ECONSTOR
Make Your Publications Visible.

A Service of

ZBW Leibniz-Informationszentrum Wirtschaft
Leibniz Information Centre for Economics

Molnar, Adam; Parsons, Christopher; Zouave, Erik

Article

Computer network operations and 'rule-with-law' in Australia

Internet Policy Review

Provided in Cooperation with:
Alexander von Humboldt Institute for Internet and Society (HIIG), Berlin

Suggested Citation: Molnar, Adam; Parsons, Christopher; Zouave, Erik (2017) : Computer network operations and 'rule-with-law' in Australia, Internet Policy Review, ISSN 2197-6775, Alexander von Humboldt Institute for Internet and Society, Berlin, Vol. 6, Iss. 1, pp. 1-15, https://doi.org/10.14763/2017.1.453

This Version is available at:
https://hdl.handle.net/10419/214037

Standard-Nutzungsbedingungen:

Die Dokumente auf EconStor dürfen zu eigenen wissenschaftlichen Zwecken und zum Privatgebrauch gespeichert und kopiert werden.

Sie dürfen die Dokumente nicht für öffentliche oder kommerzielle Zwecke vervielfältigen, öffentlich ausstellen, öffentlich zugänglich machen, vertreiben oder anderweitig nutzen.

Sofern die Verfasser die Dokumente unter Open-Content-Lizenzen (insbesondere CC-Lizenzen) zur Verfügung gestellt haben sollten, gelten abweichend von diesen Nutzungsbedingungen die in der dort genannten Lizenz gewährten Nutzungsrechte.

Terms of use:

Documents in EconStor may be saved and copied for your personal and scholarly purposes.

You are not to copy documents for public or commercial purposes, to exhibit the documents publicly, to make them publicly available on the internet, or to distribute or otherwise use the documents in public.

If the documents have been made available under an Open Content Licence (especially Creative Commons Licences), you may exercise further usage rights as specified in the indicated licence.

https://creativecommons.org/licenses/by/3.0/de/legalcode

WWW.ECONSTOR.EU

Mitglied der Leibniz-Gemeinschaft

INTERNET POLICY REVIEW
Journal on internet regulation

Volume 6 | Issue 1

Computer network operations and 'rule-with-law' in Australia

Adam Molnar
Department of Criminology, Deakin University, Melbourne, Australia, adam.molnar@deakin.edu.au

Christopher Parsons
Citizen Lab, Toronto, Canada, christopher@christopher-parsons.com

Erik Zouave
Centre for IT & IP Law, KU Leuven, Belgium, erik.zouave@kuleuven.be

Published on 14 Mar 2017 | DOI: 10.14763/2017.1.453

Abstract: Computer Network Operations (CNOs) refers to government intrusion and/or interference with networked information communication infrastructures for the purposes of law enforcement and security intelligence. The following article explores how CNOs are lawfully authorised in Australia, and considers the extent to which the current use of CNOs are subject to 'counter-law' developments. More specifically, the article finds that the scope and application of CNOs in Australia are subject to weak legislative controls, that while such operations might be 'lawful', they undermine rule of law and disturb core democratic freedoms.

Keywords: Computer network operations, Intelligence, Policing, Rule of law, Surveillance

Article information

Received: 19 Jun 2016 **Reviewed:** 20 Oct 2016 **Published:** 14 Mar 2017
Licence: Creative Commons Attribution 3.0 Germany
Competing interests: The author has declared that no competing interests exist that have influenced the text.

URL: http://policyreview.info/articles/analysis/computer-network-operations-and-rule-law-australia

Citation: Molnar, A. & Parsons, C. & Zouave, E. (2017). Computer network operations and 'rule-with-law' in Australia. *Internet Policy Review*, *6*(1). DOI: 10.14763/2017.1.453

This paper is part of Australian internet policy, a special issue of Internet Policy Review *guest-edited by Angela Daly and Julian Thomas.*

INTRODUCTION

Australians rely on companies which transit digital communications, provide digital data processing facilities, and retain data for extensive periods of time. Banking, mobile phone use, communications with government and companies, and other routine aspects of everyday life

depend on the internet and its associated services. But these services must comply with, or be subject to lawful requests, orders, and security measures from government agencies. One such set of lawful measures include 'Computer Network Operations' (CNO). A CNO entails the electronic intrusion and/or interference with equipment associated with network infrastructures, such as servers and routers, which are primarily used to transmit communications. While CNOs can also be an element of broader operations which target specific devices with malware, such as personal mobile devices, this article focuses explicitly on the use of CNOs to exploit network infrastructures and the laws authorising such activities by Australian law enforcement and intelligence agencies.

