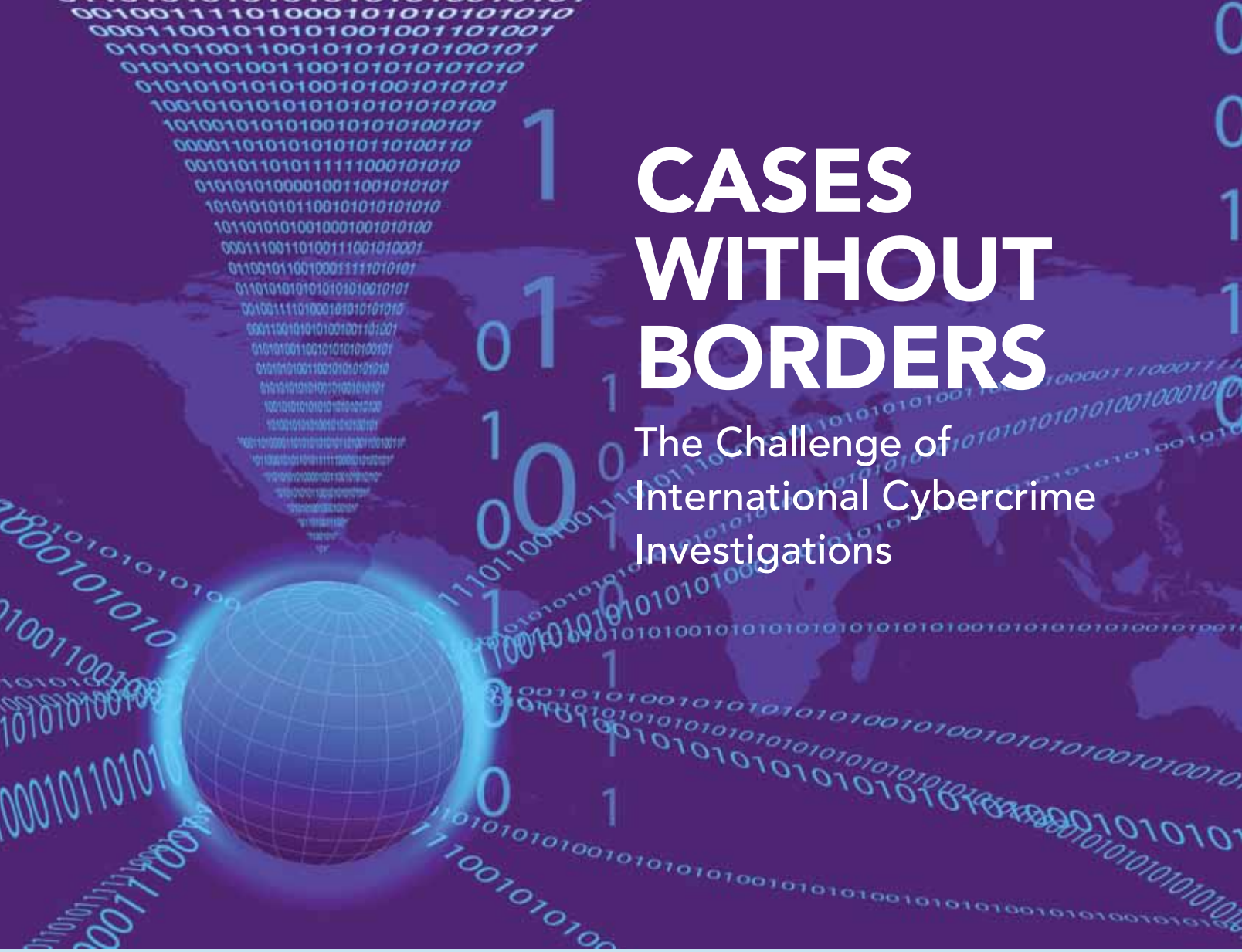

# CASES WITHOUT BORDERS

## The Challenge of International Cybercrime Investigations

BY JASON P. GONZALEZ, MATTHEW A.S. ESWORTHY, AND NEAL J. GAUGER

In the spring of 2000, the technology sector had never been so robust. The Y2K panic had been reduced to a false alarm, navigated by a combination of industrious preparation and luck. Business was booming as well, with the NASDAQ riding toward a record high on the backs of soaring dot-com companies. And so on the morning of May 4, 2000, computer experts and regular users alike gave little thought before opening an e-mail in their inboxes bearing a simple, affectionate salutation: "ILOVEYOU."

