Gough Whitlam Plaza, Suite 1, Level 5, 20-22 Wentworth Street, Parramatta, NSW 2150, Sydney, Australia

Challenges to Law Enforcement when dealing with Cybercrime

Author: *Dr Maher Magrabi*

Full article:

Cybercrime is on the rise with an estimated global economic cost of $600 billion (Lewis 2018). In its 2017 threat report, the Australian Cyber Security Centre (ACSC) presented a threat context within which the risks posed by cybercrime remain pervasive with regard to Australia's economic and national prosperity. The relatively lower risks of identification, interdiction and prosecution coupled with the ability to act on a global scale and generate much larger profits will continue to make cybercrime in Australia an attractive option for criminals (Kowalick & Connery 2016). The threats are from both state and non-state actors, who are highly organised, resourced and seeking to target Australians for various objectives including crime, espionage, and terrorism (ACSC 2017). Of note, are the increasing threat levels to Australian financial institutions, including banks (Choo 2011; McCombie 2008; Leukfeldt et al. 2017), $2.7 trillion worth of superannuation funds (ASFA 2018; APRA 2016; APRA 2017, AUSTRAC 2016), and the Australian Stock Exchange (ASX) (AUSTRAC 2017). The transnational nature of cybercrime, the evolution of technologies in encryption, distributed computing and cloud computing have created a multitude of challenges for Australian law enforcement. Furthermore, law enforcement must have the capacity and capability to react and proactively work (Hunton 2010) to deal with this growing threat. This includes the legislative framework that allows law enforcement the tools, know-how and expertise to investigate these crimes, to takedown illegal criminal operations, and the prosecution of offenders.

The National Cybercrime Working Group has defined cybercrime as encompassing both crimes directed at computers or other information communications technologies (ICTs) as well as traditional crimes enabled by computers or ICTs (AG 2013). This includes crimes such as hacking (Fell 2017); denial of service attacks (Huang & Gouda 2006); online fraud (Drew & Farrell 2018; Cross 2018a); identity theft (Farina 2015); online money laundering (Philippsohn 2001; Glonti 2015; Zhou et al. 2018); creation, storage or propagation of Child Sexual Exploitation Material (CSEM) or Child Sexual Assault Material (CSAM) (Dubowitz 2017; Krone & Smith 2017; Hui et al. 2015); Cyber-bullying or harassment (Nicol 2012; Modecki et al. 2014; Hemphill et al. 2015); and Digital Piracy and content crimes (Dent 2009).

The centralised facility for the reporting of cybercrime in Australia is the Australian Cybercrime Online Reporting Network (ACORN) has recorded 47,873 complaints between 1 July 2016 and 30 June 2017 (ACORN 2017), increasing by 12% in the following year (ACORN 2018). These numbers should also be contextualised within the issue of rampant underreporting of cybercrime incidents (Wall 2007; Hyman 2013; Cross 2018a). These complaints are in stark contrast to successful apprehension and prosecutions for these crimes (Hanson 2018). Some investigations have revealed that less than 1% of crimes reported though ACORN resulted in an investigation that successfully identified the offender, and less than 1% resulted in successful prosecution (Cross 2018b; CDPP 2018). One contributing factor to the low levels of prosecution in Australia is the trans-jurisdictional nature of cybercrime, in that the majority of cybercrimes are committed from other jurisdictions and the perpetrators, if indicted, are prosecuted in their country of origin.

The trans-jurisdictional nature of cybercrime creates challenges for law enforcement in their investigation and prosecution of the crime. Jurisdiction is the authority given to a court to try legal cases or to give a legal ruling within a specific geography. In the case of a country, it is traditionally defined as its territorial boundaries, and this includes any information and communications technology that exists physically within its territories (Brenner 2001). In international law, the concept of jurisdiction in rooted in the Westphalian tradition and has a strong resonance with territorial sovereignty, even where such a construct becomes increasingly inapplicable in the case of non-territorial cyberspace (Ryngaert 2015). Extra-territoriality is invoked when cases span across multiple jurisdictions (UNODC 2013). The more serious forms of cybercrime being classed within the principle of universality, where the crimes are seen as ‘international’ (Tehrani & Manap 2013). Cybercrime by its very nature is transnational, where the victim might be in one jurisdiction, the perpetrator in an entirely different jurisdiction, with the ICT utilised in a range of different countries (Holt et al. 2015; McCombie 2011). Establishment of jurisdiction is one of the key challenges to law enforcement (Desnoyers 2013; UNODC 2013; Brown 2015; Brittingham 2017; Qi & Lin 2018). A hacker or criminal group in Russia could carry out a ransomware attack on a victim in Australia utilising a cloud server in the US and a global botnet for distribution.

