SPECIAL REPORT

ASPI

March 2015

Underground web

The cybercrime challenge

Calum Jeffray and Tobias Feakin

ASPI
AUSTRALIAN STRATEGIC POLICY INSTITUTE

INTERNATIONAL CYBER POLICY CENTRE

Foreword

No longer can cybercrime be viewed as an emerging threat, for today it is well entrenched in criminal enterprises, has a marked impact in everyday crime and is ever present.

The fundamental basis for crime, and even crime types, have not changed greatly in the past 20 years, 50 years, 200 years. Crime is still motivated largely by profit and personal gain. What has changed are the tools, the methods and the systems used by criminal syndicates to achieve their objectives.

Cyber technologies create a new paradigm for the criminal—a more sophisticated method to attack the vulnerable—and a new fear for the victim. No longer is the evidence of the perpetrator visible to their victim. There are no smashed windows, broken doors or bones, but the trail of destruction can be no less devastating. Technology enables crime to exist before the victim is even aware that they're vulnerable.

Society's adaptation to the ever increasing world of technology provides unlimited potential for convenience,

Bitcoin is a digital peer to peer decentralized crypto-currency © Ted Soqui/Corbis.

choice, speed and customer satisfaction in the retail world, but it provides law enforcement with exponentially greater challenges when it comes to ensuring the integrity and safety of that online experience.

The technologies that society craves for its freedom, its expedience and its social livelihood are the same technologies that enable the criminal syndicate to exploit vulnerabilities in the network and the human psyche. And often from the relative anonymity of a residential basement in a town you have barely heard of, let alone been to.

Modern cybercrime draws no distinction between government targets, larger corporations and individual users. Its sole purpose is to exploit vulnerabilities for gain. Whether it is state-based, commercially driven or purely profit-driven crime against users, the methods of delivery are the same, and the tactics to defeat it must also be the same.

To be successful, law enforcement needs to be as innovative as its adversaries. Law enforcement must continue to adapt technologies, increase and import skills and enhance partnerships—but it must do this at a much faster rate than currently occurs.

As a signatory to the Budapest Convention, Australia is committed to the principles of achieving efficiency, and even harmony, in our laws, our investigation standards and methods and our relationships. Cybercrime sees no physical or geographical border as a barrier, and law enforcement must achieve the same through cooperation and synergy across international partnerships.

The two papers in this special report examine the central role that cybercrime plays in modern society and how technological developments create new opportunities for criminals to exploit. Calum Jeffray surveys the strategic cybercrime landscape and illustrates that, despite calls for law enforcement to ‘do more’ to prevent and investigate cybercrime, the agencies involved are often hampered in acting due to jurisdictional issues or the complexity of the investigations. Tobias Feakin examines the emergence of the ‘darknet’, where trading in illicit goods and services in online black markets has become increasingly commonplace and exacerbates the problems that law enforcement already faces—tracing and prosecuting illegal activities online. They are essential reading in what is an area of increased complexity and importance to fighting crime.

Commissioner Andrew Colvin
Australian Federal Police

Caught in the net: the law enforcement response to international cybercrime

Calum Jeffray

In late November 2014, Sony Pictures Entertainment confirmed that it had been the victim of a cyberattack in which large quantities of personal and commercial data—including employees' passwords, health-care files and social security numbers, as well as actors' and executives' salaries—were either stolen or destroyed. A group calling itself 'Guardians of Peace' claimed responsibility for the attack and subsequently issued threats against Sony and film theatres, ultimately leading to the cancellation of the premiere of the film *The interview*.

After the North Korean government was accused of being responsible for the attack, the situation quickly escalated into a major political incident and generated debate about the right to free expression and free speech in the digital era. What has largely been overlooked, however, is that this was one of the most high-profile international cybercrimes ever to have been committed. And while the attack has received wide condemnation, it's unlikely that the perpetrators will ever be caught or convicted of the crime, particularly if accusations of state involvement prove accurate.

Cybercrime can no longer be regarded as an emerging threat, but the reality of modern criminality. Today, almost all crime has a technological component to it, the numbers of internet users and internet-enabled devices continue to grow exponentially, and criminals (individuals, groups and networks) are able to rapidly exploit this, typically for financial gain.

There have been many calls for law enforcement to do more to prevent and investigate cybercrime, yet police are often hampered in acting because of jurisdictional issues or issues inherent in such investigations.[1] Unlike most 'traditional' crimes, cybercrime intersects with multiple jurisdictions simultaneously. Even if law enforcement agencies are able to trace the origin of an attack to a foreign jurisdiction, there can be significant challenges in securing and analysing evidence, especially in countries where there may be insufficient capacity or ineffective legal tools in place.

The Council of Europe Convention on Cybercrime—also known as the Budapest Convention—was the first intergovernmental treaty relating to cybercrime and was designed to address these challenges, particularly in the European context. Although the treaty's held up as a 'gold standard' for cybercrime investigation techniques and international cooperation, it's not without its critics. Ten years after the convention began to come into force in some European countries, this paper explores whether or not it continues to provide an effective and practical tool for law enforcement agencies, and suggests what more those agencies can do to fight global online crime.

Cybercrime: an increasingly sophisticated threat

The threat from cybercrime can be generally divided into two broad categories. *Cyber-dependent* crime includes the spreading of viruses and other malware, hacking into systems and launching distributed denial of service (DDoS) attacks. *Cyber-enabled crimes* are crimes, such as fraud and money laundering, that can be increased in their scale or reach by the use of computers, networks or other forms of ICT.[2]

Despite near-universal agreement that the threat from cybercrime is serious and increasing, obstacles remain in accurately measuring its scale and impact. While there have been a number of attempts to quantify the scale of cybercrime, particularly on national levels, their methodologies and assumptions are often challenged. The optimal method of measuring the impact of cybercrime is often disputed; proposed options have included the volume of attacks, the volume of data stolen, the value of data stolen, the cost of repairing the damage following an attack, and so on. The result is a general lack of evidence on the issue compared to other criminal activities.