What followed remains to this day one of the most far-reaching and catastrophic cyberattacks ever recorded. The ILOVEYOU e-mail contained a vicious computer worm—soon known as the "Love Bug"—designed to copy the user's passwords, overwrite files, and redistribute itself to every person in the victim's Microsoft Outlook address book. (David Kleinbard & Richard Richtmyer, *U.S. Catches "Love" Virus*, CNNMoney (May 5, 2000), http://tinyurl.com/n5ebm7a; *see also* Peter Knight, *ILOVEYOU: Viruses, Paranoia, and the Environment of Risk*, 48 Soc. Rev., no. S2, Oct. 2000, at 17.) By the time it was stopped, the Love Bug would cause over 45 million individual "infections," crash nearly 10 percent of the world's computer servers, and cause an estimated $8 billion in damage. (Knight, *supra*, at 17; *see also* James Meek, *Love Bug Virus Creates Worldwide Chaos*, Guardian, May 5, 2000; Lorenzo Franceschi-Bicchierai, *Love Bug: The Virus That Hit 50 Million People Turns 15*, Motherboard (May 4, 2015), http://tinyurl.com/po8glte.)

International investigators quickly identified a pattern, noting that the Love Bug's infections had first appeared in the Philippines before ricocheting across the world. Soon thereafter, they fingered a Philippine hacker ring known as "GRAMMERSoft" and its leaders, Onel de Guzman and Reonel Ramones, as the likely culprits. (Franceschi-Bicchierai, *supra*.) What happened next? Surprisingly, nothing. Despite being able to trace the virus to an IP address in Ramones's apartment, and despite de Guzman's admitted experience with writing computer viruses, no Philippine law

at the time provided a mechanism to prosecute individuals for computer crimes. (*Id.*; *see also* Seth Mydans, *Philippine Prosecutors Release "Love Bug" Suspect*, N.Y. Times, May 10, 2000, http://tinyurl.com/pft9m9s.) Moreover, due to a lack of international cooperation and treaty limitations, no international law enforcement arm was successful in investigating and prosecuting the GRAMMERSoft ring. De Guzman and Ramones went free, and neither has ever paid a criminal or civil penalty related to the attack.

The Love Bug saga provides a prime example of both the devastating effect of international cybercrime and the frustrating legal roadblocks that prevent perpetrators from being brought to justice. This article provides a brief survey of three unique and significant challenges that exist in investigating and prosecuting international cybercrime, as well as a review of efforts by the international community to help develop more robust and effective methods of pursuing online crime around the world.

## Issue 1: "Dual Criminality" and Jurisdictional Conflicts

"Dual criminality" is a principle of international criminal law under which an accused individual may be extradited "only if the alleged criminal conduct is considered criminal under the laws of both the surrendering and requesting nations."(United States v. Saccoccia, 18 F.3d 795, 800 n.6 (9th Cir. 1994).) This principle often provides a direct roadblock to prosecution of international cybercrime, and it was a key factor in barring prosecution of the Love Bug attack—the extradition treaty between the Philippines and the United States demands dual criminality. (*See* Extradition Treaty between the Government of the United States of America and the Government of the Republic of the Philippines, Nov. 13, 1994, S. Treaty Doc. 104-16 ("Article 2(1) defines an extraditable offense as one punishable under the laws of both Contracting Parties by deprivation of liberty for a period of more than one year, or by a more severe penalty.").) As a result of the Philippines' lack of computer crime statutes, the actions of the GRAMMERSoft ring were not considered a punishable offense outside of its borders; thus, investigators from the United States were unable to extradite members of the GRAMMERSoft hacking ring to face prosecution.