One such example of ransomware was CryptoLocker, which was taken down in 2014 through a multinational investigation involving the FBI, Europol and the United Kingdom National Crime Agency and culminated in the arrest of a Russian citizen, Evgeniy Mikhailovich Bogachev, who was charged with conspiracy, hacking, wire fraud, bank fraud and money laundering (Thompson 2014). An analysis carried out in 2017 on the public blockchain ledger has revealed that CyptoLocker has been used to extort approximately 450,000 USD (Conti et al 2018). Approximately 1000 infected systems were Australian (Blackwood, 2015; Jervis 2013). CyptoLocker was utilising amongst others, an infection vector that was a peer to peer malware called ‘Gameover Zeus’ that was distributed by a spam botnet (Jervis 2013).

Beta-testing versions of CryptoLocker include code to connect to an IP address 184.164.136.134, located in a PhoenixNAP datacentre in Arizona, USA under the administrative control of Jolly Works Hosting (ibid). An analysis of the threat actors revealed use of Virtual Private Servers (VSPs) hosted by different Internet Service Providers (ISPs) throughout the Russian Federation and former Eastern bloc countries (Conti et al. 2018).

Australian law enforcement investigating these cases, where some of the victims are Australian, would have to coordinate their efforts with governments, law enforcement authorities, prosecutors, judges, forensic specialists and ICT services providers in the countries where the crime originated, the countries that hosted the ICT infrastructure that was used in the beta testing, hosting, deployment, propagation, encryption, payment, and decryption activities associated with these ransomware attacks.

Cybercrime cases that require international cooperation that are not catered for within existing legal instruments, create complexity and difficulty for law enforcement agencies (Brown 2015). To alleviate some of the difficulties in terms of cross-jurisdictional conflict of criminal laws necessitates managing provisions for double criminality with regard to extradition treaties, Mutual Legal Assistance (Watney 2016) and diplomacy (Brown 2015). Australia has recognised the value of interstate and international cooperation, through the establishment (ANZPAA 2018) of the Australia New Zealand Policing Advisory Agency (**A**NZPAA) **e**-**C**rime **W**orking **G**roup (AeCWG), the National Cybercrime Working Group (NCWG) and has acceded to the Council of Europe (CoE) Convention on Cybercrime (AG 2013) in a bid to achieve harmonised legal frameworks within which to pursue cyber criminals. The CoE is the gold standard for cooperation in fighting cybercrime, but is nonetheless a regional instrument with non-member participants, with notable exceptions such as China, North Korea, and Russia (Brittingham, 2017). Australia has also forged a number of bilateral relationships to boost its cyber policing capability and with recent agreements with Thailand, Singapore and China (SBS 2017). Besides the attempt to achieve legal harmonization, Australian law enforcement also has direct relationships with international law enforcement organisations such as INTERPOL, United Nations Office on Drugs and Crime, EUROPOL, ASEAN police chiefs and the 'Five-Eyes' police community spanning the United States of America, the United Kingdom, Canada and New Zealand (Kowalick et al. 2018).

An example of a transnational cooperative investigation of cybercrime is the operation against the 'Infraud Organization,' culminating in its takedown. The Infraud Organization was a transnational cybercriminal enterprise that was engaged in 'carding' or the large-scale acquisition, production and the trafficking of credit card information, bank account details, and personally identifiable information. The charges also include identity theft, production and use of counterfeit identification, bank fraud, wire fraud and money laundering (DOJ 2018a; USA v Bondarenko et al. 2017). The members of this criminal enterprise, including an Australian man Edgar Andres Viloria Rojas and the Ukranian founders, Svyatoslav Bondarenko and Sergey Medvedev, actively sought to evade law enforcement by maintaining their anonymity by utilising:

various forums and chatrooms controlled by the Infraud organisation, private messaging, email, ICT-chat, proxies, Virtual Private Networks (VPNs) and protected drop sites (ibid). It was also alleged that members laundered their proceeds through methods such as Liberty Reserve, Bitcoin, Perfect Money, WebMoney and other digital currencies (ibid). According to the Department of Justice, Infraud was responsible for an estimated $US530 million actual losses and intended losses of $US2.2billion (DOJ 2018a). The takedown was the result of an undercover operation by the Homeland Security Investigations who was able to purchase around 30 compromised credit card dumps belonging to Nevada cardholders in August 2017 (Olding 2017, USA v Svyatoslav Bondarenko et al. 2017).

The 'digital' dimension is forcing revisions of traditional methodologies (Hunton 2010, 2011a, 2011b). At the forefront of the rationale for adopting these new methods of forensics is the interception, monitoring, capture and storage of admissible digital evidence (Casey 2011a). Digital evidence can be defined as "any data stored or transmitted using a computer that can support or refute a theory of how an offense occurred or that address critical elements of the offense such as intent or alibi" (Casey 2011a). Maintaining the integrity of the digital evidence is an important function of law enforcement as they seek to prosecute the cybercriminals (Stanfield 2009; Shahzad et al 2011).Cybercriminals have embraced technological advances, and in many cases have harnessed the growing market for illicit digital services, leading to the large-scale profit driven industrialisation of crime (Wainwright & Ciffullo 2017), and these illicit digital services are posing major challenges to law enforcement. These technologies include encryption (Moore & Rid 2016), 'cryptomarkets' (Martin 2017), 'cyrptocurrencies' (Broseus et al 2017), Crime as a Service (CaaS) (Wainwright & Cilluffo 2017), and botnets (Dupont 2016).

