VIRGINIA JOURNAL OF LAW & TECHNOLOGY

FALL 2011 UNIVERSITY OF VIRGINIA VOL. 16, NO. 03

Foreground and Background in Cybercrime: *A Reply to Pinguelo and Muller*

JONATHAN J. RUSCH[†]

ABSTRACT

In their recent article, *Virtual Crimes – Real Damages?*, Fernando Pinguelo and Bradford Muller presented what they termed "a primer on [c]ybercrimes [i]n [t]he United States and [e]fforts to [c]ombat cybercriminals." While their article provided a *tour d'horizon* of computer-related threats and general characteristics of cybercriminals, as well as a useful compendium of statutes, it did not present a complete picture of the nature and scope of current cybercrime threats and available responses. This Article provides a narrower and more discriminating focus on the specific types of behavior characteristic of persons who commit specific types of cybercrime and the specific types of prevention measures necessary to reduce the effects of those cybercrime types. It also emphasizes the importance of focusing on the broader background of cybercrime, i.e., cybercrime threats and responses that extend beyond the borders of the United States.

[†] Deputy Chief for Strategy and Policy, Fraud Section, Criminal Division, United States Department of Justice; Lecturer in Law, University of Virginia Law School; Adjunct Professor, Georgetown University Law Center. The views expressed herein are solely those of the author and do not necessarily reflect those of the Department of Justice or any component or officer thereof.

TABLE OF CONTENTS

I. INTRODUCTION

In the Fitz Hugh Lane painting, *Approaching Storm*,[1] the viewer immediately sees in the foreground two sailing ships whose sails are being lowered or furled under the imminent threat of a severe storm. The casual viewer's eye is drawn first to the larger ship, a schooner, and then to the smaller, a single-masted fishing boat, whose white sails and rigging and wooden hulls contrast dramatically with the indigo masses of the storm clouds and sea. But if the viewer draws his eye away from the stark contrasts in the foreground and examines the painting more closely, he can discern not only that the dress and movements of the crews in the two ships are clearly different, but that in the farther distance, three other sailing ships are menaced by the same storm, which extends for miles in all directions.

In their article, *Virtual Crimes – Real Damages*,[2] Fernando M. Pinguelo and Bradford Muller focus on the foreground of cybercrime, in presenting what they term "a primer on [c]ybercrimes [i]n [t]he United States and [e]fforts to [c]ombat [c]ybercriminals."[3] Their article offers a concise but "robust discussion on the major forms of cybercrimes affecting the government and businesses today"[4] in the United States. Their compilation of information, drawn from numerous law enforcement, information-security, and media sources, provides a *tour d'horizon* of computer-related threats to critical U.S. infrastructures and general characteristics of cybercriminals,[5] as well as examples of "basic solutions . . . for reducing a company's exposure [to various cybercrimes]."[6] They also present a useful compendium of major federal and state criminal and civil statutes in the United States that are applicable to various cybercrimes,[7] and highlight some of the major legislative and executive initiatives to improve our domestic capacity to combat cybercrime.[8]

[1] Fitz Hugh Lane, *Approaching Storm*, oil painting, c. 1860 (private collection), *available at* http://www.the-athenaeum.org/art/full.php?ID=14014.

[2] Fernando M. Pinguelo & Bradford W. Muller, *Virtual Crimes – Real Damages: A Primer on Cybercrimes in the United States and Efforts to Combat Cybercriminals*, 16 VA. J.L. & TECH. 116 (2011).

[3] *Id*. at 1.

[4] *Id*. at 5.

[5] *See id*. at 5–23.

[6] *Id*. at (5).

[7] *See id*. at 29–40, 42–81.

[8] *See id*. at 24–29, 40–42.

My principal concern with their article is not the accuracy of the information they present, but rather the extent to which that information provides a complete picture of the nature and scope of current cybercrime threats and available responses. With respect to cybercrime threats and responses, a full appreciation of the problem requires a narrower and more discriminating focus on the specific types of behavior characteristic of persons who commit specific types of cybercrime, and on the specific types of prevention measures necessary to reduce the effects of those cybercrime types. It also requires a focus on the background of cybercrime: i.e., cybercrime threats and responses that extend beyond the borders of the United States. While it is beyond dispute that "proactive measures are needed to counter this evolving threat,"[9] a complete discussion of cybercrime threats must extend beyond national borders to adopt a global perspective.