This article argues that statutory measures that authorise CNOs in Australia pose significant challenges to democratic rights and freedoms. The first section provides a definition and background of CNOs in law enforcement and national security operations. Section two sketches a theoretical framework - counter-law - that is used to analyse and critique the adoption and use of CNOs. Section three traces the Australian agencies' adoption of CNOs and the legislation authorising the use of CNO measures by Australian security and law enforcement agencies. Section four discusses and analyses how the authorisation of CNOs in Australia is subject to counter-law developments, and in so doing provides a way to understand how current lawful practices pose challenges to democratic freedoms. The article concludes by noting some risks that CNOs pose to democracy if they are not more meaningfully circumscribed by legal and human rights safeguards.

1. BACKGROUND ON CNOS

'Going Dark' is the popular notion that changes in information technology are obstructing intelligence gathering and criminal investigation. In particular, proponents of the Going Dark position are concerned that the interception of data in transit and at rest, such as emails, VoIP, chat messages, and texts, is increasingly ineffective due to encryption and the dispersed nature of online communications (FBI. 2016; Government of Canada, 2016; Comey, 2014, 2016; Hess 2015; Yates, 2015; United Kingdom Government, 2016). To counteract 'Going Dark', intelligence and investigatory authorities are adopting CNO measures into their operational policies.

CNOs represent a significant shift in how governments exercise power as it transitions from compelled collection by intermediaries, to forcibly acting upon, and collecting from intermediaries and affecting their networks, often without their assistance or knowledge. In the United States, recent changes to powers of criminal procedure under *Rule 41* widen the scope of existing warrant powers to allow federal authorities to conduct CNE across a range of devices and legal jurisdictions, both domestic and international (Wydenet al.,2016). Similarly, the UK Investigatory Powers Act, adopted in late 2016, provides police and security intelligence agencies with powers to surveil and disrupt communications in bulk, which according to the UK Home Office is necessary "in a digital age to disrupt terrorist attacks" (Murdock, 2016).

In this article, we conceptually divide CNOs into three categories of activity: Computer Network Exploitation (CNE), Computer Network Attack (CNA), and Computer Network Disruption (CND). [1] CNE refers to the intrusion, through implantation of foreign code into equipment associated with information infrastructures, as a means to monitor and/or exfiltrate data for intelligence or criminal investigations. CND refers to intrusion and/or interference with equipment associated with network infrastructures to add, modify, delete, or disrupt the integrity of data at rest or in transit. CNA refers to the use of malware to physically degrade or

destroy equipment, physical infrastructure, as well as goods and services that depend on the integrity of that infrastructure.

CNOs might be lawfully authorised under domestic legislation and be subject to a legally prescribed degree of oversight (Hardy& Williams, 2016). Such activities may, however, be deliberately obfuscated from authorising judges (2016 FC 1105) or from the oversight bodies (Security Intelligence Review Committee, 2014). They might also be conducted unlawfully, insofar as either government agencies or other parties may intrude upon intermediaries' networks or systems and affect the data the organisations are transiting without clear legislative or judicial authorisation. It is also possible for CNO-related measures to be *lawful* whilst simultaneously evading the fulsome transparency and accountability that is required for it to be recognised as a democratically legitimised activity, violating laws of foreign states, or infringing upon international human rights.

2. CNO THROUGH "COUNTER-LAW"

Developments in CNOs can be analysed through the frame of 'counter-law'. This concept emerged out of criminologist Richard Ericson's analysis of the relationship between law and socio-technical practices of surveillance and security (Ericson, 2007, 2008). There are two main forms of counter-law. The first, counter-law I, refers to the proliferation of criminal procedure and counter-terrorism statutes that erode or even eliminate constitutional standards of rule of law. Counter-law I provides state agencies with the legal authority to engage in activities with expansive operational discretion. Examples of counter-law I include, but aren't limited to, anti-terrorism legislation characterised by opaque legal definitions and weak thresholds to justify 'pre-crime' state interventions to "punish, disrupt, restrict, or incapacitate, those deemed to embody future threats to security" (McCulloch and Wilson 2015, p. 2; Zedner, 2009). Counter-law I developments are also characterised through weakened thresholds for state security and policing activities, increases in secrecy and use of clandestine powers, and might also occur under the expansion of executive mandates such as the use of ministerial authorisation to secretly authorise national security and criminal justice policies.

The second, counter-law II, refers to the proliferation of surveillance technologies and networks that facilitate new ways to control risks and uncertainties associated with criminality. CNOs for exploitation, disruption, and attack purposes can be defined as a form of counter-law II because they refer to a set of practices enabling new ways for government agencies to monitor and act through connected technologies. Moreover, technological advancements may be compounded by broadened statutory definitions and lawful powers of counter-law I in ways unforeseen by legislators, or facilitated with ambiguous legal terminology. This can occur through a disconnect between 'outdated' legislation of the technical environment, as well as through more recently passed legislation that might contain ambiguous definitions.