Encryption technology provides for privacy, authentication, anonymity, anonymous payment and hidden exchanges (Moore & Rid, 2016). The availability and widespread use of full disk encryption makes search and seizure of disks particularly challenging, if not impossible, for law enforcement (Casey 2011b; Brown 2015). Critical to being able to retrieve digital evidence is the ability to implement on-scene forensic acquisitions from live computer systems by accessing them in their decrypted states as facilitated by warrants or in some cases as part of the controlled operations (AFP 2017) facilitating key logging malware to be used in surveillance of a suspect or as a last resort having the legal framework to compel the suspect to give up the encryption key (Brown 2015).

Another challenge posed to law enforcement investigations is the interception and decryption of end-to-end encrypted communications (Hess 2016) or the ability of criminals to 'go dark' (Caproni 2011). In his address to the 2018 Cyber Security Conference, Home Affairs Minister Peter Dutton cited the involvement of Australian law enforcement agencies in the takedown of the Phantom Secure group who had become a leading supplier of device to device encrypted communications (Crowe

2018). The investigation included a host of law enforcement agencies including the Australian Federal Police, the Australian Criminal Intelligence Commission, the New South Wales Crimes Commission, New South Wales Police, Queensland Police, South Australia Police, AUSTRAC, the Australian Tax Office, the Royal Canadian Mounted Police and the US Federal Bureau of Investigation (AFP 2018), showing high levels of cooperation and collaborative investigative work. Australian involvement in the investigation began in early 2017, following an exchange of intelligence with their US and Canadian counterparts, and resulted in 19 search warrants being executed across four Australian states, resulting in the seizure of 1000 encrypted mobile devices (DOJ 2018b) and the arrest of one individual for drug possession and trafficking. AUSTRAC's financial intelligence and information played a pivotal role in enabling investigators to follow the money trail and identify payments made by companies and individuals (AFP 2018).

Phantom Secure was a Canadian based business that was indicted by a federal grand jury on charges of "intentionally participating in a criminal enterprise that facilitated the transnational importation and distribution of narcotics through the sale and service of encrypted communications" (DOJ 2018b). The company advertised its products, that were repurposed Blackberry handsets, as impenetrable by decryption, interception or legal third-party records requests, also guaranteeing remote destruction of evidence if the device was compromised. (FBI 2018a). Phantom Secure gutted purchased Blackberry devices by removing much of the typical functionality such as calling, texting, web-browsing and GPS, and then installing their custom developed encrypted email system that only allowed the phones to communicate with each other. The encrypted data was supposedly routed through servers in Panama and Hong Kong, who were represented by the company, incorrectly as it turns out, as uncooperative with law enforcement. U.S. Attorney Adam Braverman summed up the challenges to law enforcement: "When criminals go dark, and law enforcement cannot monitor their phones or access evidence, crimes cannot be solved, criminals cannot be stopped and lives can be lost" (DOJ 2018).

Special Agent Nicholas Cheviron of the FBI's San Diego Division commented on the FBI's "enterprise approach" (Wainwright & Cilluffo 2017) to transnational organized crime: "Without arresting the principals and seizing the technology, including more than 150 domain names, you wouldn't be able to disrupt the communication." The AFP Assistant Commissioner of Organised Crime, Neil Gaughan, commented on the transnational nature and its impact on Australia: "The action taken in the U.S. directly impacts the upper echelons of organized crime both here in Australia and offshore, who until now have been able to confidently control and direct illicit activity like drug importations, money laundering and associated serious criminal offending" (DOJ 2018).

'Darknet' is a colloquialism that refers to a subset of the Internet which is cryptographically hidden (Moore & Rid 2016). The darknet is enabled by unique

software, such as TOR, I_2P and Freenet, that employs a distributed computing network to create encrypted and anonymised traffic flows (ibid). The dilemma for law enforcement is that the Tor browser can also be used to host hidden services, that can be used to provide illicit goods and services such as crime for hire, stolen identities, narcotics and child pornography and sexual exploitation material, forums and chatrooms (Jardine 2016; Martin 2014). The administrators and participants in these cryptomarkets try to evade law enforcement by virtue of a combination of encryption technologies, including the onion routing of the TOR network (Jardine 2016), the automated Pretty Good Privacy (PGP) encryption of all communications and the anonymity afforded by decentralised cryptocurrency-based payments (Broseus et al 2017). Law enforcement faces considerable obstacles when it comes to the Darknet, with many agencies undertaking proactive initiatives such as developing specialised units that target Darknet activity in an undercover capacity (Dubord 2008) or through controlled operations (AFP 2017).