Despite this evidence deficit, analyses of trends suggest considerable increases in cybercrime in terms of its scope, sophistication, number and types of attacks, number of victims, and economic damage. While attacks on well-known companies and brands regularly attract the attention of the world's media, much less attention is arguably paid to 'lower level' cybercrimes committed against individuals. According to the *Financial Times*, 'Though they might not receive the same amount of news coverage, no one should harbour any ideas these acts—which range from bank fraud to online child sexual exploitation—are any less serious because they are not targeted against a large number of people.'[3]

Like all types of crime, these acts are committed by both opportunistic individuals and organised crime groups, and it has become increasingly apparent that specialised expertise isn't a prerequisite for committing cybercrimes. Criminals with limited technical competence are able to commit crimes online simply by purchasing specialist services, particularly as 'Any kind of cybercrime can be procured even without technical skills—password cracking, hacking, tailor-made malware or DDoS attacks.'[4]

Commentators suggest that these highly sophisticated online marketplaces operate as fluid 'transactional' networks, in which criminals offer their services to the highest bidder, rather than through allegiance to particular organised crime groups. As noted by *The Independent,* this new breed of criminal organisation operates differently from traditional hierarchical mafia-style gangs, 'with a fluid structure of specialists often working to order to develop programmes for criminal gangs planning specific online scams'.[5]

The vast majority of cybercrimes are in the pursuit of financial gain. While many criminals continue to steal money directly (by unlawfully gaining access to online bank accounts, for example), it's increasingly common for them to target large volumes of personal and corporate data, which can be repeatedly sold on to other criminals via underground markets. Recent notorious examples include the theft of personal and identification information for 70 million customers of US retailer Target in 2013 and the theft of 56 million customer payment cards from Home Depot in 2014; in October 2014, the accounts of 76 million JP Morgan customers were hacked.[6]

While cybercriminals will continue to target the networks of businesses and large commercial organisations, commentators suggest that the sophistication of cybercrimes targeting individual users will increase, particularly personalised scams. New and popular devices, content platforms and payment systems are other likely future targets. 'Criminal hackers tend to attack popular platforms where the yield is likely high', according to internet security firm Kaspersky Lab. 'If no one adopts Apple Pay, then no one will target it. However, if Apple Pay is as popular as Apple's other traditional and mobile offerings, then we may be writing about Apple Pay hacks sooner rather than later.'[7]

Other concerns relate to the ways in which criminals are likely to exploit social media (malware embedded in Facebook videos surfaced in 2014), the anonymity offered by the dark web, or the increased number of potential vulnerabilities associated with the 'internet of things' (some fear that criminals will soon be able to hack directly into our homes, cars and wearable technology). A final concern is the potential role of states, as the boundary between criminal and state involvement in particular crimes begins to blur (evidenced by the attack on Sony in November).

What these future concerns have in common is that they all make it more difficult for law enforcement to identify the perpetrators. The attribution problem associated with cyberattacks is widely known and well documented, and is compounded by the fact that the origin of the attack may be overseas. Cybercrime operations often span multiple jurisdictions and, as the Sony hack demonstrates, the transnational nature of much cybercrime continues to present one of the most significant obstacles to law enforcement. That said, it's important to dispel the myth that cybercrimes originate only from 'bad' countries, since anywhere that's an attractive place to conduct legitimate business online also tends to be an environment conducive to cybercrime. Countries with sophisticated IT infrastructure—which is both cheap and easy to use—and global financial and logistical hubs are particularly attractive places for criminals to launch cyberattacks.

However, such locations are also attractive *targets* for cybercriminals. In its 2014 *Internet Organised Crime Threat Assessment*, the European Cybercrime Centre suggests that 'The European Union is a key target for cybercrime because of its advanced Internet infrastructure, rates of adoption and increasingly Internet-mediated economies and payment systems.'[8] The assessment goes on to suggest that 'new international strategic and operational partnerships' will be the key to combating future cybercrime threats.[9]

There are three main reasons why the transnational nature of cybercrime creates difficulties for law enforcement. First, the level of information exchange and cooperation between law enforcement agencies in different countries can be poor. Even when dealing with cooperative jurisdictions, slow and cumbersome mutual legal assistance treaty processes can significantly hamper investigations, and the disproportionate effort involved in even modest cases is a constraint in times of austerity.[10]

Second, the country where the perpetrator is based mightn't have the necessary capacity or sufficient skills and knowledge to conduct a suitable investigation, determine the source or identity of the perpetrator, or acquire and preserve the necessary evidence.

Finally, the country in which the culprit is located may have insufficient legislation or legislation that's incompatible with that of the victim's country, making investigations and prosecutions extremely difficult and even impossible in some cases. One well-known example is the 'Love Bug' computer worm that was developed in the Philippines in 2000 and reportedly infected millions of computers worldwide. Local investigations were hindered by the fact that the malicious development and spreading of damaging software was not, at the time, adequately criminalised in the Philippines.[11]

A more coordinated approach: the Budapest model

The member states of the EU have a long history of cooperation on transnational crime, from setting up the Trevi group in 1976 to tackle terrorism and coordinate policing to the establishment of the European Police Agency (Europol) in 1998. Despite these institutional efforts, the rapid and effective cooperation often needed in response to cybercrime could still be hampered by the varying legislation within each country, as well as the burdensome requirements of mutual legal assistance treaties. According to the UN Office on Drugs and Crime, a large number of existing treaties are still based on 'formal, complex and often time-consuming procedures. The establishment of procedures for quick responses to incidents and requests for international cooperation is therefore considered vital.'[12]

One approach to overcoming this problem, improving international cooperation and addressing the transnational dimension of cybercrime is to develop and standardise relevant legislation. Even within the EU, differences in legislation and legal instruments to detect, attribute and exchange information in relation to cybercrimes cause significant impediments, not only to law enforcement *per se* but also to law enforcement agencies' cooperation with the private sector.[13]

While a number of legal developments have taken place in recent years, the Convention on Cybercrime remains the only intergovernmental treaty relating to cybercrime. In 1997, the Council of Europe appointed the Committee of Experts on Crime in Cyberspace to identify and define new crimes, jurisdictional rights and criminal liabilities concerning the internet.[14] In addition to the council's 47 member countries, Canada, Japan, South Africa and the US were invited to participate in the discussions as observer nations. As noted by one scholar:

> The goal was to create a set of standard laws concerning cybercrimes for the global community and create a common criminal policy to protect against cybercrimes. The country representatives sought to make it easier for law enforcement to cooperate in collecting evidence in investigating computer crimes.[15]

The first states signed the treaty in November 2001, and it began to come into force in July 2004. By January 2015, 44 nations had ratified the convention, including many non-European countries such as Australia, the Dominican Republic, Japan and the US.[16] Other countries—such as Argentina, Egypt, Pakistan and the Philippines—have modelled parts of their legislation on the convention without formally acceding to it.[17]

In addition to outlining the use of a common lexicon, the text of the convention requires state parties to do the following:[18]

1. *To establish specific types of conduct as criminal offences in domestic legislation*

   Theses offences include, among others, illegal access, illegal interception, data interference, system interference, misuse of devices, computer-related forgery, computer-related fraud, offences related to child pornography, and offences related to copyright.