The concept of counter-law is focused through Robert Reiner's (2010) analytical dualism of "the black letter of the law" (i.e. law doctrine) and the "blue letter of the law" (operational discretion and activities). Legal permissiveness of "black letter law", particularly through counter-law I, creates a "blue letter law" or "law in action", which refers to actual practices of policing. Bowling and Sheptycki (2015) discuss how the limits of black letter law in cross-border law enforcement operations establishes a space wherein blue letter law exists as a kind of 'post-legal' space. Just one example of a 'post-legal' space involves a case where the US Federal Bureau of Investigation (FBI) previously obtained a warrant to 'hack' computers around the world, after which it shared

collected evidence with foreign law enforcement agencies. This showcases how legal permissiveness - the capability to engage in such CNE activities - combined with the legal permissiveness of data sharing regimes between international police forces can enable activity, such as hacking of foreign devices, which might have normally required heightened judicial approval as part of international warranting practices (Cox, 2016). In this context, law is used 'against law', where legal instruments are used to manipulate, undermine, or nullify the 'spirit' and effects, if not the letter, of other legal instruments (Bowling& Sheptycki, 2015, p. 169). Consequently, global policing as a form of "law in action under transnational conditions" does not exemplify rule of law but instead exemplifies as a form of *rule with law*. Bowling and Sheptycki (2015) conclude that the emergence of a permissive black letter frame unbounds blue letter law, thereby redrawing the boundaries of discretionary authority and proportionality.

3. CNOS AND LAW ENFORCEMENT IN AUSTRALIA

Australia's 2016 Cyber Security Strategy announced AU$230 million to be spent over four years to improve the security of public and private information communications infrastructure (Coyne, 2016). The funds will develop the Australian Cyber Security Centre (ACSC), which co-locates intelligence analysts and operation agents from the Australian Signals Directorate (ASD), Defence, Australian Security Intelligence Organisation (ASIO), the Australian Federal Police (AFP), the Australian Criminal Intelligence Commission, as well as establishing a host of joint public-private partnerships for the sharing of threat intelligence (Commonwealth of Australia, 2016). The ACSC is reminiscent of wider trends in security governance toward a blurring of boundaries between military, intelligence, security, and law enforcement agencies and functions (Bowling & Ross, 2006). In both lawful authority and practice, the Australian Signals Directorate (ASD) possesses offensive CNO capabilities and, in some situations, may provide assistance to other domestic government agencies (Intelligence Services Act 2001, s.13 and s.13(a)).

A series of unauthorised public disclosures and court documents from the US suggest that federal and state agencies in Australia use, with others interested in using, such technological measures. In 2014, the Queensland Police Services' (QPS) 'Task Force Argos' took over a child pornography website for several months to unmask the IP addresses of visitors to the website (Cox, 2016). While it is unclear if the server was located in Australia or whether the activity was judicially approved, the operation did result in at least 30 IP addresses being disclosed to US authorities (Cox, 2016). WikiLeaks revealed in 2014 that the New South Wales (NSW) Police acquired several licenses for Gamma Group International's FinFisher spyware platform. The Australian Federal Police (AFP) initially refused to provide responsive documents to a FOI concerning AFP contracts with Gamma Group International but were ultimately revealed as clients of Hacking Team's CNO systems since 2011(Sveen& Ockenden, 2015). Northern Territory Police (NT), NSW Police, ASIO, and Victoria's Independent Broad-based Anti-Corruption Commission (IBAC) also consulted Hacking Team to learn about their CNO products (Sveen& Ockenden, 2015). These events showcase significant domestic interest in adopting CNO technology for law enforcement and national security operations. As discussed in the following section we will see that some Australian legal frameworks have already existed, where others have been recently amended to further expand the use of CNO measures that lawfully target telecommunications and internet intermediary points.

AUTHORISING LAW ENFORCEMENT USE OF CNOS

Several pieces of state and federal legislation authorise Australian government agencies' use of CNOs for security and law enforcement purposes. Given space constraints, we briefly discuss Commonwealth (federal) policy and legislation premised on relevant agencies and functions.

TELECOMMUNICATIONS INTERCEPTION (AND ACCESS) ACT 1979, CNOS, AND COUNTER-LAW

The Telecommunications (Interception and Access) Act 1979 (the TIA) is the primary legal framework for security intelligence and police access to communications that transit telecommunications infrastructure in Australia. It has been incrementally amended since its inception (Bronitt & Stellios, 2005, 2006). Originally, the TIA existed as an instrument for the investigation of serious drug offences through "real-time" interception of communications (voice, data, text, images, and signals) "passing over a telecommunications system" (s.5F) but has subsequently been amended to apply more broadly, including access to stored communications for any criminal offence without judicial authorisation, and can also be used to authorise CNE.