II. PROFILING CYBERCRIMINALS

Pinguelo and Muller begin with what they term "a profile of the cybercriminal."[10] Although they state that "[t]here is no static 'profile' for a cybercriminal,"[11] immediately thereafter they cite general findings by the Internet Crime Complaint Center (IC3)[12] that more likely than not the cybercriminal whom American consumers and businesses encounter "will be a male from the United States," the majority of whom live in eight states and the District of Columbia.[13] They also briefly mention that "cybercriminals are not always lone wolves, but at times band together to further their criminal enterprises."[14] They later note that "disgruntled employees [in the government and business contexts] can be an especially harmful brand of cybercriminal,"[15] citing varied examples of insider misconduct such as theft of intellectual property, sabotage, and identity theft.[16]

Here, Pinguelo's and Muller's analysis, like some crime researchers' efforts to profile cybercrime,[17] is inadvertently reductionist. Without disputing that cybercriminals sometimes are lone wolves and sometimes band together, it is important for law enforcement officials and information-security specialists to understand in detail who commits different types of cybercrime, when cybercriminals act as lone wolves or in packs, how they commit different cybercrimes, and why.[18]

With respect to insider threats, for instance, the U.S. Secret Service conducted a multi-year Insider Threat Study (ITS), in collaboration with Carnegie Mellon University's Computer Emergency Response Team (CERT) Program. The ITS included separate

[9] *Id*. at 4.

[10] *Id*. at 5.

[11] *Id*. at 6.

[12] *See* INTERNET CRIME COMPLAINT CENTER, http://www.ic3.gov (last visited Sept. 22, 2011).

[13] Pinguelo & Muller, *supra* note 2, at 6 (citing INTERNET CRIME COMPLAINT CENTER, 2009 INTERNET CRIME REPORT 7 (2010), *available at* http://www.ic3.gov/media/annualreport/2009_IC3Report.pdf).

[14] *Id*. at 7.

[15] *Id*. at 11.

[16] *See id*. at 12–13.

[17] *See, e.g.*, Rutger Leukfeldt et al., *Cybercrime is Van Het Volk*, SECONDANT 1, at 42, March 2011, *available at* http://www.hetccv.nl/binaries/content/assets/ccv/secondant/2011/secondant_maart_2011.pdf.

[18] *See* MICHAEL CROSS & DERRA LITTLEJOHN SHINDLER, SCENE OF THE CYBERCRIME 92 (2008).

studies of illicit cyber activity in the banking and finance,[19] information technology and telecommunications,[20] government sectors,[21] and computer sabotage in critical infrastructure sectors.[22] These four studies revealed significantly different patterns of behavior and cybercrime techniques used to commit the offenses:

- *Banking and Finance*: This study found that most of the incidents were not technically sophisticated or complex, as "they typically involved exploitation of non-technical vulnerabilities such as business rules or organization policies . . . and were carried out by individuals who had little or no technical expertise."[23] In 70 percent of the cases studied, "the insiders exploited or attempted to exploit systemic vulnerabilities in applications and/or processes or procedures (e.g., business rule checks, authorized overrides) to carry out the incidents."[24] In 78 percent of the incidents, the insiders "were authorized users with active computer accounts at the time of the incident."[25] But only 23 percent of the insiders were employed in technical positions (with 17 percent possessing system administrator/root access within the organization), and 39 percent "were unaware of the organizations' technical security measures."[26]

- *Information Technology and Telecommunications*: This study found that current and former employees carried out their illicit activities "in nearly equal numbers [53 current 47 former];" most insiders "were either previously or currently employed full-time in a technical position within the organization;" 38 percent of the insiders had been arrested previously (and 56 percent of those insiders with a prior criminal history had multiple prior arrests and convictions); insiders "represented a wide range of ages, from 17 to 58 years;" the majority of insiders "were single at the time of the attack, and had never been married;" and 91 percent of the insiders were male.[27]

- *Government*: This study found that "insiders did not share common demographic characteristics," for gender (50 percent were men, 50 percent women), race (42 percent were African-American, 39 percent Caucasian, 8 percent Asian, and 5

[19] *See* Marisa Reddy Randazzo, Michelle Keeney, Eileen Kowalski, Dawn Cappelli & Andrew Moore, *Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector* (August 2004), *available at* http://www.secretservice.gov/ntac/its_report_040820.pdf.

