is a global problem. In March 2010, Spanish and Slovenian investigators arrested the creators of the Mariposa botnet, a computer virus estimated to have infected more than 12 million computers in 190 countries.[2] In January 2017, Lloyd's Bank had to engage in a "cat-and-mouse game across the planet" to geo-block a cyber attack.[3] And the infamous Russian Business Network purportedly provides hosting services and internet access to large-scale criminal operations that operate throughout the world. It is no wonder that by 2019 cyber crime is expected to cost the global economy as much as US$2 trillion a year.[4]

Cyber crime is hard to stop, in part because cyber criminals are notoriously difficult to identify and locate.[5] For example, the Russian Business Network "has no legal identity; it is not registered as a company; its senior figures are anonymous, known only by their nicknames. Its websites are registered at anonymous addresses with dummy e-mails. It does not advertise for customers. Those who want to use its services contact it via internet messaging services and pay with anonymous electronic cash."[6] Moreover, as experts have noted, the challenges of identifying, locating, arresting, and prosecuting cyber criminals are compounded by "legal and investigative instruments that are fragmented across jealously but ineffectually guarded national and jurisdictional borders."[7]

See also "In a Candid Conversation, FBI Director James Comey Talks About the 'Evil Layer Cake' of Cybersecurity Threats" (Jun. 3, 2015); and "Comey Discusses Cooperation Among Domestic and International Cybersecurity Law Enforcement Communities" (Jun. 17, 2015).

The Budapest Convention

In 2001, the Council of Europe introduced the first international treaty designed to combat internet and computer crime, the Budapest Convention on

Cybercrime (the Budapest Convention). The Budapest Convention aims to harmonize national laws in favor of "a common criminal policy aimed at the protection of society against cybercrime" by criminalizing certain offenses (Articles 2-11), establishing common procedures among parties (Articles 14-21), and fostering co-operation among States and between States and private industry (Articles 23-35).[8] To date, the Budapest Convention has been ratified by 52 states, including 10 states that are not members of the Council of Europe.[9] Non-member signatories include, among others, the United States, Canada, Australia, Japan, and Israel.[10]

Articles 2 through 11 of the Convention are aimed at eliminating safe havens for cyber criminals. These articles require member states to criminalize certain enumerated activities, such as illegal access, illegal interception, data interference, system interference, misuse of devices, computer-related forgery, computer-related fraud, offenses related to child pornography, offenses related to infringements of copyright and related rights and attempts and aiding or abetting any of the previous offenses.[11]

Articles 23 through 35 of the Convention establish a framework for cooperation between Convention signatories. These articles provide, among other things, a mechanism for extradition (making the offenses outlined above extraditable, provided that they are punishable under the laws of both Parties concerned "by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty"[12]), general requirements of mutual assistance and specific requirements of mutual assistance in respect of access of stored computer data, collection of traffic data and interception of content data,[13] the spontaneous sharing of information,[14] the expedited preservation of stored computer data,[15] the expedited disclosure of preserved traffic data,[16] and the designation of a point of contact available on a 24-hour, seven-days-a-week basis.[17]

By many accounts, the Budapest Convention is an important achievement that establishes effective international governance over cyber crime.[18] It does, however, have some limitations. Critics have complained that it does not specifically cover identity theft,[19] and that its mutual legal assistance provisions are "too complex, lengthy and resource-intensive to obtain electronic evidence."[20] The Convention is also limited by its membership. China and Russia have refused to join and, even amongst its members, the Council of Europe has noted that "Parties have different views as to whether a Party meets the requirements of the Budapest Convention."[21]

The Budapest Convention is the most widely adopted and comprehensive treaty governing cyber crime. There are, however, other regional frameworks that have also addressed cyber crime, including the 2013 Directive of the European Parliament and of the Council on attacks against information systems.[22]

INTERPOL

INTERPOL is the world's largest international police organization, with 190 member countries. INTERPOL partners with local law enforcement authorities to investigate transnational cyber crimes and, in that respect, further helps to promote cooperation between nation states.[23] With respect to cyber crime, INTERPOL provides:

- operational and investigative support,
- cyber intelligence and analysis,
- digital forensics,
- innovation and research,
- capacity building, and
- national cyber reviews.[24]

In 2014, INTERPOL opened the Global Complex for Innovation (IGCI), a research and development facility in Singapore. IGCI seeks to bring together and leverage cyber expertise from law-enforcement and private-sector partners.[25]

Business Regulation, Data Protection, and Privacy

In addition to cyber warfare and cyber crime, there have also been efforts to regulate cybersecurity in the context of business activit – i.e.,ensuring that businesses take appropriate steps to protect digital information and information systems. These efforts typically take place at the national or regional level,[26] but their effects may extend beyond traditional jurisdictional norms.[27]

See, e.g., "How GE's Global CPO Approaches Shifting Regulations With Dynamic Implications" (Aug. 24, 2016).