Law enforcement has also successfully compromised Tor exit nodes by traffic monitoring or by introducing malicious code within Tor websites to trick users into revealing their true IP and location (Martin 2016; Poulson 2013). One challenge for law enforcement in keeping up with of cybercriminal trends is the expertise and awareness required across many different fields (Broadhead 2018) including finance, law, technology. This expertise might be highly specialised such as employing Artificial Intelligence (AI) based big data mining to analyse network traffic flows to cloud platforms (Daryabar el al. 2016) or across darknet exit nodes or blockchain cyptocurrency ledgers (Turner & Irwin 2018), or financial intelligence gathering (Chen & Nunamaker 2016) to pick up irregularities in ASX share trading data or superannuation funds (AUSTRAC 2017) or detection of botnets using Neural Networks (Obeidat 2017).

Law enforcement agencies and their legal counterparts, particularly the judges, need to be kept current through ongoing training in digital forensics, cybercrime, darknet, encryption, cryptocurrency operations and emerging technology trends in order to effectively investigate and prosecute cybercrimes (Brown 2015).

In a recent operation dubbed ‘Operation Disarray’ run by the FBI’s Joint Criminal Opioid Darknet Enforcement Team (J-CODE) comprising the Drug Enforcement Administration, U.S. Customs and Border Protection, IRS, Department of Homeland Security and the U.S. Postal Inspection Service, 160 individuals known to have bought or sold drugs from darknet marketplaces were targeted, searched, interviewed and some arrested. it was the first operation of its kind run simultaneously in all 50 states (French 2018, FBI 2018b). The message to law enforcement is clear; the investigation of these type of crimes requires a high level of coordination, multi-disciplinary team work, intelligence sharing and real-time synchronised and coordinated execution of operations. Special Agent Chris Best commented on the capability of law enforcement to pierce the anonymity provided by the dark net: “The point of Operation Disarray is

to put drug traffickers on notice: Law enforcement is watching when people buy and sell drugs online. For those who think the Darknet provides anonymity, you are mistaken" (FBI 2018b). Despite the multitude of takedowns these illicit cryptomarkets continue to be established (Broseus et al 2017; Décary-Hétu & Giommoni 2017), and their multi-faceted infiltration, intelligence gathering, investigation, and takedowns is an ongoing priority for law enforcement. A key facet in the investigation of these illicit markets is the incorporation of financial intelligence and for investigators to leverage off resources such as AUSTRAC and the ATO in Australia and the IRS-CI in the United States.

A Parliamentary Joint Committee on Law Enforcement (PJC-LE) inquiry into the gathering and use of criminal intelligence has identified the need for a single national repository for criminal intelligence. The current intelligence landscape is fragmented into state, territory and federal law enforcement agencies who work across national security, serious and organised crime and policing and community safety. An intelligence sharing solution across these domains, including sharing with international law enforcement partner organisation, will help provide an understanding of complex criminal behaviours and allow the formulation of appropriate preventative and investigative responses (PJC-LE 2013).

The challenges to law enforcement in Australia are further reinforced by a recent empirical study on the challenges facing specialist police cybercrime units conducted by Harkin et al (2018) in which they found that sheer volume of cybercrime, indicated by the ACORN reports, is imposing a very high work load on the law enforcement agencies in Australia and these agencies feel overwhelmed and under-resourced, with staff-retention flagged as an on-going issue (Harkin et al 2018). The more technically skilled staff were often lured to other teams or to the private sector. These challenges are being exacerbated by the ever increasing demand for more budgets and more resources as the scope of digital evidence and forensics due to the accelerated growth rate of computing devices and Internet of Things (IoT) devices (Tung 2017) has also resulted in individual cases being far more time-consuming as there are now far a greater number of objects of interest for the digital forensic analyst to investigate (ibid).

Australian law enforcement have a multitude of challenges in investigating and prosecuting cybercrime including trans-jurisdictional issues that can be managed through multilateral and bilateral relationships, and the harmonization of laws within which to prosecute criminals and take down criminal enterprises. The quandary of digital forensics is processing the massive volume of information in cyberspace and arriving at actionable intelligence from a prevention point of view and evidence for prosecution, where it comes to successfully prosecuting cyber criminals. The big data analysis techniques required to mine blockchain ledgers and the ability to disrupt detect and disrupt botnets are new skillsets that law enforcement needs. Such expertise may only reside within academia or the private sector, and the law enforcement challenge is to be able to work with trusted experts within the private sector or where there is a commercial incentive to the private sector partner, to novate the issue or at least the leadership to them (Kroeker 2011; Greene 2012). Successful

law enforcement operations have involved a range of different government agencies so that the political, financial, and criminal aspect of cybercrime can be attended to.