More recently, the 2014 hack of Sony Pictures Entertainment has met similar investigatory roadblocks. Intelligence officials from the United States have concluded that the hack originated in North Korea, and may have been sponsored by the North Korean government. (David E. Sanger & Nicole Perlroth, *U.S. Said to Find North Korea Ordered Cyberattack on Sony*, N.Y. Times, Dec. 17, 2014, http://tinyurl.com/nmz7uhh.) While the North Korean government has attempted to deny involvement (referring to the attack as "the righteous deed of supporters and sympathizers"), it has unsurprisingly also failed to provide any assistance to international prosecution efforts. (*Id.*) The outcome is plainly evident—without the cooperation of the North Korean government, there is simply no mechanism for foreign governments to take effective legal action against the individuals who perpetrated the hack.

In response to these frequent dead ends, the international community has taken steps to help encourage greater cooperation between nations with respect to cybercrime, including passage of UN General Assembly Resolution 55/63, designed to combat international "criminal misuse of information technologies." Resolution 55/63 specifically calls on all member states to "eliminate safe havens for those who criminally misuse information technologies," and further establishes that "law enforcement cooperation in the investigation and prosecution of international cases of criminal misuse of information technologies should be coordinated among all concerned States." (G.A. Res. 55/63, U.N. Doc. A/RES/55/63 (Jan. 22, 2001).) These global efforts have been echoed on the regional level as well, with groups such as the Organization of American States (OAS) calling upon its member states to "creat[e] a framework for enacting laws that protect information systems, prevent the use of computers to facilitate illegal activity, and punish cybercrime." (Adoption of a Comprehensive Inter-American Strategy to Combat Threats to Cybersecurity: A Multidimensional and Multidisciplinary Approach to Creating a Culture of Cybersecurity, OAS Res. AG/RES 2004 (XXXIV-O/04) (June 8, 2004), http://tinyurl.com/ns2uuyn.)

Despite these efforts, there remains significant resistance to abandoning the "dual criminality" principle, as nations are loath to expose their citizens to international criminal liability when such acts are not illegal under (and sometimes condoned by) the accused's native government. Moreover, as seen in the Sony hack, many nations (including the United States) recognize the utility of cyberwarfare as a key method of nonmilitary aggression, and they may be resistant to allowing foreign governments to extend jurisdiction over such actions. (*See, e.g.*, David E. Sanger, *Obama Order Sped Up Wave of Cyberattacks against Iran*, N.Y. Times, June 1, 2012, http://tinyurl.com/d4tjk6j (discussing the Stuxnet cyberattack launched by the United States and Israel against the computer systems operating Iran's nuclear enrichment facilities); David Hancock, *Feds Out-Hack Russian Hackers*, CBS News (May 12, 2002), http://tinyurl.com/q8dq64m (discussing the Invita operation, the FBI counterhacking sting of Russian nationals engaged in the theft of credit card information).)

At this time, jurisdictional and other issues related to "dual criminality" seem likely to persist into the future; insufficient incentives exist for governments to change current practices and allow greater international oversight over their online actions and the actions of their citizens. Despite this, countries may find themselves needing to weigh the advantages of jurisdictional sovereignty against their ability to effectively combat an ever-increasing number of cross-border cybercrime attacks.

**JASON P. GONZALEZ** *is a partner with Nixon Peabody in Los Angeles and* **MATTHEW A.S. ESWORTHY** *is a partner with Shapiro Sher Guinot & Sandler in Baltimore.* **NEAL J. GAUGER** *is an associate at Nixon Peabody.*

## Issue 2: Challenges with Investigation Coordination and Consistency

Even where cooperation between nations can be achieved, significant roadblocks stand in the way of effective international cybercrime investigations. The mechanisms available to facilitate investigations are often inefficient and lack oversight as to the process by which cybercriminals are pursued.