Specifically, the TIA legalises exfiltration of intelligence from systems pursuant to Part 2.2 and 2.5 warrants. Part 2.2 warrants are issued to the Australian Security Intelligence Organisation (ASIO) under executive ministerial authorisation by the federal Attorney-General for both domestic (s.9, s.9a) and foreign intelligence (s.11a-c). Part 2.5 warrants are issued to federal and state law enforcement agencies by judges and members of the Administrative Appeals Tribunal (AAT) pursuant to investigating federal and state level offences (s.39). Each type of warrants may be issued with respect to either a 'telecommunications service' or 'a person' (s.39(1); see also Bronitt & Stellios, 2006, p. 415).

Exfiltration under the TIA is not based on reasonable suspicion that an individual has, or will, commit a serious offence, but:

1. upon "reasonable grounds for suspecting that a particular person is using, or is likely to use" (s.46 c) a telecommunications service; or
2. if information collected under the interception "would be likely to assist in connection with the investigation" (s.46 d) in which the particular person is "involved" (s.46 dIi).

The loose categorical definition of *involvement* sidesteps a reasonable suspicion threshold to sweep up a more loosely defined category of 'person(s) of interest' (Bronnit & Stellios, 2006, p. 416). Notably, Australian law enforcement and security agencies can use warrants issued for "telecommunications service" (s.46) to authorise CNE to target intermediary points in a telecommunications network. When targeting end-point devices such as laptops or mobile phones, authorities can use s.6(q) of the TIA to gain authorisation for collecting communications made by means of a 'telecommunications device' used by a person of interest.

The TIA was amended in 2006 to make Part 2.2 and Part 2.5 warrants available for intruding upon the private lives of persons of interest as well as persons who are uninvolved in any specific criminal activity (Stellios & Bronnitt, 2006, p. 417). Authorities can use "B-Party" warrants to exfiltrate communications from someone who uses a telecommunications service to communicate with a person of interest (Bronitt & Stellios, 2006 p. 417). As long as there is a connection between the security or law enforcement objective and the use of the B-party's telecommunications service, a B-Party warrant may be issued. B-Party warrants may be sought at the mere likelihood that monitoring the communication of the B-Party or "a telecommunications service", if it is also used by a person that is "reasonably suspected of being

engaged in… activities prejudicial to security" (TIA s.9). The black-letter of the TIA places no explicit limitations on the identity of the party who might use the telecommunication service, on the content of the intercepted communication, or on the identity of innocent third parties to the intercepted communication (Bronnitt and Stellios, 2006, p. 417). In principle, the black-letter of CNEs authorised through B-Party warrants could apply, in the blue-letter operational space, to a broad category of persons, including judges, politicians, lawyers, journalists, medical professionals, and civil rights defenders.

Furthermore, the black-letter of the B-Party warrant authority means that significant segments of a "telecommunications service" could be intercepted to target even a single subject. Even if, the B-Party amendment was initially intended to authorise collection on another 'single' party on a one-to-one wireline conversation, as counter-law II developments in information infrastructures evolve, the black-letter of the TIA might now authorise the collection of bulk traffic in and out of a mobile tower.

THE SURVEILLANCE DEVICES ACT 2004, CNOS, AND COUNTER-LAW

The Surveillance Devices Act (Cth) 2004 (SDA) also authorises the use of CNE-related CNO activities. The Australian Federal Police, the Australian Crime Commission (ACC), the police force of each State or Territory, the New South Wales Crime Commission, amongst others, (SDA s6(1)) are authorised to conduct CNE when investigating serious offences.

A range of warranting powers were included in the SDA. One of them, for a "data surveillance device" (s.6(1)), can be used to compromise mobile phones, laptops, or other digital devices operated by Australian citizens. A data surveillance device is defined in the Act as "a device or program used to record or monitor the input into or out of a computer" (S.6(1)). By extension, a "computer", is defined under the Act as "any electronic device for storing or processing information" (s. 6 SD Act).

In practice, the aforementioned black-letter definitions could include the use of *any* type of technical device or programme in blue-letter CNE activities to gain access to data inside, or flowing into or out of, any electronic, smart or connective technology, such as computers, iPads, tablets, smartphones, GPS systems, and vehicular control systems. The black-letter ambiguity in the SDA regarding data surveillance device warrants might also authorise targeting upstream of the end-point device, such as a router or other networks many devices use, to the effect of a single warrant affecting thousands of devices and users. While clearly being *one device* or possibly *one system*, a router for instance relays information regarding *multiple devices* relying on that router.

In addition to the ambiguity of "device" in black-letter terms, the SDA consistently uses terminology suggesting warrants will be used to target specific computing devices – a "computer", a "device", an "instrument", an "apparatus" – and thus implies a degree of targeted specificity in the warrant scheme. S.18 of the SDA expands this definition to include multiple devices. Per Section 18(3)(b) and(f), surveillance devices and "enhancement equipment in relation to the surveillance device" can be connected to any "system" to perform the operation. Furthermore, s.19(5) authorises interference with third parties' property that is not the subject of the investigation. In effect, this means that, similar to counter-law I developments concerning B-Party warrants in the TIA, third parties can be affected by CNEs by authorities for domestic investigative purposes.