2. *To provide criminal justice authorities with effective means for investigations*

   This section outlines procedural law issues, such as the search and seizure of computer data, the expedited preservation of stored data, and the interception and collection of communications data.

3. *To engage in efficient international police and judicial cooperation*

   This section relates mainly to parties providing real-time assistance to one another, including points of contact available 24 hours a day, 7 days a week. It also

> requires parties to ensure that their law enforcement responders are properly trained and equipped, and provide appropriate technical assistance to others when necessary.

One of the biggest perceived successes of the convention is that it exists in the first place. Given the multitude of perspectives of the vast number of stakeholders involved (particularly non-state actors), the negotiation of treaties relating to cybersecurity is notoriously challenging. As one commentator has noted, the internet and ICT sector today involves such a large number of stakeholders that 'it would seem very difficult to bring all interests under an international agreement of the scope and depth of the Budapest Convention.'[19]

Ten years after the convention was signed, Thorbjørn Jagland, Secretary General of the Council of Europe, praised the success of the treaty and claimed that:

> The convention has proven to work. Thanks to it, there has been a broad harmonisation of cybercrime legislation, not only in Europe but worldwide. In addition, offences such as illegal access to computer data or illegal interception of computer data or computer-related forgery or fraud, have been criminalised.[20]

There's also evidence of increased cooperation at the operational level, particularly in the context of Europol, which launched the European Cybercrime Centre in January 2013 and its Joint Cybercrime Action Taskforce in September 2014. This has allowed for the coordination of international investigations into some of the most serious cybercrime threats of recent years. Three of the largest investigations are detailed below.

Operation Tovar

In May 2014, 10 national law enforcement agencies took part in an operation to disrupt the Gameover Zeus botnet and seize computer servers crucial to malicious CryptoLocker software. Gameover Zeus was a sophisticated type of malware designed to steal banking and other credentials from the computers it infected, which was then used to transfer money to accounts controlled by the criminals. More than a million computers worldwide were infected by the malware.[21] The infected computers also distributed ransomware known as CryptoLocker, which encrypted all files on the victim's computer until a ransom was paid to buy the password necessary to unlock the files. After the law enforcement agencies disrupted the criminal infrastructure by taking control of the domains and arresting a suspect from Anapa in Russia, the then head of the European Cybercrime Centre, Troels Oerting, said, 'This big, and very successful, operation has been an important test of the EU Member States' ability to act fast, decisively and coordinated against a dangerous criminal network.'[22]

Remote access Trojans

In November 2014, Europol and several law enforcement and judicial authorities carried out actions against EU citizens suspected of using remote access Trojans (RATs). RATs are malware used to spy on victims' computers and access personal information, record on-screen, webcam and microphone activity, and collect passwords or credit card details. Fifteen people were arrested in several European countries, including France, Romania, Latvia, Italy and the UK. Troels Oerting once again attributed the success of the operation to 'an alliance of EU law enforcement agencies' joining forces, allowing them to collate intelligence, analyse collective data to identify the perpetrators, and coordinate action and arrests.[23]

Operation Onymous

Also in November 2014, representatives from the law enforcement agencies of 17 countries gathered at Europol to collaborate on one of the biggest operations against dark-web websites. The action aimed to stop the sale, distribution and promotion of illegal and harmful items, including weapons and drugs, sold in online 'dark' marketplaces. The primary target was the notorious Silk Road 2.0 site, although an additional 413 illicit services were reported to have been shut down. Recognising the way that criminals use the dark web and 'hide behind international borders so they can stymie law enforcement', US Assistant Attorney-General Leslie Caldwell praised the way 'the global law enforcement community has innovated and collaborated to disrupt these "dark market" websites'.[24]

National to global: addressing vulnerabilities

While cooperation between countries may have improved since the Budapest Convention first came into force a decade ago, and there have been operational successes, Europol recognises that a number of shortcomings remain in the approach of European law enforcement to cybercrime:

> EU law enforcement, Europol included, has not fully conceptualised how to integrate this cyber dimension into all relevant aspects of police work, let alone devise a strategy and implementation plan to make this happen.[25]

Not all these shortcomings can be blamed on the Budapest Convention, although the agreement continues to attract its critics, particularly those who believe it to be a largely 'symbolic' treaty, likely to have only a 'limited effect on cybercrime in the long-term'.[26]

One reason for this criticism has been that ratification or accession to the convention has been slower than expected. In some countries, the treaty has come into force only recently, while some key European nations—Greece, Ireland and Sweden—have yet to ratify it. While recognising that '[t]he impact of the Convention on Cybercrime cannot be measured solely by the number of States that have signed or ratified the Convention', the UN Office on Drugs and Crime noted in 2010 that 'compared to global standards, the number and speed of signature and ratification certainly remains an issue'.[27] This delay may be due in part to the time needed to implement the appropriate legislative measures, since all provisions within the convention are required to be reflected in domestic legislation by the time of ratification or accession.

Even though the treaty outlines specific laws that need to be passed, there may also be inconsistencies from country to country in how those laws are written and applied. This

This photo provided by the Dutch Ministry of Security and Justice on 13 February 2014 shows weapons and ammunition purchased by undercover police. Five men have been arrested in Germany and the Netherlands in a sting operation against a website allegedly used to sell illegal drugs and weapons © AP via AAP/Dutch Ministry of Security and Justice.

is particularly true in relation to laws about the interception and retention of communications data for the purposes of law enforcement—a topic that remains controversial in much of Europe. From the perspective of law enforcement, the limits currently placed on how much data can be held and for how long mean that police cannot effectively trace and prosecute criminals. Europol's *Internet Organised Crime Threat Assessment* claims that:

> Current data retention laws are insufficient for law enforcement. The majority of intelligence and evidence for cyber investigations comes from private industry. With no data retention, there can be no attribution and therefore no prosecutions. In this context a new EU Directive on data retention following the European Court of Justice's annulment of the existing measure is urgently required.

Critics, however, argue that extending the powers of law enforcement agencies in this area would unnecessarily intrude upon the privacy of citizens.