An example of one such mechanism is the use of mutual legal assistance treaties, commonly known as MLATs. Under an MLAT, prosecutors in one country may request assistance from their counterparts in a foreign country in order to perform tasks such as the investigation of suspects and the collection of evidence. (T. Markus Funk, Mutual Legal Assistance Treaties and Letters Rogatory: A Guide for Judges 2–3 (Fed. Judicial Ctr. 2014), http://tinyurl.com/o5kpqmo.) Once provided by the foreign counterpart, the collected evidence may be used in a prosecution in the requesting attorney's country. (*Id.*)

While simple in concept, the MLAT process is often difficult and time-consuming to accomplish. As an example, for an attorney from the United States to seek subpoena information, execute a search warrant, or gain compliance with a court order under an MLAT, the attorney must provide a specific request (which must be approved by the foreign nation's courts) identifying, among other information, the requesting agency, a description of the subject matter and nature of the investigation (including the specific criminal offenses suspected to have been committed), and a description of the evidence, information, or other assistance sought. (*Id.* at 7.) The detailed nature of this request and the requirement for international approval can often complicate and impede efforts at information gathering. This can be particularly true early in an investigation, when the theories driving a prosecution effort may still be in the process of development.

Even if a sufficient request can be drafted, prosecutors who use MLATs are often required to conduct their inquiry at arm's length; rather than traveling abroad to conduct a firsthand investigation, the prosecutors must rely on their counterparts in the foreign jurisdiction to execute the requested task. (Peter Swire & Justin D. Hemmings, *Re-Engineering the Mutual Legal Assistance Treaty Process*, 71 N.Y.U. Ann. Surv. Am. L. (forthcoming 2016).) This requirement can cause frequent miscommunications and delays: Because the foreign jurisdiction often has a full slate of domestic matters that require its attention, a requesting attorney may find that the request is given low priority in light of domestic cases that implicate local victims. (*Id.*) In a 2013 study conducted by the United States executive branch, it was found that the average "turnaround" time for an MLAT request is 10 months, "with some requests taking considerably longer." (Richard A. Clarke et al., Liberty and Security in a Changing World: Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies 226–27 (2013), http://tinyurl.com/o5x8cea.) As discussed below in Issue 3, these delays can severely damage the effectiveness of a cybercrime investigation, wherein criminals often move quickly to erase traceable records of their actions online.

Despite these challenges, the MLAT process remains preferable to the use of "letters rogatory," the predominant alternative method for gathering information across international borders. Under an MLAT, a request for information is made based on a binding treaty guaranteeing cooperation between the contracting nations; in comparison, a letter rogatory is merely an informal request that relies on the goodwill of foreign courts and law enforcement officials to be properly executed. (Pamela D. Pengelley, *A Compelling Situation: Enforcing American Letters Rogatory in Ontario*, 85 La Revue du Barreau Canadien 345, 346–47 (2006).)

***Even where cooperation between nations can be achieved, significant roadblocks stand in the way of effective international cybercrime investigations.***

In the face of these limitations, reforming MLAT procedures to allow a requesting attorney to have greater oversight and control (including direct participation in the foreign investigation) may lead to greater coordination, consistency, and outcomes. The efficacy of this proposal can be seen in investigations where nations have worked together to facilitate informal communications and cooperation in addition to their treaty obligations.

For example, in 2014, the US Department of Justice (DOJ) successfully led a multinational criminal investigation and prosecution against the Gameover ZeuS botnet, a global network of criminals who caused over $100 million dollars in losses to businesses and consumers worldwide. (Press Release, U.S. Dep't of Justice, U.S. Leads Multi-National Action against "Gameover Zeus" Botnet and "Cryptolocker" Ransomware, Charges Botnet Administrator (June 2, 2014), http://tinyurl.com/owgkfrw.) By using a broad-spectrum, carefully coordinated approach, and by freely sharing information across public and private entities as varied as Italy's *Polizia Postale e delle Comunicazioni* (Postal and Communications Police), Ukraine's Ministry of Internal Affairs, Carnegie Mellon University, and Microsoft, investigators were able to efficiently and

effectively secure indictments against the leaders of the Gameover ZeuS group.