The most notable example may be the European Union's Data Protection Directive, which governs the processing of personal data within the European Economic Area (EEA).[28] While the Directive is primarily focused on activities taking place within the European Union, it also covers international data transfers. The Directive provides that, subject to certain exceptions, transfers to third countries may only be made when the third country ensures an adequate level of protection.[29]

"The E.U.'s New Rules: Latham & Watkins Partner Gail Crawford Discusses the Network Information Security Directive and the General Data Protection Regulation" (Jan. 20, 2016).

This restriction on international transfers prompted the negotiation of the E.U.-U.S. Safe Harbor, which allowed U.S. companies to receive data from the E.U. as long as they self-certified with the U.S. Department of Commerce that they adhered to certain data protection principles.[30] In July 2000, the European Commission approved the Safe Harbor program, and it remained in effect for the next 15 years.

On October 6, 2015, the European Court of Justice (ECJ) decided the Schrems case, invalidation the European Commission's decision approving the Safe Harbor program and terminating the Safe Harbor program throughout the EU.[31] The ECJ's decision was the culmination of growing concerns in the E.U. that U.S. companies were unable to keep data private from U.S. law enforcement agencies.[32]

On February 2, 2016, the E.U. Commission and the U.S. Government reached agreement on a replacement program, the E.U.-U.S. Privacy Shield.[33] The Privacy Shield agreement imposes "[s]trong obligations on companies handling Europeans' personal data and robust enforcement," "[c]lear safeguards and transparency obligations on U.S. government access," and "[e]ffective protection of E.U. citizens' rights with several redress possibilities."[34]

See "Key Requirements of the Newly Approved Privacy Shield" (Jul. 20, 2016); "European Data Protection Supervisor Offers Advice on Privacy Shield Review and GDPR Preparation" (May 3, 2017).

The European Union's Data Protection Directive and the successive agreements reached between the E.U. and the United States to facilitate U.S. companies' operations in Europe illustrate some of the challenges that companies and governments face in navigating regulatory requirements that cross state borders. These challenges are only going to increase as stricter regulations are promulgated.

On April 27, 2016, the European Parliament adopted the General Data Protection Regulation (GDPR), which will replace the Directive as of May 25, 2018.[35] The GDPR preserves the principles of the Directive but expands existing protections. In particular, the GDPR will allow national watchdogs to issue significant fines, enshrine the so-called "right to be forgotten" into European law, require companies to inform national regulators within three days of any reported data breach, require parental consent for any children under 16 before using popular social network services, and extend the rules to any company that has customers in the European Union, even if the company is based outside the E.U. [36]

See also, "One Year Until GDPR Enforcement: Five Steps Companies Should Take Now" (May 31, 2017); and

"A Discussion With Ireland's Data Protection Commissioner Helen Dixon About GDPR Compliance Strategies (Part One of Two)" (Mar. 22, 2017); Part Two (Apr. 5, 2017).

Seth Rothman is a litigation partner at Hughes Hubbard & Reed LLP who focuses his practice on complex commercial litigation, arbitration, products liability and mass torts. He has more than 25 years of experience representing clients in courts throughout the country, in arbitrations, and before other tribunals. He has been involved in high-stakes matters on behalf of leading pharmaceutical companies, financial institutions, and multinational corporations. Rothman is co-chair of the firm's Asia Pacific practice group and has significant experience representing Japanese clients in international arbitrations and U.S. litigation. Seth is also co-chair of the firm's data privacy and cybersecurity practice group and co-chair of the eDiscovery Practice Group. In these capacities, he has advised clients on compliance, cybersecurity, data privacy, document management, eDiscovery, and litigation preparedness. He writes and speaks regularly on cybersecurity, data privacy, and eDiscovery.

Andreas S. Baum is an associate in Hughes Hubbard & Reed's Litigation department and a member of the firm's arbitration & alternative dispute resolution practice. Baum worked as an analyst at a boutique strategy consulting firm in Boston, and can apply both technical and business skills to complex issues in litigations and arbitrations. He focuses his practice on international disputes and has extensive experience with issues involving the application of public international law. Before joining Hughes Hubbard & Reed, Baum served as a legal intern at the International Criminal Tribunal for Rwanda, where he assisted in the prosecution of war crimes and crimes against humanity.

The authors are grateful for the assistance of Casey Duffy in preparing this article.