[20] *See* Eileen Kowalski, Dawn Cappelli & Andrew Moore, *Insider Threat Study: Illicit Cyber Activity in the Information Technology and Telecommunications Sector* (January 2008), *available at* http://www.secretservice.gov/ntac/final_it_sector_2008_0109.pdf.

[21] *See* Eileen Kowalski, Tara Conway, Susan Keverline, Megan Williams, Dawn Cappelli, Bradford Willke & Andrew Moore, *Insider Threat Study: Illicit Cyber Activity in the Government Sector* (January 2008) , *available at* http://www.secretservice.gov/ntac/final_government_sector2008_0109.pdf.

[22] *See* Michelle Keeney, Eileen Kowalski, Dawn Cappelli, Andrew Moore, Timothy Shimeall & Stephanie Rogers, *Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors* (May 2005), *available at* http://www.secretservice.gov/ntac/its_report_050516.pdf.

[23] Cappelli, et al., *ITC: Banking and Finance*, *supra* note 19, at 8.

[24] *Id.* at 9.

[25] *Id.*

[26] *Id.*

[27] Kowalski, et al., *ITC: Telecommunications*, *supra* note 20, at 14–16.

percent Hispanic), or age (19 to 55); the majority of insiders (58 percent) were current employees in administrative and support positions that required limited technical skills; and nearly all were current employees of the target organizations.[28]

- *Sabotage*: This study found that the majority of insiders were former employees; at the time of the incident, 59 percent of the insiders were former employees or contractors of the affected organizations and 41 percent were current employees or contractors; the former employees or contractors left their positions for a variety of reasons (firing 48 percent, resigning 38 percent, and being laid off 7 percent); most insiders were previously or currently employed full-time (77 percent), in a technical position within the organization (86 percent), including system administrators (38 percent), programmers (21 percent), engineers (14 percent), and IT specialists (14 percent);[29] insiders were demographically varied with regard to age (17 to 60), racial and ethnic background, gender (96 percent male), and marital status (49 percent married, 45 percent single, 4 percent divorced); and 30 percent of the insiders had been arrested previously, including arrests for violent offenses (18 percent), alcohol or drug related offenses (11 percent), and nonfinancial/fraud related theft offenses (11 percent).[30] Furthermore, with regard to attack techniques, the study found that 57 percent of the insiders were granted system administrator access upon hire, but 85 percent of those no longer legitimately retained that level of access at the time of the incidents; in 57 percent of the cases, the insiders "exploited or attempted to exploit systemic vulnerabilities in applications, processes, and/or procedures" (e.g., business rule checks and authorized overrides); and in 61 percent of the cases, the insider's actions "were limited to relatively unsophisticated methods of attack," including user commands, information exchanges, and exploitation of physical security vulnerabilities.[31] The study also found that in 87 percent of the cases, the victim organizations permitted employees remote access (56 involving solely remote access, 35 percent only from within the workplace, and 8 percent both from within the workplace and remotely).[32]

More recently, Verizon, in cooperation with the Secret Service, issued a detailed report on data breaches.[33] While it is organized differently from the Secret Service studies, the Verizon report provides detailed data on the nature of the criminals and the nature and types of data breach-related attacks. Most significantly, the report found that 70 percent of the attacks, but 98 percent of the data stolen, involved external agents (largely organized criminal groups) and 48 percent involved insiders (a notable 26

[28] *See* Kowalski, et al., *ITC: Government Sector*, *supra* note 21, at 14–15.
[29] *See* Keeney, et al,, *ITC: Sabotage, supra* note 22, at 11.
[30] *Id.* at 12.
[31] *Id.* at 17.
[32] *Id.* at 18.
[33] *See* VERIZON, 2010 DATA BREACH INVESTIGATIONS REPORT (2011), *available at* http://www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf.

percent increase from the preceding year);[34] 48 percent of attacks involved an attacker's misuse of system privileges, 40 percent hacking, 38 percent malware, 28 percent social tactics, and 15 percent physical attacks.[35] The report also noted that 85 percent of attacks were not considered highly difficult, and 96 percent of breaches were avoidable through simple or intermediate controls.[36]

As both sets of studies make clear, there are often significant differences in the personal and attack characteristics associated with different types of cybercrime. Those differences substantially affect not only how potential target organizations defend themselves against such acts, but also how law enforcement investigates those acts.[37] Analysis that lumps together those differences to produce highly generalized statements about cybercriminals has little value for information-security scholars or practitioners.