While it is widely accepted that the formal MLAT procedures will require reform to be effective against cybercrime, the Gameover ZeuS case provides a fantastic example of how informal international cooperation can and will help provide effective prosecutorial outcomes. In an area where technology consistently outpaces the laws that govern it, such collaborative action will likely be needed to ensure governments keep pace with cybercriminals going forward.

### Issue 3: Difficulties with Identification and Disclosure of Traffic Data

Separate from intercountry inefficiencies, nearly all cybercrime investigations encounter a common impediment—the anonymity of the Internet, and the ability of criminals to cover their tracks. Since 1998, the Internet Corporation for Assigned Names and Numbers (ICANN) has been responsible for, among other tasks, "coordinating the allocation and assignment of three unique identifies for the internet": domain names, IP addresses, and protocol port and parameter numbers. (*Bylaws for Internet Corporation for Assigned Names and Numbers*, ICANN (July 30, 2014), http://tinyurl.com/pljjwh4.) In plain English, this means that ICANN directly or indirectly oversees how and where individuals and their computers are identified on the Internet. Under current standards, ICANN effectively allows anonymous registration of domains, and does not appear to independently verify contact information provided to it by third-party registrar companies. (*Current Agreement*, ICANN (May 21, 2009), http://tinyurl.com/p3mpgjr; *see also Verifying Contact Information for ICANN Validation*, GoDaddy, http://tinyurl.com/qxf3evg (verifying only that a user has provided GoDaddy with an "active and accurate" e-mail account in order to confirm ICANN validation).)

Minor changes to the operation of ICANN could provide significant barriers to the use of computer networks for criminal purposes. For example, if ICANN were to require the submission and verification of a government-issued identification in order to register a domain name, the pool of individuals who submit false information would almost certainly shrink. A similar reduction in fraud would likely be seen by barring the use of prepaid credit cards or bitcoin to pay registration fees; a registration process that requires payment from authorized banks would undoubtedly provide more effective mechanisms for tracing individual actions online to the persons who committed them. Of course, while effective for law enforcement, such actions would likely draw strong objections from lawful users who, beyond the scope of domain name registration, prize the option of keeping their real-life identifies separate from their nameless online interactions. (*See, e.g.*, *Cheating Website Ashley Madison Hacked, Personal Info Posted*, Big Story (July 20, 2015), http://tinyurl.com/phwagcp.) As ICANN's registration requirements evolve, the organization will have no choice but to weigh privacy concerns against the need for effectively tracing online criminal actions.

Apart from ICANN's registration requirements, many other inefficiencies exist in pursuing the identities of cybercriminals. International cybercrime cases often involve tracing a hack through multiple IP addresses around the world, which can, in turn, mean digging through multiple layers of anonymity. Because speed is key to keeping online "trails" from growing cold, some intergovernmental organizations have recognized a special need to expedite disclosure of cyberspace traffic data across international borders. One such effort has been spearheaded by the Council of Europe, which requires (with few exceptions) that where a "tracing" request is made between council member states, "a sufficient amount of traffic data" must be "expeditiously disclose[d]" in order "to identify th[e] service provider and the path through which the communication was transmitted." (Council of Europe, Convention on Cybercrime, art. 30, Nov. 23, 2001, Eur. T.S. No. 185.)

***Intergovernmental organizations have recognized a special need to expedite disclosure of cyberspace traffic data across international borders.***

The open trade of "traffic data" between member states is a potentially fertile area for cooperation between governments. Because such data provides only the pathways through which a criminal act was allegedly taken, rather than the subject matter of the act itself, the scope of information provided does not require the more sophisticated analysis and approval of an MLAT request or other information-gathering mechanisms. While larger structural changes to international cooperation would likely be welcomed by many prosecutors, small changes like this can provide key advantages in combating fast-moving criminals online.

Ultimately, if the global community is able to meet the unique challenges presented by cybercrime, it will do so because sovereign nations band together, combine their resources, and recognize that cybercriminals rarely restrict themselves to the borders of a single nation. By embracing a policy of openness, and by placing an emphasis on efficient and effective collaboration, the world will be best able to beat back the ever-growing and increasingly sophisticated plague of hackers lurking online. ■