ACORN. 2017. ACORN Statistics Reports 1 Jul 2016 to 30 Jun 2017, accessed 22 Oct 2018, https://www.acorn.gov.au/resources

ACORN. 2018. ACORN Statistics Reports 1 Jul 2017 to 30 Jun 2018, accessed 22 Oct 2018, https://www.acorn.gov.au/resources

ACSC. 2017. 'ACSC 2017 Threat Report.' Australian Cyber Security Centre, Australian Government, accessed 22 Oct, 2018, https://www.acsc.gov.au/publications/ACSC_Threat_Report_2017.pdf

AFP. 2017. Controlled Operations Annual Report 2016-17, Part IAB of the Crimes Act 1914. Australian Federal Police.

AFP. 2018. 'International operation dismantles organised criminal enterprise operating encrypted communications,' 16 March 2018, Australian Federal Police media release, accessed 24 Oct, 2018, https://www.afp.gov.au/news-media/media-releases/international-operation-dismantles-organised-criminal-enterprise-operating

AG. 2013. 'National Plan to Combat Cybercrime.' Attorney General's Department, Australian Government, Commonwealth of Australia. Accessed 20 Oct, 2018, https://www.homeaffairs.gov.au/crime/Documents/national-plan-combat-cybercrime.pdf

ANZPAA. 2018. Cybercrime, Australia New Zealand Policing Advisory Agency, accessed 22 Oct, 2018, http://www.anzpaa.org.au/priorities/projects/cybercrime

APRA. 2016. 'Insights from APRA's 2016 Cyber Security Survey,' *Insight*, 2016, Issue 3, accessed 26 Oct, 2018, https://www.apra.gov.au/sites/default/files/Pages/insight-issue3-2016.html#private

APRA. 2017. 'Insights from APRA's 2017 Cyber Security Survey,' *Insight*, 2017, Issue 4, accessed 26 Oct, 2018, https://www.apra.gov.au/sites/default/files/Pages/insight-issue4-2017.html#article2

ASFA. 2018. 'Superannuation Statistics,' Association of Superannuation Funds of Australia, accessed 26 Oct, 2018, https://www.superannuation.asn.au/resources/superannuation-statistics

AUSTRAC. 2016. 'Australia's superannuation sector – Money Laundering and Terrorism Financing Risk Assessment,' accessed 26 Oct, 2018, http://austrac.gov.au/sites/default/files/super-annuation-risk-assessment-WEB.pdf

AUSTRAC. 2017. 'Australia's Securities and Derivatives Sector – Money Laundering and Terrorism Financing Risk Assessment,' accessed 26 Oct, 2018, http://austrac.gov.au/sites/default/files/securities-and-derivitives-ra-FINAL-2.pdf

Blackwood, Fiona. 2015. 'Cyptolocker virus: Australians forced to pay as latest encryption virus is 'unbreakable', security expert says.' 10 Aug 2015, accessed 22 Oct 2018, https://www.abc.net.au/news/2015-08-09/australians-paying-thousands-after-ransomware-virus-infection/6683618

Brenner, S. W. 2001. 'Cybercrime investigation and prosecution: the role of penal and procedural law.' *Elaw Journal : Murdoch University Electronic Journal of Law*, 8(2), pp.1–38

Brittingham, B. 2017. 'Cybercrime: An In-Depth Study into the Challenges and Impediments to Conducting Criminal Investigations in the Cyber Domain,' ProQuest Dissertations and Theses.

Broséus et al., 2017. A geographical analysis of trafficking on a popular darknet market. Forensic Science International, 277(C), pp.88–102.

Brown C.S.D. 2015. 'Investigation and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice.' International Journal of Cyber Criminology, Vol 9 (1), pp. 55-119.

Caproni, V. 2011. 'Going Dark: Lawful Electronic Surveillance in the Face of New Technologies.' Statement by Valerie Caproni, General Counsel, Federal Bureau of Investigation, before the House Judiciary Committee, Subcommittee on Crime, Terrorism, and Homeland Security, Washington, D.C. 17 February 2011, accessed 25 Oct, 2018, https://archives.fbi.gov/archives/news/testimony/going-dark-lawful-electronic-surveillance-in-the-face-of-new-technologies

Casey, E., 2011a. *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet,* Academic Press.

Casey E., 2011b. 'The growing impact of full disk encryption on digital forensics.' *Digital Investigation*, 8(2), pp.129–134.

Choo, K. R. 2011. 'Cyber threat landscape faced by financial and insurance industry.' *Trends & Issues in Crime and Criminal Justice*, Australian Criminal Intelligence Commission, Feb 15, 2011.

Conti, M., Gangwal, A. & Ruj, S. 2018. 'On the economic significance of ransomware campaigns: A Bitcoin transactions perspective.' *Computers & Security*, 79, pp.162–189.

CPDD. 2018. Statistics by Crimes Act/Criminal Code. Criminal Annual Reports Statistics, Charges Dealt with Summarily and on Indictment – Commonwealth Criminal Code 1995, 1 July 2016 to 30 June 2017, as accessed 20 Oct, 2018, https://www.cdpp.gov.au/statistics/additional-tables

Cross, C., 2018a. 'Expectations vs reality: Responding to online fraud across the fraud justice network.' *International Journal of Law, Crime and Justice*.