A final criticism is that membership of the treaty is confined to EU members and selected others, which limits the effectiveness of efforts to improve international cooperation. A number of important countries haven't signed or ratified the convention, including countries with some of the highest cybercrime rates in the world, such as Russia, China, India and Brazil. This has led the CEO of Kaspersky Lab to describe the Budapest Convention as a 'convention of the victim countries'.[28] Because the treaty was prepared by the Council of Europe and not by, say, the UN, it's also difficult to persuade some countries to now join the treaty. Experience has shown that, regardless of the subject, states are generally reluctant to ratify or accede to conventions that they haven't contributed to developing or negotiating.[29]

Not all the challenges for law enforcement derive from the Budapest Convention, and political and legal agreements can only go so far in supporting law enforcement in combating the threat from cybercrime. Many of the most significant challenges for agencies in relation to cybercrime involve problems of capacity, process and even cultural mindset at the national and subnational levels.

Information sharing and, in particular, the real-time exchange of information between agencies remain an ongoing challenge. Effective data sharing is becoming more critical than ever, given the speed at which cybercrime can occur. As noted by the *Financial Times*, while there are plenty of proposals for information exchange on cybercrime under discussion, 'they now need to be implemented so that all those involved have effective and sustainable systems for sharing large volumes of data across organisational boundaries'.[30]

Taking into account the complexity of the issue and constant developments in technology, there's a continuing need for sustained recruitment of specialists and ongoing training for law enforcement officers involved in investigations. In November 2014, the inspectorate responsible for assessing police forces in England and Wales found that 'the gap between the threat and police capability is widening'.[31] It concluded that police are 'falling behind the curve of rapidly changing criminality' because of a 'deficit in the skill and experience of the investigating officers'. [32] It suggested that one of the reasons for this is that law enforcement agencies are struggling to recruit enough high-calibre technology experts—many of whom are able to command higher salaries in the private sector—and called for a fundamental rethink on police recruitment to tackle cybercrime.

Rob Wainwright, Director of Europol, has suggested that 'Across the board in Europe, the police are really struggling to get the right guys through the doors because they can't afford to pay the rates that criminals and the tech guys do', admitting that 'We're not getting the right people and there's not enough training of existing cops.'[33]

Given that most crimes now have a technological component, and the number of 'low-level' cybercrimes affecting the public at large will only increase in future, tackling cybercrime should be the responsibility of all officers, rather than a select few. In the context of new forms of online abuse, the use of digital currencies and the consumption of radical and extreme content, for example, police officers need to be trained to understand these emerging crimes and to distinguish between cases that require police attention and those that don't.[34] To both disrupt and prevent cybercrime, significant changes may be needed in the working culture of some police forces to see beyond traditional (and of course national) boundaries. In the light of the report on policing in England and Wales, for example, *The Independent* reported on the changes needed to the 'tribal' behaviour of different forces, in which 'police and agencies [are] protecting their own sources and techniques in a fractured response to an area of crime that has been identified as a key national security threat'.[35]

Finally, wider public perceptions of cybercrime need to be addressed. In particular, the scale of under-reporting of cybercrimes remains considerable. According to the UK Home Office, just under 1% of adult internet users report unauthorised access to their data to the police, while businesses report just under 2% of online incidents. Part of the reason for such low levels of reporting is likely to be the victims' belief that there's little that the police could or would do.[36] A further consequence of under-reporting is that cybercrimes don't commonly feature among national crime statistics; where such data is available, it's often not detailed enough to provide reliable information about the scale or extent of offences.[37]

National capabilities for international efforts

In countries such as the UK, it's increasingly recognised that cybercrime is not an emerging threat but the reality of crime now, and that forces need to adapt quickly to meet the threat.[38] Given the inherently transnational nature of cybercrimes and the complexities involved in investigating them, coordination and cooperation between law enforcement agencies operating in different jurisdictions are crucial. The ratification of the Budapest Convention by many countries has certainly helped them in this regard and has paved the way for increased institutional capacity, particularly within Europol.

However, agreements such as the convention can only go so far in combating international cybercrime. At the national level, more needs to be done to understand the scale of the problem in each country by encouraging individuals and businesses to report cybercrimes, as well as by improving the recording of such crimes. Given the pace of technological change and continual increases in the sophistication of criminal attacks, law enforcement agencies must also possess the necessary capabilities, skilled officers and expertise and provide ongoing training to fulfil the obligations laid out in the Budapest Convention. To do so, they must recognise the cultural changes they must make in their organisations to address such a rapidly changing threat as cybercrime.

As the recent attack on Sony reminds us, international cybercrime is an important strategic issue. Responding to such an attack (particularly if it involves state collusion) is extremely difficult for law enforcement agencies. There's potential for cross-border cooperation through the framework of the Budapest Convention, but better coordination at the international level shouldn't be to the detriment of ensuring that national capabilities are sufficient to address the threat. There's still much that can be done at the national and subnational levels to ensure that law enforcement agencies are able to work jointly with their counterparts overseas more effectively. Without these national building blocks in place, cybercriminals, such as those who launched the attack on Sony, are likely to continue to slip through the net.

Notes

[1] Nancy Marion, 'The Council of Europe's cyber crime treaty: an exercise in symbolic legislation', *International Journal of Cyber Criminology*, 4(1–2):699.

[2] M McGuire and S Dowling, *Cyber crime: a review of the evidence*, Home Office Research Report 75, October 2013.

[3] 'View: Police must face up to cyber threats', *Financial Times*, 16 December 2014.

[4] 'European Cybercrime Centre—one year on', media release, European Commission, 10 February 2014.

[5] Director of Europol: "Top computer graduates are being lured into cybercrime"', *The Independent*, 29 December 2014.

[6] JP Morgan sees 76 million customer accounts hacked', *BBC News*, 3 October 2014.

[7] 'Kaspersky's global research and analysis team's nine security predictions for 2015', *Kaspersky Lab Daily*, 10 December 2014, online.

[8] Europol, *The Internet Organised Crime Threat Assessment (iOCTA) 2014*, European Police Office, The Hague, 2014, 3.

[9] Europol, *The Internet Organised Crime Threat Assessment (iOCTA) 2014*.

[10] Europol, *The Internet Organised Crime Threat Assessment (iOCTA) 2014*, 69–70.

[11] UN, *Twelfth United Nations Congress on Crime Prevention and Criminal Justice*, Salvador, Brazil, 12–19 April 2010, online.