III. DEVELOPING A GLOBAL RESPONSE TO CYBERCRIME

A. Enforcement Responses

At various points, Pinguelo and Muller cite examples of cyber attacks that are directed or launched outside the United States and have effects in the United States and elsewhere.[38] Yet their analysis does not address the implications of these data. No matter how broadly Congress and state legislatures draft criminal offenses and civil statutes to address cybercrime, U.S. investigators and prosecutors can do little to have any significant effect on conduct beyond our borders without assistance from foreign countries. In cybercrime cases with trans-border elements, U.S. and foreign law enforcement alike need timely access to foreign evidence, active cooperation with their foreign counterparts, and foreign statutes that clearly define various cybercrimes as criminal offenses for purposes of mutual legal assistance and extradition.

Pinguelo and Muller quote without comment another scholar's assertion that "[l]aw enforcement resources in cyberspace cannot keep pace with sophisticated cybercrime subcultures in anonymous offshore havens."[39] In fact, while law enforcement around the world constantly faces the challenges of keeping pace with technological developments in cybercrime,[40] U.S. and foreign law enforcement agencies have an

[34] *See id.* at 2–3. Totals of percentages add up to greater than 100 percent, as some breaches involved more than one type of behavior.

[35] *See id.*

[36] *See id.*

[37] *See* Leonard Kwan, Pradeep Ray & Greg Stephens, *Towards a Methodology for Profiling Cyber Criminals*, Proceedings of the 41st Hawaii International Conference on System Sciences (2008), *available at* http://origin-www.computer.org/plugins/dl/pdf/proceedings/hicss/2008/3075/00/30750264.pdf?template=1&loginState=1&userData=anonymous-IP%253A%253AAddress%253A%2B173.73.123.111%252C%2B%255B172.16.161.5%252C%2B173.73.123.111%252C%2B127.0.0.1%255D.

[38] *See* Pinguelo & Muller, *supra* note 2, nn.7, 29, 32–35, 44–46 and accompanying text.

[39] *Id.* at 82 (citing Michael L. Rustad, *Private Enforcement of Cybercrime on the Electronic Frontier*, 11 S. CAL. INTERDISC. L.J. 63, 66 (2001)).

[40] *See, e.g.*, *McAfee Trains U.K. Law Enforcement on Cybercrime*, SECURITY NEWS, (June 30, 2010), http://www.securityweek.com/mcafee-trains-uk-law-enforcement-cybercrime#.

extensive and growing arsenal of international conventions and domestic criminal offenses and civil statutes to pursue transnational cybercrime effectively.

First among the relevant international conventions is the Council of Europe Cybercrime Convention.[41] The Cybercrime (or Budapest) Convention is the first international treaty or convention expressly drafted to address several categories of crimes committed by means of the Internet and other computer networks.[42] It sets forth essential categories of cybercrimes that Parties to the Convention commit to establishing as criminal offenses in their respective legal systems.[43] It also sets forth essential categories of procedural requirements that Parties to the Convention commit to establishing in their domestic legal systems, such as preservation of stored computer and traffic data and disclosure thereof and real-time collection of traffic and content data.[44] Finally, it prescribes specific international cooperative measures, ranging from general principles on extradition[45] and mutual assistance[46] to specific principles of cooperation on issues such as preservation and disclosure of data,[47] mutual assistance in real-time collection of data,[48] and operation of a "24/7 network" for round-the-clock points of contact on cybercrime-related requests for assistance.[49]