Cross, C., 2018b. 'There's a gap between what people expect when they report cybercrime, and what police can deliver,' *The Conversation*, 18 Sep, 2018, accessed 22 Oct, 2018, https://theconversation.com/theres-a-gap-between-what-people-expect-when-they-report-cybercrime-and-what-police-can-deliver-102781

Crowe, D. 2018. Increasing cyber-crime attacks 'costing up to $1b a year', Sydney Morning Herald, 11 April, 2018 as accessed 23 Oct, 2018, https://www.smh.com.au/politics/federal/increasing-cyber-crime-attacks-costing-up-to-1b-a-year-20180410-p4z8ui.html

Daryabar, F., Dehghantanha, A., & Choo, K. 2017. 'Cloud storage forensics: MEGA as a case study.' *Australian Journal of Forensic Sciences,* 49(3), 344-357.

Décary-Hétu, D. & Giommoni, L. 2017. 'Do police crackdowns disrupt drug cryptomarkets? A longitudinal analysis of the effects of Operation Onymous.' *Crime, Law and Social Change*, 67(1), pp.55–75.

Dent, C. 2009. 'Copyright as (decentred) regulation: digital piracy as a case study.' *Monash University Law Review*, 35(2), pp.348–375.

Desnoyers, S., Riddell, C., Gonnella, C., & Low, M. 2013. *The Challenges of Cybercrime for International Law Enforcement*, ProQuest Dissertations and Theses.

DOJ. 2018a. ‘Thirty-six Defendants Indicted for Alleged Roles in Transnational Criminal Organization Responsible for More than $530 Million in Losses from Cybercrimes,’ United States Department of Justice , 7 February 2018, accessed 26 Oct, 2018, https://www.justice.gov/opa/pr/thirty-six-defendants-indicted-alleged-roles-transnational-criminal-organization-responsible

DOJ. 2018b. ‘Chief Executive and Four Associates Indicted for Conspiring with Global Drug Traffickers by Providing Encryption Services to Evade Law Enforcement and Obstruct Justice,’ 15 Mar, 2018, accessed 24 Oct, 2018, https://www.justice.gov/usao-sdca/pr/chief-executive-and-four-associates-indicted-conspiring-global-drug-traffickers

Drew, J.M. & Farrell, L. 2018. ‘Online victimization risk and self-protective strategies: developing police-led cyber fraud prevention programs.’ *Police Practice and Research*, 19(6), pp.537–549.

Dubord, B. 2008. *Handbook of digital and multimedia forensic evidence* / edited by John J. Barbara., Totowa, N.J.: Humana.

Dubowitz, H. 2017. ‘Child sexual abuse and exploitation—A global glimpse.’ *Child Abuse & Neglect*, 66, pp.2–8.

Dupont, B. 2017. ‘Bots, cops, and corporations: on the limits of enforcement and the promise of polycentric regulation as a way to control large-scale cybercrime.’ *Crime, Law and Social Change*, 67(1), pp.97–116.

Farina, K.A. 2015. ‘Cyber Crime: Identity Theft.’ In *International Encyclopedia of the Social & Behavioral Sciences.* pp. 633–637.

FBI. 2018a. ‘International Criminal Communication Service Dismantled,’ 16 March 2018. Federal Bureau of Investigation. accessed 24 Oct 2018, https://www.fbi.gov/news/stories/phantom-secure-takedown-031618

FBI. 2018b. ‘Operation Disarray: Shining a Light on the Dark Web,’ 2 Apr, 2018, accessed 25 Oct, 2018, https://www.fbi.gov/news/stories/operation-disarray-040318

Fell, J., 2017. ‘Cyber crime - History: Hacking through history.’ *Engineering & Technology*, 12(3), pp.30–31.

French, L. 2018. ‘FBI Darknet Enforcement Team Completes First Operation Targeting Opioid Traffickers,’ *Forensic Magazine*, 3 April, 2018.

Garcia, E. et al., 2017. *Bitcoin Transaction Tracing and Purchasing Behavior Characterization of Online Anonymous Marketplaces Using Side Channels*., ProQuest Dissertations and Theses.

Glonti, A., 2015. ‘Money laundering via internet in Georgia.’ *European Scientific Journal*, 2015, Vol.11(SI), p.S39.

Greene, T. 2012. ‘Inside Microsoft botnet takedowns.’ *Network World (Online)*, p.25.

Hanson, F. 2018. ‘Time to admit we’re failing on cybercrime,’ 16 Feb 2018, The Strategist, Australian Strategic Policy Institute, accessed 20 Oct 2018, https://www.aspistrategist.org.au/time-admit-failing-cybercrime/

Harkin, D., Whelan, C. & Chang, L. 2018. ‘The challenges facing specialist police cyber-crime units: an empirical analysis.’ *Police Practice and Research*, 19(6), pp.519–536.