12 UN, *Twelfth United Nations Congress on Crime Prevention and Criminal Justice*, 4.

13 Europol, *The Internet Organised Crime Threat Assessment (iOCTA) 2014*, 9.

14 Marion, 'The Council of Europe's cyber crime treaty'.

15 Marion, 'The Council of Europe's cyber crime treaty'.

16 Council of Europe, *Convention on Cybercrime*, online.

17 UN, *Twelfth United Nations Congress on Crime Prevention and Criminal Justice*, 11.

18 Council of Europe, *Convention on Cybercrime*.

19 Alexander Seger, *The Budapest Convention on Cybercrime 10 years on: lessons learnt or the web is a web*, Council of Europe, online.

20 Thorbjørn Jagland, 'Budapest Convention on Cybercrime—10th anniversary meeting', speech given in Strasbourg, Council of Europe, 23 November 2011, online.

21 Federal Bureau of Investigation (FBI), 'GameoverZeus Botnet disrupted', FBI, Washington DC, 2 June 2014, online.

22 'International action against "Gameover Zeus" botnet and "Cryptolocker" ransomware', media release, Europol, 2 June 2014.

23 'Users of remote access trojans arrested in EU cybercrime operation', media release, Europol, 20 November 2014.

24 'Dozens of online "dark markets" seized pursuant to forfeiture complaint filed in Manhattan federal court in conjunction with the arrest of the operator of Silk Road 2.0', media release, FBI, Washington DC, 7 November 2014.

25 Europol, *The Internet Organised Crime Threat Assessment (iOCTA) 2014*, 71.

26 Marion, 'The Council of Europe's cyber crime treaty', 702.

27 UN, *Twelfth United Nations Congress on Crime Prevention and Criminal Justice*, 11.

28 Eugene Kaspersky, keynote speech, International engagement on cyber: developing international norms for a safe, stable, and predictable cyber environment, Georgetown University, 10 April 2013, online.

29 UN, *Twelfth United Nations Congress on Crime Prevention and Criminal Justice*, 12.

30 'View: Police must face up to cyber threats', *Financial Times*, 16 December 2014.

31 Her Majesty's Chief Inspector of Constabulary, *State of policing: the annual assessment of policing in England and Wales 2013–2014*, Her Majesty's Chief Inspector of Constabulary, London, November 2014, 22.

32 Her Majesty's Chief Inspector of Constabulary, *State of policing.*

33 'Director of Europol: "Top computer graduates are being lured into cybercrime"', *The Independent*, 29 December 2014.

34 Her Majesty's Chief Inspector of Constabulary, *State of policing*, 16.

35 'Police "failing to train key staff to fight growing threat of cyber crime"', *The Independent,* 7 December 2014.

36 McGuire and Dowling, *Cyber crime: a review of the evidence*, 6–7.

37 UN, *Twelfth United Nations Congress on Crime Prevention and Criminal Justice*, 2.

38 Her Majesty's Chief Inspector of Constabulary, *State of policing*, 7.

Cryptomarkets—illicit goods in the darknet

Tobias Feakin

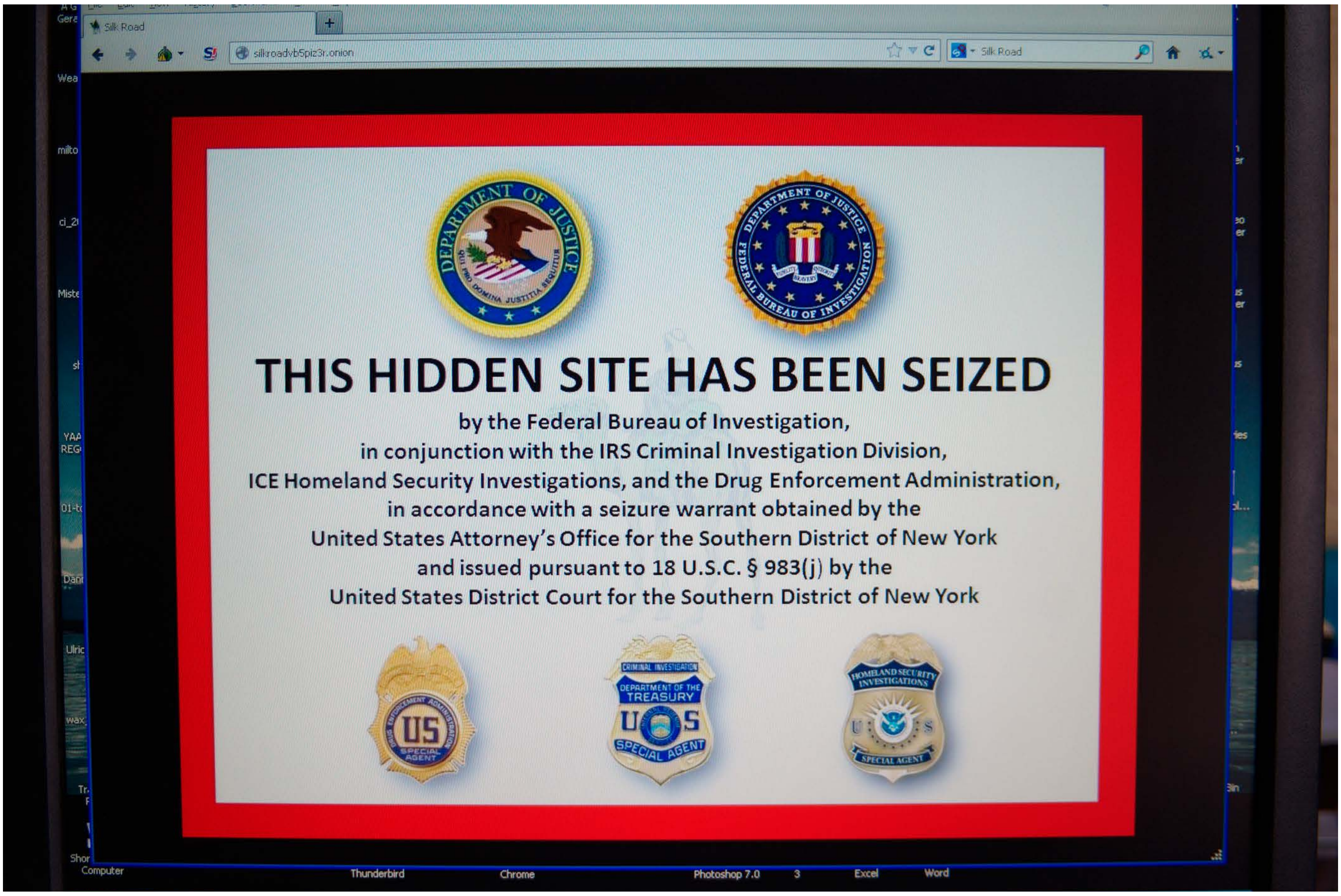
An environment such as cyberspace, where possible gains are high, the probability of capture is low and deniability rules, is a highly attractive medium for the whole range of threat actors. Nowhere is this exemplified more potently than in the 'darknet'—a part of the 'deep web'[1], where content isn't accessible through traditional search engines such as Google and where access is anonymous and largely untraceable. In the darknet, trading in illicit goods and services in online black markets has become increasingly commonplace and exacerbates the problems that law enforcement already faces in tracing and prosecuting illegal activities online.