Two United Nations Conventions—the United Nations Convention Against Transnational Organized Crime[50] (the UNTOC or Palermo Convention) and the United Nations Convention Against Corruption[51] (the UNCAC or Merida Convention)—are also applicable to a variety of scenarios involving cybercrime. The Palermo Convention directs that States Parties adopt legislative and other measures to establish as criminal offenses, inter alia, participation in an organized criminal group, laundering of proceeds of crime, corruption involving public officials, and obstruction of justice.[52] By its terms, the scope of offenses under the Convention would reach any structured group of three or more persons acting in concert with the aim of committing one or more serious offenses established in accordance with the Convention.[53] Thus, even cybercrime-related criminal

[41] Council of Europe, Convention on Cybercrime, ETS No. 185 (2001) [hereinafter Cybercrime Convention], *available at* http://conventions.coe.int/Treaty/EN/Treaties/html/185.htm. The next four paragraphs of this section draw extensively from Jonathan J. Rusch, *Iago's Net: Notes for an International Legal Regime to Combat Identity-Related Crime*, 42 GEO. J. INT'L L. 923 (2011).

[42] KRISTIN ARCHICK, CONG. RESEARCH SERV., RS21208, CYBERCRIME: THE COUNCIL OF EUROPE CONVENTION 1 (July 22, 2004), *available at* http://fpc.state.gov/documents/organization/36076.pdf.

[43] *See* Cybercrime Convention, *supra* note 41, arts. 2 (illegal access to computer systems), 3(illegal interception of non-public transmissions of computer data), 4 (damaging, deletion, deterioration, alteration or suppression of computer data), 7 (computer-related forgery), and 8 (computer-related fraud).

[44] *See id*. arts. 16–18, 20–21.

[45] *See id*. art. 24.

[46] *See id*. arts. 25–27.

[47] *See id*. arts. 29–30.

[48] *See id*. arts. 31–34.

[49] *See id*. art. 35.

[50] United Nations Convention Against Transnational Organized Crime, G.A. Res. 55/25, U.N. Doc. A/55/383 (Jan. 8, 2001) [hereinafter Palermo Convention].

[51] United Nations Convention Against Corruption, G.A. Res. 58/4, U.N. Doc. A/58/4 (Oct. 31, 2003) [hereinafter Merida Convention].

[52] Palermo Convention, arts. 5, 6, 8, and 23.

[53] *Id*. art. 2(a)–(b).

conduct by groups of three or more could fall under the Convention's provisions. The Convention also contains its own array of provisions to foster international cooperation in the pursuit of transnational organized crime.[54] Finally, the Merida Convention, which addresses corruption in the public and private sectors, urges States Parties to consider adopting legislative and other measures to criminalize bribery and embezzlement in the private sector.[55] It also directs States Parties to take appropriate cooperation measures pertaining to law enforcement authorities and to national authorities, and prompts the cooperation between national investigating and prosecuting authorities and the private sector.[56]

Beyond these international conventions, a growing number of countries, whether because of or independent of the Budapest Convention, have enacted robust criminal and civil measures. In the United States, numerous federal offenses, including those that Pinguelo and Muller summarize,[57] are applicable to cybercrime. Other countries have also enacted or revised national criminal offenses pertinent to cybercrime, including Australia[58] and the United Kingdom.[59] Wherever the United States has Mutual Legal Assistance Treaties or extradition treaties with other countries, and substantial cooperation from foreign authorities, the prospects of genuine international cooperation and of actual apprehension and prosecution of cybercriminals are very real.[60]

B. Prevention Responses

In contrast to their extensive description of the scope and severity of cybercrime, Pinguelo and Muller give regrettably little attention to the problem of preventing cybercrime. They acknowledge the difficulty of protection from "cyber spies," but then assert that "individual companies can easily implement policies to reduce their exposure,"[61] citing an automobile manufacturer's blocking employees from using Facebook and some companies' hiring of former hackers.[62] In their conclusion, they also assert, without further discussion, that "merely educating one's employees as to the

[54] *Id*. arts. 18–29.

[55] Merida Convention, arts. 21–22.

[56] *Id*. arts. 37–39.

[57] *See* Pinguelo & Muller, *supra* note 2, at 123–135.

[58] *See* Press Release, Minister of Home Affairs and Justice, Austl. Gov't (Feb. 10, 2011), *available at* http://www.ag.gov.au/www/ministers/oconnor.nsf/Page/MediaReleases_2011_FirstQuarter_10February2011-Legislationpassedtohelpvictimsofidentitycrime.