Hemphill, S.A., Tollit, M., and Kotevski, A. 2015. 'Predictors of Traditional and Cyber-Bullying Victimization: A Longitudinal Study of Australian Secondary School Students.' *Journal of Interpersonal Violence*, 30(15), pp.2567–2590.

Hess, A. 2016. 'Deciphering the Debate Over Encryption,' Statement by Amy Hess, Executive Assistant Director, Science and Technology Branch, Federal Bureau of Investigation before the House Committee on Energy and Commerce, Subcommittee on Oversight and Investigation Washington, D.C. 19 Apr, 2016, accessed 25 Oct, 2018, https://www.fbi.gov/news/testimony/deciphering-the-debate-over-encryption

Holt, T. J., Bossler, A. M., and Seigfried-Spellar, K. C. 2015. *Cybercrime and Digital Forensics : An Introduction*. Florence: Routledge. Accessed October 21, 2018. ProQuest Ebook Central.

Huang, C.T. & Gouda, M.G. 2006. 'Denial-of-Service Attacks. In Hop Integrity in the Internet.' *Advances in Information Security*. Boston, MA: Springer US, pp. 25–30.

Hui, D., Xin, C., & Khader, M. 2015. 'Understanding the behavioral aspects of cyber sexual grooming: Implications for law enforcement,' 17(1), 40-49.

Hunton, P. 2011. 'A rigorous approach to formalising the technical investigation stages of cybercrime and criminality within a UK law enforcement environment.' *Digital Investigation*, 7(3), pp.105–113.

Hunton, P. 2011. 'The stages of cybercrime investigations: Bridging the gap between technology examination and law enforcement investigation.' *Computer Law and Security Review: The International Journal of Technology and Practice*, 27(1), 61-67.

Hyman, P. 2013. 'Cybercrime: It's Serious, But Exactly How Serious? Association for Computing Machinery.' *Communications of the ACM*, 56(3), pp.18–20.

Jardine, E. 2016. 'The Dark Web Dilemma', Control Publications Pty Ltd, Hawksburn.

Jervis, K. 2013. CryptoLocker Ransomware, SecureWorks Counter Threat Unit Threat Intelligence, 18 Dec, 2013, accessed 22 Oct, 2018, http://www.secureworks.com/research/cryptolocker-ransomware

Kolias, C. et al., 2017. DDoS in the IoT: Mirai and Other Botnets. Computer, 50(7), pp.80–84.

Kowalick, P., & Connery, D. 2016. 'Special Report: Opportunities Abound Abroad: Optimising our Criminal Intelligence Systems Overseas.' Australian Strategic Policy Institute, Canberra.

Kowalick, P., Connery, D. & Sarre, R. 2018. 'Intelligence-sharing in the context of policing transnational serious and organized crime: a note on policy and practice in an Australian setting.' *Police Practice and Research*, 19(6), pp.596–608.

Kroeker, K. 2011. 'Microsoft Dismantles Rustock Botnet.' *Association for Computing Machinery. Communications of the ACM*, 54(5), pp.20–20.

Krone, T. & Smith, R. G. 2017. 'Trajectories in online child sexual exploitation offending in Australia.' *Trends & Issues in Crime and Criminal Justice*, (524), p.1.

Leukfeldt, E., Lavorgna, R. & Kleemans, A. 2017. 'Organised Cybercrime or Cybercrime that is Organised? An Assessment of the Conceptualisation of Financial Cybercrime as Organised Crime.' *European Journal on Criminal Policy and Research*, 23(3), pp.287–300.

Lewis, J. 2018. 'Economic Impact of Cybercrime – No Slowing Down.' Center for Strategic and International Studies (CSIS). February 2018. Accessed 26 Oct, 2018, https://csis-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf

Li, X. & Qin, Y. 2018. 'Research on Criminal Jurisdiction of Computer cybercrime.' *Procedia Computer Science*, 131, pp.793–799.

Li, W., Chen, H. & Nunamaker, J.F., 2016. Identifying and Profiling Key Sellers in Cyber Carding Community: AZSecure Text Mining System. Journal of Management Information Systems, 33(4), pp.1059–1086.

Lohachab, A. & Karambir, B., 2018. Critical Analysis of DDoS—An Emerging Security Threat over IoT Networks. Journal of Communications and Information Networks, 3(3), pp.57–78.

Martin, G. et al., 2018. WannaCry—a year on. BMJ, 361, pp.BMJ, 4 June 2018, Vol.361.

Martin, J. 2013. 'Lost on the Silk Road: Online drug distribution and the cryptomarket.' *Criminology and Criminal Justice*, Vol 14, Issue 3, 2014.

McCombie, S. 2008. 'Trouble in Florida: The Genesis of Phishing attacks on Australian Banks.' Australian Digital Forensics Conference, 1 - 3 December 2008. Edith Cowan University, Perth, Australia.