This paper examines the growth of cryptomarkets in the darknet, the current and future challenges that they present for law enforcement agencies, and measures that the agencies could take to improve law enforcement responses.

The end of the beginning—the Silk Road take-down

In October 2013, the US Federal Bureau of Investigation (FBI) was celebrating the arrest of Ross Ulbricht (alias 'Dread Pirate Roberts') and the take-down of his online marketplace, Silk Road. He was believed to have amassed around US$80 million from Silk Road, where people bought a range of legal and illegal goods and data, such as drugs, 'exploit' software kits, credit card details and fake identification. However, despite the taking down of Silk Road, the past year has produced a larger problem: a diversification of cryptomarkets that are expanding to meet the demand of an ever increasing clientele.

Publicity about the take-down of Silk Road caused some of that growth, but so did the cryptomarkets' mimicking of legal e-commerce sites such as eBay and Amazon, where convenience, product choice, price and peer review play a



THIS HIDDEN SITE HAS BEEN SEIZED

by the Federal Bureau of Investigation,
in conjunction with the IRS Criminal Investigation Division,
ICE Homeland Security Investigations, and the Drug Enforcement Administration,
in accordance with a seizure warrant obtained by the
United States Attorney's Office for the Southern District of New York
and issued pursuant to 18 U.S.C. § 983(j) by the
United States District Court for the Southern District of New York

Silk Road, the best-known underground marketplace for the trade of illegal drugs on the internet has been closed by the US authorities after an arrest of Ross William Ulbricht, alleged to be the owner of the site, screengrab 3 October 2013 © David Colbran/Demotix/Corbis.

large role. In July 2014, the BBC reported that listings of illegal drugs online in the darknet had more than doubled from the previous year.[2] In October 2013, there were 18,174 drug listings in four major markets; by 31 July 2014, there were 43,175 in 23 markets. Three of the largest markets were Silk Road 2.0 (largely based on its predecessor), Agora and Evolution, each of which had more listings than the original Silk Road did at the time of its demise.[3]

Those three markets all ban child pornography, but their other operating principles vary greatly. Silk Road 2.0 focused on drugs, while Agora also sells weapons. However, the fastest growing of all is Evolution, which has the loosest restrictions and advertises guns, stolen credit-card data, stolen medical information and fake identification. Evolution's popularity has been driven not only by its amoral approach compared with the original Silk Road, which had a strict libertarian ethos, but also by its more professional operation and its offer of more secure transactions. One security feature that separates it from its competition is a bitcoin payment feature called 'multi-signature transactions'. When a purchase is made, users deposit their bitcoins in an escrow account created by Evolution. The account is controlled by Evolution's administrators, the buyer and the seller. At least two of the three must authorise the transaction before the payment is made. This means that it's far more difficult for the bitcoins to be stolen or be seized by law enforcement officials. To add to the difficulties for law enforcement and the appeal for users, the site also provides encryption when logging on, when activated users are required to decrypt a message with a private Pretty Good Privacy (PGP) key.[4]

However, these markets aren't the most malicious parts of the darknet. There are genuine concerns that the darknet provides a haven for dealers in child pornography, contract killers, human traffickers, terrorists and sellers of state secrets. One alarming study from the University of Portsmouth stated that, even though drug forums and contraband markets are the largest single category of sites hidden in the darknet, traffic to those sites is dwarfed by visits to child pornography sites. Four out of five visits to hidden services sites were to sites holding paedophilic content.[5]

A recent RAND report examined the growth of activity in such marketplaces and concluded not only that black markets are growing in size and complexity, but that the hacker market in particular had developed considerably over the past 20 years:

> The hacker market—once a varied landscape of discrete, ad hoc networks of individuals initially motivated by little more than ego and notoriety—has emerged as a playground of financially driven, highly organized, and sophisticated groups. In certain respects, the black market can be more profitable than the illegal drug trade; the links to end-users are more direct, and because worldwide distribution is accomplished electronically, the requirements are negligible.[6]

The report noted how resilient these black markets had become after law enforcement actions, which had led to higher levels of encryption and more rigorous and aggressive vetting of individuals. This means that law enforcement agents attempting to infiltrate these groups (a common tactic in the past) will find such attempts more challenging in the future.

Anonymity online—the Tor browser

The key to these activities is the relative anonymity that users have when accessing the darknet using via browsers such as Tor (The Onion Router, known by that name because of the layers of encryption that surround and obscure the data being passed back and forth when it's used). The genesis of Tor was in the research of three US Naval Research Laboratory scientists. As late as 2011, the US Government supplied 60% of its funding, and Google supports the non-profit organisation that administers it.[7] There are plenty of reasons why the US Government would fund such a tool: military and intelligence agencies could use it for covert communications, and police could use it to receive anonymous tips and investigate illegal online activities without alerting the targets. It has also provided an avenue for dissidents and journalists living under authoritarian regimes to speak out and communicate with others beyond their borders.[8]

The ability to browse illegal goods anonymously and the growth in cryptocurrencies that allow relatively anonymous payment for those goods make it hard for law enforcement to keep up. Bitcoin have been the most well-known cryptocurrency, but is now becoming passé. New currencies, such as Zerocash, which claims to be a privacy-preserving version of its predecessor, are increasing the headache for hi-tech crime units around the world.[9]

Law enforcement fights back

As evidenced since the Silk Road take-down, police have a real problem on their hands. As soon as the authorities shut down cryptomarkets, they reappear in another place, with stronger vetting of users and greater encryption capabilities. However, police have had some wins.