THE ASIO ACT, CNOS, AND COUNTER-LAW

CNO measures are authorised by Section 25(a) of the Australian Security Intelligence Organisation Act 1979 (ASIO Act). The statute empowers the Attorney-General to issue a "computer access warrant" following a request from the Director-General of ASIO. Such warrants authorises ASIO to intrude on "a target computer", a "telecommunications facility operated by a Commonwealth or a carrier", or "any other electronic storage equipment" or a "data storage device" (ASIO Act, s.25(a)). These warrants are granted when the Attorney-General is satisfied that there are reasonable grounds for believing that access to data held in a computer would "substantially assist the collection of intelligence" in relation to a "security matter" (ASIO Act, s.25(a)).

ASIO's CNO-related powers were expanded in late 2014 under the ASIO Act. The definition of a "computer" was broadened to include "one or more computers", "one or more computer systems", "one or more computer networks", or "any combination of the above" (ASIO Act, s.4). The warrants also let ASIO use "any other computer or communication in transit to add, copy, delete or alter data…for the purpose of obtaining access to data relevant to the security matter and held on the target computer" (National Security Legislation Amendment Bill (No.1) 2014), Explanatory Memorandum). As a result, a single computer access warrant can allow CNE-facilitated surveillance of entire businesses, university networks, telecommunications companies, or core internet infrastructure for gathering intelligence or disrupting activities (Hardy, 2015). The only explicit limitation on ASIO's use of CNO measures is if the operation would "cause any other material loss or damage to other persons lawfully using a computer" (s.25A(5)(b)). What constitutes "material loss" is not defined or set out in the Act or Explanatory Memorandum that accompanied the amendment.

THE AUSTRALIAN SIGNALS DIRECTORATE AND DOMESTIC ASSISTANCE IN CNOS

The ASD has a mandate to assist domestic agencies to carry out their functions under the Intelligence Services Act 2001 (ISA) (s.13 and s.13(a)). [2] In particular, they can provide practical assistance when domestic agencies are addressing activities that are, or "are likely to be", a threat to security (ISA 2001, s.9;s.13,s.13a) with ministerial authorisation. This assistance draws on the ASD's "cryptography", "communication" and "computer technologies" capabilities (s.7). Under existing law and practice it is unclear how often ASD provides technical assistance. In a similar jurisdiction, such as Canada, approximately 300 requests were made for domestic assistance in a four-year period between 2009 and 2012 (Freeze, 2014).

CNOs are also subject to a limited degree of oversight and accountability mechanisms even though they can be deeply intrusive investigative and intelligence tools. Such mechanisms tend to be structurally deficient, however, because many of the agencies responsible for oversight and review are restricted to performing a legal compliance function. And as we note in the following section, in an era where CNOs are characterised by counter-law developments it can be challenging for intelligence and policing agencies to exceed such extraordinarily broad black-letter statutes when it comes to *actual* blue-letter practice.

DEMOCRATIC SAFEGUARDS, SECRECY, AND COUNTER-LAW

Many CNO measures in Australia are performed with executive oversight. Such oversight is meant to ensure compliance with the law as well as to propose non-binding recommendations to influence government policy and strategy on counter-terrorism matters. [3] Furthermore, legislation that enhances the Australian secrecy regime and establishes anti-whistleblower laws have exacerbated constraints on public disclosure and debate surrounding government usage of

CNOs. While a full review of the Australian oversight, accountability, secrecy and whistleblower regimes are beyond the scope of this article (however, see Hardy & Williams, 2016, 2014) there are several weaknesses in these regimes linked with CNOs and counter-law.

First, while the Parliamentary Joint Committee on Intelligence and Security (PJCIS) can review the ASIO's administration and expenditure, it lacks a mandate to review intelligence-gathering matters or operations (Lynch et al., 2014, p. 156). ASIO can also redact information in committee reports provided to the PJCIS (Lynch et al., 2014, p.156). Secondly the Office of the Inspector-General of Intelligence and Security (IGIS) serves as an independent executive oversight body for the intelligence community. The IGIS' is mandated to ensure legal compliance of security intelligence activities, such as guaranteeing that all ministerial guidelines and directives are appropriately followed (Inspector-General of Intelligence and Security Act 1986 (Cth). It relies on classified submissions from security intelligence and law enforcement agencies to assess adherence with laws, directions, and guidelines, and 'group-specific' human rights codes (e.g., *Age Discrimination Act 2004*, *Disability Discrimination Act 1992*, *Racial Discrimination Act 1975*, or the Sex Discrimination Act 1984). However, whereas proportionality tests might normally include balancing against a formal Bill of Rights, Australia lacks this aspect of basic law (barring that which exists in the State of Victoria and ACT). As a result, balancing is generally less robust in Australia than in other jurisdictions such as Canada and Europe. Moreover, even the Victoria bill of rights contains black-letter exceptions. S.21(3) seemingly grants an exception regarding impacts upon innocent third parties during the lawful use of CNOs, so long as the operation is "in accordance with procedures, established by law" (s.21(3)). Broadly, the lack of a federal bill of rights in tandem with exemptions mean that a commonplace method of evaluating the proportionality of CNO measures is lacking.