[59] *See* John Austen, *U.K. Cyber-Crime Law Changed*, ISSA REV., Mar. 2007, at 18, *available at* http://www.issa.org/Library/Journals/2007/March/Austen%20-%20U.K.%20Cyber-Crime%20Law%20Changed.pdf.

[60] *See, e.g*., Press Release, U.S. Dep't of Justice (Mar. 25, 2011) (reporting that 46 persons in U.S.-Egypt hacking and phishing ring were convicted in federal court), *available at* http://www.cybercrime.gov/merziGuilty.pdf; Press Release, U.S. Dep't of Justice (Feb. 28, 2011) (reporting a 82-month prison sentence on a defendant who participated in an international hacking conspiracy), *available at* http://www.cybercrime.gov/palaSent.pdf; Press Release, U.S. Dep't of Justice (Apr. 26, 2010) (reporting 81-month prison sentence for defendant's role in an international hacking and securities fraud operation*), available at* http://www.justice.gov/opa/pr/2010/April/10-crm-484.html.

[61] Pinguelo & Muller, *supra* note 2, at 125.

[62] *Id*.

reality of the cyber threat and simple steps they can take to reduce the company's exposure could go a long way."[63]

The reality of cybercrime prevention is vastly more complicated. While end-user education about cybercrime risks is necessary and useful as part of a larger prevention strategy, it is far from sufficient. Even if every government and private-sector employee refrained from using Facebook or P2P software while at work and patched home-computer software regularly, cybercrime would not be brought to its knees. As criminal organizations have learned that cybercrime can create new revenue streams for their enterprises, they have gravitated to attacking key commercial repositories of digital data and extracting large quantities of data for resale or criminal use.[64] In March 2011, for example, Epsilon Interactive, a leading e-mail service provider that sends out more than forty billion emails a year for corporate clients in the United Kingdom and the United States, suffered a major data breach affecting at least fifty leading companies with transnational business.[65]

One of the many complexities of cybercrime prevention is that some key points of cyber-vulnerability are found in products or systems of multiple companies that individually have no clear legal or economic incentive to correct the vulnerability. Here are two examples of this problem:

1. Browser Vulnerabilities. A 2010–2011 survey by a compliance vendor found that approximately 80 percent of Internet users' browsers are insecure. More than half of the vulnerabilities found reportedly stem from vulnerable "plug-in" applications (e.g., Java, Adobe Reader, Flash, and Windows Media Player), many of which are in widespread use, while only about 20 percent of the vulnerabilities are due to native browser applications.[66] The vendor ascribed this difference to the fact that while browsers affirmatively alert users to the need to install updates or automatically install updates, few plug-ins automatically update, which requires information technology departments to determine whether updates are necessary and identify plug-ins that have auto-update programs.[67]

2. Payment-Card Vulnerabilities. To reduce the incidence of payment-card fraud, a number of leading financial institutions have adopted so-called "chip and PIN technology:" i.e., inclusion of a computer chip in the payment card that contains

[63] *Id*. at 188.

[64] *See, e.g.*, *Identity Theft: A Victims Bill of Rights, Hearing Before the Subcomm. on Information Policy, Census, and National Archives of the H. Comm. on Oversight and Government Reform*, 111th Cong. (2009) (prepared statement of Jason Weinstein, Deputy Assistant Attorney General, Criminal Division, U.S. Department of Justice), *available at* http://www.justice.gov/ola/testimony/111-1/2009-06-17-crm-weinstein-identity-theft.pdf.

[65] Robert McMillan, *Epsilon Says 50 Major Companies Hit in E-mail Marketing Breach*, CIO UK MAGAZINE, (Apr. 5, 2011), http://www.cio.co.uk/news/3268303/epsilon-says-50-major-companies-hit-in-e-mail-marketing-breach/.

[66] Matthew J. Schwartz, *80% of Browsers Have Known Vulnerabilities*, INFORMATIONWEEK, (Feb. 23, 2011), http://www.informationweek.com/news/security/vulnerabilities/showArticle.jhtml?articleID=229219113.