In February 2014, Dutch and German police shut down Utopia, a similar darknet site, as part of Operation Commodore. Utopia had been used to trade drugs, stolen credit cards, weapons and a host of other illegal goods. The site was up and running for only nine days, but in that time there were around 13,000 listings, many offering global postage services—illustrating how popular such sites have become. Police made five arrests and confiscated firearms and 900 bitcoins, which were worth about US$610,900 at the time.[10] The message from the authorities was clear: 'You are not untouchable using the Tor browser and the darknet.'

The most recent high-profile law enforcement action taken in the darknet, and the largest ever carried out, was Operation Onymous. The operation's most prominent target was Silk Road 2.0, but it was reported to have taken down more than 400 other illicit services based on the Tor network. The operation was conducted by the US FBI, the UK National Crime Agency and 15 other nations' law enforcement agencies. Seventeen arrests were made in sixteen countries, including of the alleged head of Silk Road 2.0, Blake Benthall. The authorities seized US$1 million worth of bitcoin, as well as drugs, guns and large amounts of cash.[11]

LKA
LKA
DHL
EILIGE UND WICHTIGE SENDUNG
345300-1' oder www.dhl.de/express

Bavarian Criminal Investigation Department employee holds a seized envelope and amphetamins (speed) in Munich, Germany, 9 July 2013. Investigators were able to arrest a group which had specialized in trading drugs via darknets © Tobias Hase/dpa/Corbis.

After the initial reports of more than 400 take-downs, the numbers became confused. According to Europol, the European Union's law enforcement agency, 'upwards of 50' sites were disrupted, and the FBI would only publicly confirm the closing of 27 markets.

Whatever the numbers, the operation closed some significant markets, including the following:

- Silk Road 2.0, Pandora, Blue Sky, Hydra and Cloud Nine, all of which were black markets offering a range of illegal goods and services including drugs, stolen credit-card data, counterfeit currency and fake identity documents
- Executive Outcomes, which specialised in firearms (including assault rifles, automatic weapons and sound suppressors) and stated that it used secure drop-ship locations throughout the world so that anonymity was ensured throughout the shipping process and that all serial numbers from the weapons it sold were removed and refilled with metal
- Fake Real Plastic, which offered to sell counterfeit credit cards, encoded with 'stolen credit card data' and 'printed to look just like real VISA and Mastercards'; the cards were guaranteed to have at least $2,500 left on the credit card limit and could be embossed with 'any name you want on the card'
- Fake ID, which offered fake passports from a number of countries, advertised as high quality and having all the security features of original documents, and which advertised its ability to 'affix almost all kind of stamps into the passports'
- Fast Cash! and Super Notes Counter, which offered to sell counterfeit euros and US dollars in exchange for bitcoin.[12]

Within hours of the operation being announced, a Silk Road 3.0 site appeared via the Tor network, showing just how quickly those involved in these cryptomarkets can re-establish themselves after aggressive police action. Their speed and agility pose a serious problem for law enforcement. The scope of the problem shouldn't be underestimated, as some markets that are still trading, such as Agora and Evolution, will soon outsize the Silk Road franchise, and the money to be made means that other competitors are bound to emerge in the near future. The number of people trading in these markets also poses a capacity problem for law enforcement. For example, it was found during the trial of Ross Ulbricht, the owner of the original Silk Road site, that between 6 February 2011 and 23 July 2013 there had been 1,229,465 completed transactions, involving 146,946 buyer accounts and 3,877 vendor accounts.[13]

What can law enforcement do?

For law enforcement agencies, cybercrime is a significant and complex national, human and economic security challenge. Their response must often be multijurisdictional, demanding close collaboration with international and domestic partners. Criminal elements can split and merge, reshape and reprioritise, and move or disperse at will. Government agencies don't have that flexibility and can often be held up by their own structures and agreed-upon areas of responsibility. There's no doubt that the complexity, sophistication and impact of cybercrime are growing, so there's an onus on law enforcement agencies to respond and at least keep pace with the criminals.

The problems that law enforcement agencies face in the darknet are an amplification of problems that they face in the broader cybercrime area. They already struggle with the relative anonymity of the online world, and Tor and the darknet further obscure who the actors are and where they're based.

In many respects, the agencies are playing catch-up in multiple areas, especially in trying to apply laws that aren't nationally or internationally tailored to combating cybercrime. However, there are three key ways that they can increase their capabilities:

- *Invest in technology*. It's vital that agencies' technology is the best available and is kept up to date. Cybercriminals are well funded, can invest in the latest technologies and can quickly bring them into operation, while government agencies struggle to purchase and absorb new technology quickly enough for it to give them an edge. This clearly needs to change. Agencies need to include some technology forecasting in their analytical and strategy work, and they should reach out to the private sector in order to understand the latest technical trends.
- *Build a sustainable skills base*. Advances in technology occur quite independently of users, who can get access to the most advanced software but be completely oblivious to it and the advantages it could bring. Combating cybercrime will become as difficult as the best software engineers can make it, so without an appropriate skills base it will be impossible for law enforcement to be able to respond. Training should be a central part of any agency's strategy, and upskilling its members so that all are 'cybersavvy' is essential. The agencies need to aim to recruit, develop and retain staff with specialist skills and create clear career paths for those staff within their organisations. This should include innovative schemes for international placements and secondments into the private sector in order to understand problems from multiple angles.
- *Build international partnerships*. Most cybercrimes, including those using Tor, the darknet and the illicit markets found there, involve linkages across international boundaries. Therefore, countering them requires increased international cooperation and coordination between the agencies involved. In the case of Operation Onymous, the US Justice Department stated:

  > It is a plain fact that criminals use advanced technology to commit their crimes and conceal evidence—and they hide behind international borders so they can stymie law enforcement … But the global law enforcement community has innovated and collaborated to disrupt these 'dark market' websites, no matter how sophisticated or far-flung they have become.[14]

Asia–Pacific cybercrime cooperation—Australia's international challenge

Because one of the most potent ways to respond to cybercrime is through international cooperation and legislative alignment between nations, there are distinct challenges in the Asia–Pacific region, and subsequently for Australia. The level of cybercrime is likely to continue growing in the region because of three factors: the economic growth of the region as a whole, the growth in internet penetration in the region, and the disparities in legislative approaches and capability and capacity in the region. For example, a recent ASPI report examining cyber maturity in the Asia–Pacific found that Australia, Japan and South Korea all have well-developed legislation and law enforcement capabilities, whereas nations such as Papua New Guinea, Cambodia and Myanmar are still in the early stages of developing their cybercrime legislation and capabilities.[15] This means that as cybercrime continues on an upward trajectory there's an urgent need to help less developed nations reach an adequate level of capability.