And lastly, the *Privacy Act 1988* places few limits on the sharing, retention, integrity, and accuracy of personal information acquired through CNOs amongst Australian security intelligence and law enforcement organisations (Molnar& Parsons, 2016; Privacy Act 1988). ASIO and the ASD are exempt from the Act in its entirely (Privacy Act 1988, s.7). And while law enforcement agencies are broadly covered by the Act they enjoy considerable exemption under the Act. Generally speaking, disclosing personal information is permitted for law enforcement if it is "reasonably necessary for the enforcement of the criminal law, or of a law imposing a pecuniary penalty, or for the protection of the public revenue (ALRC, 2008, s.37).

These privacy concerns are exacerbated by the *security* risks linked to CNO measures. Where malware code is used to target an individual, and designed to affect the type of device or application they are using, then the code is simultaneously capable of running against the same devices and applications of non-targeted persons. By concealing the weaknesses of the device or exploit code used to perform the CNO, not only is the security of a specific target compromised, but so is the security of *all other persons* who happen to use the same device or rely on the same codes. Exploits are reproducible, and so the failure to disclose vulnerabilities can mean that other parties (e.g., nation-state actors, cyber mercenary firms, independent hackers, or academics) can also identify and exploit the same vulnerabilities. Furthermore, in failing to notify companies of weaknesses in their defenses or flaws in their software code those companies can suddenly fall victim to the state's exploit code when it is accidentally released to the public. In the US for example, the intelligence development of vulnerabilities is subject to independent review by committee through the so-called vulnerabilities equities program (Daniel, 2014). The black-letter of Australian legislation and policy, as well as the oversight system, fails to account for how the blue-letter operations introduce systemic threats to individual and collective privacy and security.

The relative weakness of the structure of oversight, accountability, official oversight and review functions is worsened by counter-law I legislation that cloaks most CNO measures in secrecy. When CNOs are pursued through ASIO Act computer access warrants, they can be designated as a "special intelligence operation" (SIO) by the Attorney-General (ASIO Act, s.35(b), a measure that provides civil and criminal immunity for ASIO officers and affiliates involved in the operation (Hardy & Williams, 2016, ASIO Act, s.35(k)) and that also imposes a five year penalty for "disclosing information" related to the operation. This term can be extended to ten years if the disclosure "will endanger the health or safety of any person or prejudice the effective conduct of a special intelligence operation" (ASIO Act 35(p)). There are no exceptions for journalists or whistleblowers, and the statute has been understood by the Attorney-General to apply "generally to all citizens" (Williams, 2014). While SIOs represent the most harsh secrecy provisions in Australia, two others are worth mentioning. Section 70 of the Crimes Act would make any disclosure of a CNO (including those not designated as a SIO) by any current or former Commonwealth officer punishable by imprisonment of up to two years for sharing if the disclosure "would be prejudicial to the effective working of government" (Hardy and Williams 2014, p. 802; Crimes Act 1914, s.70). Another secrecy offence in the Crimes Act, Section 79, is also generally applicable to both citizens and non-citizens and carries an increased maximum penalty of seven years' imprisonment. Unlike s.70 and 35P, the disclosure, however, must be accompanied with an intention to cause harm (Hardy & Williams, 2014, p. 803-807; Crimes Act 1914, s.79). Aggressive secrecy provisions surrounding information that may pertain to an ongoing SIO could also undermine any responsible vulnerability reporting process that help to maintain the security and integrity of internet communication infrastructures as a broader public good.

4. DISCUSSION

Counter-law is exemplified by CNOs through the collision of technological advancements and legal powers. This occurs in two main ways. First, outdated definitions of technology in legislation are surpassed by an interconnected technological environment that works to decouple the use of CNOs from clearly defined boundaries. The disconnect between ambiguous black-letter definitions in primary legislation from technological environments results in the relatively unrestrained application of CNOs. While the use of CNOs can remain 'lawful' in a narrow sense, their application in blue-letter space, including the range of privacy, civil liberties, and security risks they introduce, are disproportionately broad.

Second, even more recent counter-law I developments have involved a purposeful counter-law trend black-letter 'catch-all' terminology. For instance, the 2014 amendment of the black-letter definition of "a computer" under the ASIO Act as "a network" or "any combination" of computers *and* networks presents an unrestrained limit to perform CNOs in the current technological environment. Furthermore, more recent counter-law I developments allow CNOs in domestic contexts to reach remotely beyond mere interception of information that is transiting networks and to actually annul and/or modify information and processes existing on systems, sometimes even potentially to include physical effects on the infrastructure. The introduction of disruption measures places strain on rule of law principles of procedural fairness and due process rights.