[67] *See id*. The survey noted that the 80 percent statistic represented a decline from the nearly 90 percent of browsers with vulnerabilities in June 2010. *Id.*

identification and authentication data for the cardholder that cannot be copied as readily as identifying data recorded on magnetic-stripe cards, coupled with the use of a unique PIN. Financial institutions in Europe have deployed chip and PIN over the past decade;[68] Asian countries including Japan, Singapore, and Taiwan had high adoption rates of chip and PIN in the past five years;[69] in Australia, Visa began a four-year plan in 2009 to move to chip and PIN card use by financial institutions and retailers,[70] and more recently, banks in sub-Saharan African countries such as Nigeria and South Africa and Central and South American countries such as Brazil and Mexico have increasingly deployed chip and PIN cards.[71]

Although chip and PIN have not been invulnerable to certain criminal techniques,[72] countries that have adopted chip and PIN have reported striking successes in reducing identity-related crime. In the United Kingdom, chip and PIN implementation reportedly has been a major factor in reducing payment-card fraud within the country.[73] One report found that after the United Kingdom's adoption of chip and PIN in 2003, domestic losses on United Kingdom transactions declined by 55 percent by 2008.[74] In Australia, in 2010, according to the Australian Payments Clearing Association, overall skimming fraud on Australian-issued credit, debit, and charge cards declined to AU $34.5 million (a 24 percent reduction). Within that total, skimming fraud on cards used in Australia accounted for AU $12.2 million (a 38 percent reduction), and skimming fraud on cards used outside of Australia accounted for AU $22.3 million (a 13 percent

[68] Richard Oliver, *Soccer Balls and Payment Cards: A Push for Global Standards*, PORTALS AND RAILS, (July 19, 2010), http://portalsandrails.frbatlanta.org/2010/07/soccer-balls-payment-cards-push-for-global-standards.html.

[69] *See* Negar Salek, *Fighting Fraud with Chip & PIN*, SECURE COMPUTING, (Mar. 7, 2008, 12:12 PM), http://www.securecomputing.net.au/Feature/106597,fighting-fraud-with-chip--pin.aspx#.

[70] Press Release, Visa Asia Pacific, Visa Announces Dates for Chip and PIN Rollout for Australia (Nov. 2, 2009), http://www.visa-asia.com/ap/au/mediacenter/pressrelease/NR_Au_021109_security_plan.shtml.

[71] *See* Allie Johnson, *U.S. Credit Cards Becoming Outdated, Less Usable Abroad*, CREDITCARDS.COM, (Oct. 1, 2008), http://www.creditcards.com/credit-card-news/outdated-smart-card-chip-pin-1273.php; *Postilion Helps Drive Africa's Migration to Chip and PIN*, MODERN GHANA, (Apr. 28, 2009), http://www.modernghana.com/news/213562/1/postilion-helps-drive-africas-migration-to-chip-an.html; *Chip and PIN Card Users on the Rise, Retailers Ready*, BIZCOMMUNITY.COM (Mar. 2009), http://www.bizcommunity.com/Article/196/182/34015.html.

[72] *See, e.g.*, Saar Drimer, Steven J. Murdoch & Ross Anderson, *Thinking Inside the Box: System-Level Failures of Tamper Proofing*, 711 U. CAMBRIDGE COMPUTER LABORATORY TECHNICAL REP. (Feb. 2008), *available at* http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-711.pdf; Colin Fernandez, *Chip and PIN Flaw That Banks Tried to Censor: Cambridge Scientist Exposed Security Failures*, DAILY MAIL, (Dec. 29, 2010, 9:54 AM), http://www.dailymail.co.uk/news/article-1342218/Chip-PIN-flaw-banks-tried-censor-Cambridge-scientist-exposed-security-failures.html; Steve Bird, *'Catch Me if You Can,' Said Student Behind Biggest Chip and PIN Fraud*, TIMES (London), Oct. 29, 2008, *available at* http://www.timesonline.co.uk/tol/news/uk/crime/article5034185.ece.

[73] *HSBC: Card Fraud 'Reduced by Chip and Pin,'* MONEY NEWS, (Jan. 26, 2009), http://www.moneynews.co.uk/6089/hsbc-card-fraud-reeduced-by-chip-and-pin-/.