Nations in the region will increasingly be targets for criminal activity as criminals follow emerging sources of income and seek out legislative settings that are less likely to lead to their arrest and conviction. There's clear motivation for Asia–Pacific nations to coordinate their efforts to combat cybercrime, but there are difficulties in making that a reality.

From the legal and operational standpoints, signatories to the Council of Europe's Convention on Cybercrime are at an advantage. The convention harmonises legal and operational frameworks, which makes transboundary coordination and convictions much easier.[16] However, there are only three signatories in the Asia–Pacific (Australia, Japan and the US), which makes wider coordination much more difficult. It would be logical for nations in the region to at least align their legislative settings with those in the convention. Many have begun to do so, but others have inadequate laws, ineffective law enforcement or both, and risk becoming safe havens for cybercriminals or sites for infrastructure used for cybercrime.

Two further barriers stand in the way of deeper regional cooperation on cybercrime. First, some nations in the region, most prominently China, are ideologically opposed to the Convention on Cybercrime because they see it as a construct of European nations and European vested interests, and because they weren't involved in its development. Second, the utility of cybercrime as a proxy for pursuing state goals could also limit the scope of any agreement and compliance with it.[17]

This means that Australian law enforcement has to work mainly on a bilateral basis on specific cases, negotiating coordination case by case, which slows down investigations and subsequent prosecutions. Australia has worked hard in this area, with some success (for example, in Indonesia, the Australian Federal Police has helped to establish a Cyber Crime Investigation Centre and several associated cyber units).[18] However, that success isn't being replicated across the rest of the region, so cybercrime investigations remain enormously problematic.

Getting ahead of the game

It's a certainty that malicious darknet activity and cryptomarkets will continue along their current trajectory and increase in size and scope. The benefits for cybercriminals far outweigh the costs, and the increased use of encryption and vetting of those people using darknet services create a blanket of security that law enforcement will have to again break through. What has been proven through recent law enforcement take-downs is that the developers of these sites, the vendors of illicit goods and the technology itself are resilient to law enforcement efforts. Far from being put off by police actions, users are increasingly attracted to the darknet as a result of publicity about those actions.

If law enforcement doesn't innovate and keep up with and occasionally overtake emerging trends, it will lag behind cybercriminals.

Government policymakers would do well to set the policy wheels in motion quickly, in an effort to keep up with or overtake the criminals. It's no good being purely reactive in such a rapidly evolving space.

Notes

[1] The deep web is the collection of all the websites and databases that search engines such as Google don't or can't index. It holds many times the volume of information available on the web as most of us know it.

[2] Angus Crawford, 'Dark net drugs adverts double in less than a year', *BBC News,* 31 July 2014.

[3] 'The Amazons of the dark net', *The Economist*, 1 November 2014.

[4] Andy Greenberg, 'The dark web gets darker with rise of the 'evolution' drug market, *Wired*, 18 September 2014, online.

[5] Andy Greenberg, 'Over 80 percent of dark web visits relate to pedophilia, study finds', *Wired,* 30 December 2014, online.

[6] Lillian Ablon, Martin C Libicki, Andrea A Golay, *Markets for cybercrime tools and stolen data—hackers' bazaar*, RAND Corporation, 2014.

[7] Lev Grossman, Jay Newton-Small, 'The secret web: where drugs, porn and murder live online', *Time*, 11 November 2013.

[8] Jamie Barlett, 'The lighter side of the dark net', *The Telegraph,* 16 September 2014, online.

[9] See www.zerocash-project.org.

10 Leo Kelion, ‘Five arrested in Utopia dark net marketplace crackdown’, *BBC News,* 12 February 2014, online.

11 Tom Fox-Brewster, ‘Silk Road 2.0 targeted in “Operation Onymous” dark-web takedown’, *The Guardian,* 7 November 2014, online.

12 FBI, ‘More than 400 .Onion addresses, including dozens of ‘dark market’ sites, targeted as part of global enforcement action on Tor network’, media release, 7 November 2014, online; Benjamin Weiser, Doreen Carvajal, ‘International raids target sites selling contraband on the “dark web”’, *New York Times,* 7 November 2014, online.

13 Lorenzo Franceschi-Bicchierai, ‘The Silk Road online drug marketplace by the numbers’, *Mashable Australia*, 5 October 2013, online.

14 FBI, ‘More than 400 .Onion addresses, including dozens of “dark market” sites, targeted as part of global enforcement action on Tor network’.

15 Tobias Feakin, Jessica Woodall, Klee Aiken, *Cyber maturity in the Asia–Pacific region 2014*, ASPI International Cyber Policy Centre, ASPI, Canberra, 2014, online.

16 Council of Europe, Convention on Cybercrime, 2001, online.

17 Tobias Feakin, *Enter the cyber dragon: understanding China’s intelligence agencies’ cyber capabilities*, ASPI special report, ASPI, Canberra, June 2013, online; Simon Hansen, *China’s emerging cyberpower: elite discourse and political aspirations*, ASPI special report, ASPI, Canberra, November 2014 online.

18 Jessica Woodall, ‘Engaging Vietnam—a softly, softly approach’, *The Strategist,* 7 October 2014, online.

Acronyms and abbreviations

DDoS	distributed denial of service
EU	European Union
FBI	Federal Bureau of Investigation (US)
ICT	information and communications technology
UN	United Nations

About the authors

Calum Jeffray is a research analyst at the Royal United Services Institute in London, UK.

Tobias Feakin is an ASPI Senior Analyst specialising in national security. He is also the Director of ASPI’s International Cyber Policy Centre.

Important disclaimer

This publication is designed to provide accurate and authoritative information in relation to the subject matter covered. It is provided with the understanding that the publisher is not engaged in rendering any form of professional or other advice or services. No person should rely on the contents of this publication without first obtaining advice from a qualified professional person.

About Special Reports

Generally written by ASPI experts, Special Reports are intended to deepen understanding on critical questions facing key strategic decision-makers and, where appropriate, provide policy recommendations. In some instances, material of a more technical nature may appear in this series, where it adds to the understanding of the issue at hand. Special Reports reflect the personal views of the author(s), and do not in any way express or reflect the views of the Australian Government or represent the formal position of ASPI on any particular issue.

ASPI

Tel +61 2 6270 5100
Fax + 61 2 6273 9566
Email enquiries@aspi.org.au
Web www.aspi.org.au

Facebook.com/ASPI.org

@ASPI_org

RRP $5.00 ISSN 2200-6648