[1] See INTERPOL, Cybercrime, (last visited Feb. 8, 2017).
[2] See Press Release, Federal Bureau of Investigation, FBI, Slovenian and Spanish Police Arrest Mariposa Botnet Creator, Operators (July 28, 2010) (last visited Feb. 8, 2017).
[3] Patrick Collinson, "Lloyds Bank Accounts Targeted in Cybercrime Attack," The Guardian, (Jan. 23, 2017), (last visited Feb. 8, 2017).
[4] See Steve Morgan, "Cybercrime Costs Projected to Reach $2 Trillion By 2019," Forbes, Jan. 17. 2016, (last visited Feb. 8, 2017).
[5] See, e.g., Jonathan Clough, "A World of Difference: The Budapest Convention on Cybercrime and the Challenges of Harmonisation," 40 Monash U. L. Rev. 698, 700 (2014).
[6] A "Walk on the Dark Side," The Economist, Aug. 30, 2007, (last visited Feb. 10, 2017).
[7] Tony L. Putnam and David D. Elliott, "International Responses to Cyber Crime, in The Transnational Dimension of Cyber Crime and Terrorism" 35, 36 (Hoover Press 2001), (last visited Jan. 30, 2017).
[8] Budapest Convention on Cybercrime, Preamble, Nov. 23, 2001, ETS No. 185 [hereinafter Budapest Convention]; see also Francesco Calderoni, "The European Legal Framework on Cybercrime: Striving for an Effective Implementation," 54 Crime, Law and Social Change 339, 342-43 (2010).
[9] See, Council of Europe, Chart of Signatures and Ratifications of Treaty 185 (Jan. 1, 2017), (last visited Jan. 30, 2017).
[10] Id.
[11] Budapest Convention arts. 2-11.
[12] Budapest Convention art. 24.
[13] Id. arts. 25, 31, 33, 34.
[14] Id. art. 26.
[15] Id. art. 29.
[16] Id. art. 30.
[17] Id. art. 35.
[18] SeeCalderoni, supra note 33, at 8.
[19] See Clough, supra note 30, at 701.
[20] See, e.g., Council of Europe Cybercrime Convention Committee (T-CY), T-CY "Assessment Report: The Mutual Legal Assistance Provisions of the Budapest Convention on Cybercrime" 4 (Dec. 3, 2014), (last visited Jan. 31, 2017).

[21] See, e.g., Council of Europe Cybercrime Convention Committee (T-CY), "Assessment Report: Implementation of the Preservation Provisions of the Budapest Convention on Cybercrime, Supplementary Report" 4 (June 21, 2015), (last visited Jan. 31, 2017).
[22] Directive 2013/40/EU, of the European Parliament and of the Council of 12 August 2013 on "Attacks Against Information Systems and Replacing Council Framework Decision" 2005/222/JHA, 2013 O.J. (L 218) 8-14, (last visited Jan. 30, 2017).
[23] See INTERPOL, Cybercrime, (last visited Feb. 8, 2017).
[24] Id.
[25] Id.
[26] The efforts are typically intended to protect (i) the privacy rights of individuals or (ii) critical infrastructure, such as power grids and banking systems.
[27] See McKay Cunningham, "Complying with International Data Protection Law," 84 U. Cin. L. Rev. 421, 421 (2016).
[28] Directive 95/46/EC, of the European Parliament and of the Council of 24 October 1995 on the "Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data," 1995 O.J. (L 281), 31-50, (last visited Jan. 30, 2017). The Directive applies directly to members of the European Union. Members of the EEA are required to adopt the Directive pursuant to Annex XI of the EEA Agreement.
[29] Directive 95/46/EC, supra note 53, art. 25.
[30] See Export.gov, U.S.-E.U. Safe Harbor Overview, (last visited Jan. 30, 2017).
[31] Case C-362/14, Schrems v. Data Protection Comm'n, 2015 EUR-Lex 627 (Oct. 6, 2015), (last visited Feb. 7, 2017).
[32] There was particular concern that E.U. data would not be protected from the Patriot Act. In 2013, these concerns were exacerbated by Edward Snowden's revelations regarding the NSA's surveillance activities.
[33] European Commission, Press Release, E.U. Commission and United States agree on new framework for transatlantic data flows: E.U.-U.S. Privacy Shield, (last visited Jan. 30, 2017).
[34] Id.
[35] Commission Regulation 2016/679, "On the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive" 95/46/EC, 2016 O.J. (L 119) 1, (last visited Jan. 31, 2017).
[36] See Mark Scott, "Europe Approves Tough New Data Protection Rules," N.Y. Times (Dec. 15, 2015), (last visited Jan. 31, 2017).