McCombie, S. 2011. *Phishing the Long Line : Transnational Cybercrime from Eastern Europe to Australia.* Macquarie University, Department of Computing.

Modecki, K.L., Mincbin, J., Harburgh, A.G., Guera, N.G., and Runions, K.C. 2014. 'Bullying Prevalence Across Contexts: A Meta-analysis Measuring Cyber and Traditional Bullying.' *Journal of Adolescent Health*, 55(5), pp.602–11.

Moore D. & Rid T. 2016. 'Cryptopolitik and the Darknet,' *Survival*, 58:1, 7-38.

Nicol, Sarah, 2012. 'Cyber-bullying and trolling.' *Youth Studies Australia*, 31(4), pp.3–4.

Obeidat, A.A. 2017. 'Hybrid Approach for Botnet Detection Using K-Means and K-Medoids with Hopfield Neural Network.' *International Journal of Communication Networks and Information Security (IJCNIS)*, 9(3), pp.305–313.

Olding, R. 2018. 'Australian man among 36 arrested in US cyberfraud takedown,' 8 Feb, 2018, Sydney Morning Herald, accessed 26 Oct, 2018, https://www.smh.com.au/world/north-america/australian-man-among-36-arrested-in-us-cyberfraud-takedown-20180208-p4yzna.html

Philippsohn, S. 2001. 'Money Laundering on the Internet.' *Computers & Security*, 20(6), pp.485–490.

PJCLE (Parliamentary Joint Committee on Law Enforcement). 2013. 'Inquiry into the gathering and use of criminal intelligence.' Canberra: Australian Parliament House.

Poulson, K. 2013. 'FBI ADMITS IT CONTROLLED TOR SERVERS BEHIND MASS MALWARE ATTACK,' 13 Sep, 2013 accessed 25 Oct, 2018, https://www.wired.com/2013/09/freedom-hosting-fbi/

Ryngaert, C. 2015. 'The concept of jurisdiction in international law,' in Orakhelashvili, A. (ed.), *Research Handbook on Jurisdiction and Immunities in International Law*, Cheltenham, UK : Edward Elgar Publishing, pp. 50 – 76.

Shahzad, S., Popov, O., & Dahman, R. 2011. 'Evaluation of Security Methods for Ensuring the Integrity of Digital Evidence.' *Innovations*, 2011 , pp. 220-225.

SBS 2017. ‘Aust, Asia boost cybercrime co-operation,’ *SBS News*, accessed 24 Oct 2018, https://www.sbs.com.au/news/aust-asia-boost-cybercrime-co-operation

Stanfield, A. 2009. *Computer forensics, electronic discovery and electronic evidence* (1st ed.). Chatswood, N.S.W.: LexisNexis Butterworths.

Tehrani M., & Manap, A. 2013. ‘A rational jurisdiction for cyber terrorism.’ *Computer Law & Security Review: The International Journal of Technology Law and Practice*, 29(6), pp.689–701.

Thompson, L., Riddell, C. M. & Cooper, H. R., 2014. ‘Defending against cybercrime. Defending against cybercrime.’ ProQuest Dissertations and Theses.

Tung, L. 2017. ‘IoT devices will outnumber the world's population this year for the first time,’ ZDNet, 7 February 2017, accessed 26 Oct, 2018, https://www.zdnet.com/article/iot-devices-will-outnumber-the-worlds-population-this-year-for-the-first-time/

Turner, A. & Irwin, A.S.M., 2018. ‘Bitcoin transactions: a digital discovery of illicit activity on the blockchain.’ *Journal of Financial Crime*, 25(1), pp.109–130.

UNODC. 2013. Comprehensive Study on Cybercrime Draft-February 2013. United Nations Office on Drugs and Crime.

USA v Bondarenko et al. 2017. ‘First Superseding Criminal Indictment 2:17-cr-306-JCM-PAL, United States District Court,’ District of Nevada, 31 Oct, 2017, accessed 26 Oct, 2018, https://www.justice.gov/opa/press-release/file/1032021/download

Wainwright, R., and Cilluffo, F.J. 2017. *Responding to Cybercrime at Scale: Operation Avalanche – A Case Study*, Centre for Cyber & Homeland Security, The George Washington University, accessed 24 Oct 2018, https://cchs.gwu.edu/sites/g/files/zaxdzs2371/f/Responding%20to%20Cybercrime%20at%20Scale%20FINAL.pdf

Wall, D. 2007. *Cybercrime : the transformation of crime in the information age*, Cambridge, UK ; Malden, MA: Polity.

Watney, M.M. 2016. ‘Cross-Border Law Enforcement: Gathering of Stored Electronic Evidence.’ *Journal of Information Warfare*, 15(3), pp.69–80.

Zhou, Y., Wang, X., Zhang, J., Zhang, P., Liu L., Jin, Huan, and Jin, Hongbo. 2018. ‘Analyzing and Detecting Money-Laundering Accounts in Online Social Networks.’ *Network*, IEEE, 32(3), pp.115–121.