[74] Steve Brunswick, *Chip and PIN - Not Perfect, But the Best We Have*, FINEXTRA. (Feb. 15, 2010), http://www.finextra.com/community/fullblog.aspx?id=3808.

reduction). Notably, even skimming fraud in Australia with cards issued outside Australia sharply declined by 47 percent to AU $34.6 million.[75]

What remains problematic for countries that have implemented chip and PIN is "card-not-present" fraud (i.e., fraud involving the remote use of payment-card data in transactions via the Internet, telephone, or mail).[76] Criminals who steal chip and PIN cards or data associated with non-U.S. residents can use them for online purchases of high-priced items that can be fenced, or for cash withdrawals from financial institutions in jurisdictions where chip and PIN technology is not deployed (principally the United States).[77]

In theory, preventing browser vulnerabilities has a simple solution: i.e., require all software vendors that offer "plug-in" technology to update their software to ensure automatic updating. Imposing that requirement through legislation, however, would be problematic on many levels—not least of them being the undesirability of using legislation to impose technology-specific solutions on multiple information-technology companies. Other possible means of accomplishing the same end, such as voluntary adoption of an auto-updating industry standard, would require someone in government or the private sector to initiate and coordinate the discussion with multiple participants in more than one industry sector.

Similarly, preventing payment-card vulnerabilities theoretically has a simple solution: i.e., require the U.S. financial sector to adopt chip and PIN or other "smart-card" technology that would be compatible with other countries' payment systems. U.S. financial institutions, however, are reportedly concerned that transition to chip and PIN or other smart-card technology would require replacement of approximately 60 million magnetic-stripe readers with chip and PIN readers[78]—an expense that individual retailers, rather than financial institutions, would be expected to bear. Moreover, the sheer multiplicity of participants in the payment-card system —card associations like Visa and MasterCard, card issuers, and merchants of all sizes, each of which has different financial incentives and disincentives[79]—and the lack of an obvious least cost avoider complicate the task of moving toward a nationwide solution.[80]

[75] *Chip Technology Shifts Australian Fraud Landscape*, FINEXTRA, (Dec. 7, 2010), http://www.finextra.com/news/fullstory.aspx?newsitemid=22077.

[76] *See* Steve Brunswick, *Chip and PIN Impacts Australian Card Fraud*, FINEXTRA, (Dec. 7, 2010), http://www.finextra.com/community/fullblog.aspx?blogid=4784.

[77] *See* CRIMINAL INTELLIGENCE SERVICE CANADA, 2010 REPORT ON ORGANIZED CRIME 29 (2010), *available at* http://www.cisc.gc.ca/annual_reports/annual_report_2010/document/report_oc_2010_e.pdf; John Leyden, *Internet Scams Dominate UK Card Fraud Losses*, THE REGISTER, (Mar. 4, 2007), http://www.theregister.co.uk/2007/03/14/uk_card_fraud_trends/.

[78] *See* Michael Kassner, *Debit/Credit Card Fraud: Can Smart Payment Cards Prevent It*, TECHREPUBLIC, (Sept. 21, 2010), http://www.techrepublic.com/blog/security/debitcredit-card-fraud-can-smart-payment-cards-prevent-it/4451.

[79] *See* Adam J. Levitin, *Private Disordering?: Payment Card Fraud Liability Rules*, 5 BROOK. J. CORP. FIN. & COM. L. 1, 6 (2011).

[80] For an indication of a possible voluntary solution, see Oliver, *supra* note 68.

This is not to say that these (and other) cybercrime-prevention problems are insoluble, but simply that solutions are neither simple nor easy to develop and implement at a national level, especially when elements of that solution require the active engagement of key participants based outside the United States. In the borderless world of the Internet and digital payments system, the concept of a "security culture" that Pinguelo and Muller apparently favor[81] can be fully realized only if public- and private-sector entities in many countries play a role in developing and maintaining that culture.

IV. CONCLUSION

Appreciation of any major crime phenomenon, like appreciation of a landscape or seascape, requires a patient and thorough examination of the whole scene. If Pinguelo and Muller have not provided a complete depiction of the cybercrime phenomenon, they at least deserve thanks for the rendering of the foreground. Other cybercrime scholars need to add their own brushstrokes to complete the scene.

[81] *See* Pinguelo & Muller, *supra* note 2, at 131.