Moreover, the mechanisms that democratically elected representatives created - namely oversight and review bodies - in combination with judicial authorities are not necessarily able to assure the public that basic democratic freedoms are not inappropriately trodden upon. Laws, as

they are currently written, provide authority to identify and evaluate instances where security and policing agencies act illegally; this means, however, that oversight and review bodies are similarly ensnared in counter-law developments because they may be deeply challenged to find illegal what is overtly made legal by these agencies' lawful authority (as example, see Robinson, 2015). While the general trend of counter-law developments and CNOs are likely to be felt across many liberal democratic jurisdictions, Australia is in a novel position in comparison to its Five Eyes partners. Unlike Canada, the United States, New Zealand, and the United Kingdom, Australia does not have a formal bill of rights or a regional judicial body to adjudicate on human rights. Given that government agencies possess lawful authority to conduct unbounded CNO operations and can seek relatively unbounded warrants instead of those with strongly circumscribed limits, the rule of law has become distorted and replaced with *rule with law* (Bowling & Sheptyicki, 2015). The combined force of the technical environment outpacing laws on the books, along with new laws which are passed to provide wide legal remit for blue-letter CNO operations, have considerably threatened the rule of law itself. As a result, the 'lawful' use of CNOs in Australia can disturb the preservation of democratic freedoms and procedural justice.

5. CONCLUSION

While this article focused on the reach and implications of CNOs in Australia, our discussion carries broader implications concerning debates surrounding meaningful regulation CNOs in national security and policing operations. Future work might consider the extent to which a space of 'post-legal' exceptionality is emerging for the use of CNOs via counter-law developments. In pursuing this line of analysis it would be useful to juxtapose the Australian case with others, where similar counter-law manifestations are taking place but which possess a formal bill of rights. Specifically, is it the case that such a bill would effectively moderate counter-law infringements on civil liberties as they pertain to CNOs? Though the state 'drives' CNO operations they are resisted by private companies and NGOs that attempt to make such operations more transparent, more clearly accountable to lawmakers or the public, and more demonstrably targeted. Additional lines of research might also investigate the effectiveness, and tactics used, to reinforce the rule of law. Are such efforts broadly successful, or are they dependent on specific popular media or other kinds of social capital?

A number of ethical questions concerning procedural fairness and due process also emerge. For instance, while forensics standards exist for analysing computers there are no equivalent standards for using malware that transmits evidence across the internet. The result is that there is a very low standard required to use the tools without an equivalent balancing to ensure that their operation does not render collected information inadmissible in court as a result of mistakes in how exploit code is crafted, deployed, or potentially tampered with by a third-party while in transit. Furthermore, the use of CNOs might be in excess of the threat posed, or also run contrary to the intended effect. Mistakes in how exploit code is crafted or deployed can have unexpected consequences when deployed in production environments and disruptions could inhibit the communications of targets and non-targets alike.

CNOs represent a significant transformation of state authority to intrude and affect digital information. Such measures often occur under a veil of exceptional secrecy and jeopardise the universal security of information communication systems. Thus, in addition to such activities raising questions about the appropriate degree of power invested in state authorities, the proliferation of CNOs by governments around the world for domestic investigations that have

global reach (Cox, 2016), for intelligence operations targeting individuals and millions of persons alike (Gallagher, 2014; Schneier, 2013), and for damaging critical infrastructure and computer records (Zetter, 2014; Zetter, 2016; Greenwald & Fishman, 2015), it should also raise vital questions about the appropriateness, democratic interest, and accountability of state operations that expose populations to the pervasive insecurity through exploitable weaknesses that can further potential abuse against innocent third parties.

REFERENCES

Commonwealth of Australia, Department of the Prime Minister and Cabinet. (2016). *Australia's cybersecurity strategy: Enabling innovation, growth, & prosperity*. Retrieved from https://cybersecuritystrategy.dpmc.gov.au/assets/img/PMC-Cyber-Strategy.pdf

Australian Government Attorney-General's Department. (2015). *Surveillance Devices Act 2004 Annual Report 2014-2015*. Retrieved from https://www.ag.gov.au/NationalSecurity/TelecommunicationsSurveillance/Documents/Surveillance-Devices-Act-2004-Annual-Report-2014-15.pdf

Australian Security Intelligence Organisation Act 1979 (Cth). Retrieved from http://www.austlii.edu.au/au/legis/cth/consol_act/asioa1979472/

Australian Law Review Commission (ALRC). (2008). *For Your Information: Australian Privacy Law and Practice* (ALRC Report 108). Retrieved from http://www.oaic.gov.au/privacy/privacy-resources/privacy-fact-sheets/other/privacy-fact-sheet-17-australian-privacy-principles

Bowling, B., & Ross, J. (2006). The Serious and Organised Crime Agency: Should we be afraid? *Criminal Law Review, December*, 1019-1034.

Bowling, B., & Sheptycki, J. (2015). Global policing and transnational rule with law. *Transnational Legal Theory*, *6*(1), 141-173. doi:10.1080/20414005.2015.1042235 Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2560226

Bronitt, S., & Stellios, J. (2005). Telecommunications interception in Australia: Recent trends and regulatory prospects. *Telecommunications Policy*, *29*(11), 875-888. doi:10.1016/j.telpol.2005.06.010 Retrieved from https://www.academia.edu/2435183/Telecommunications_interception_in_Australia_Recent_trends_and_regulatory_prospects

Bronitt, S., & Stellios, J. (2006). Regulating telecommunications interception and access in the twenty-first century: Technological evolution or legal revolution? *Prometheus*, *24*(4), 413-428. doi:10.1080/08109020601030001

Coleman, G. (2014). *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous*. London: Verso.

Comey, J.B. (2014). *Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?*. Federal Bureau of Investigation Speeches. Retrieved from https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course

Comey, J.B. (2016). Encryption Tightrope: Balancing Americans' Security and Privacy. Federal Bureau of Investigation. Retrieved from https://www.fbi.gov/news/testimony/encryption-tightrope-balancing-americans-security-and-privacy

Crimes Act 1914 (Cth). (1914). Retrieved from http://www.austlii.edu.au/au/legis/cth/consol_act/ca191482/index.html#s70

Daniel, M. (2014, April 28). Heartbleed: Understanding when we disclose Cyber vulnerabilities.

Retrieved from https://www.whitehouse.gov/blog/2014/04/28/heartbleed-understanding-when-we-disclose-cyber-vulnerabilities

Ericson, R.V. 2007. "Security, surveillance and counter-law." *Criminal Justice Matters*, *68*(1): 6-7. doi:10.1080/09627250708553271

Ericson, R.V. 2008. *Crime in an Insecure World*. Cambridge: Polity.

Gallagher, R. (2014, December 13). The inside story of how British spies hacked Belgium's largest Telco. *The Intercept*. Retrieved from https://theintercept.com/2014/12/13/belgacom-hack-gchq-inside-story/

Hardy, K. (2014, September 16). Sweeping security law would have computer users surrender privacy. *The Conversation*. Retrieved from https://theconversation.com/sweeping-security-law-would-have-computer-users-surrender-privacy-30041

Williams, G., & Hardy, K. (2014). Terrorist, Traitor, or Whistleblower? Offences and Protections in Australia for Disclosing National Security Information. *University of New South Wales Law Journal, 37*(2), 784-819.

Hess, A. (2015). Encryption and Cyber Security for Mobile Electronic Communication Devices. Federal Bureau of Investigation Testimony. Retrieved from https://www.fbi.gov/news/testimony/encryption-and-cyber-security-for-mobile-electronic-communication-devices

Intelligence Services Act 2001 (2001). Retrieved from http://www.austlii.edu.au/au/legis/cth/consol_act/isa2001216/index.html#s7

Lynch, A., McGarrity, N. & Williams, G. (2014). *Inside Australia's Anti-Terrorism Laws and Trials*. Sydney: NewSouth Publishing, University of New South Wales Press.

Marczak et al (2015). China's Great Cannon. *Citizen Lab*. Retrieved from https://citizenlab.org/2015/04/chinas-great-cannon/

McCulloch, J. and Wilson, D. (2015). *Pre-crime: Pre-emption, precaution and the future*. Abingdon: Routledge.

Molnar, A., & Parsons, C. (2016). Unmanned Aerial Vehicles (UAVs) and Law Enforcement in Australia and Canada: governance through 'privacy' in an era of counter-law? In R. Lippert, K. Walby, I. Warren & D. Palmer (Eds.), *Security, Surveillance and Law in Comparative Context* (pp. 225 - 247). Cham: Springer International Publishing. doi:10.1007/978-3-319-43243-4_10

Murdock, Jason. (2016 November 29). UK green-lights mass spying, hacking and bulk collection of your internet records. *International Business Times*. Retrieved from http://www.ibtimes.co.uk/uk-green-lights-mass-spying-hacking-bulk-collection-your-internet-records-1594046

National Security Legislation Amendment Bill No.1, 2014. (2014). Retrieved from http://www.austlii.edu.au/au/legis/cth/bill_em/nslab12014440/memo_0.html

Parsons, C. (2015). Beyond Privacy: Articulating the Broader Harms of Pervasive Mass Surveillance. *Media and Communication*, *3*(3) doi:10.17645/mac.v3i3.263

Privacy Act 1988. (1988). Retrieved June 18 2016 from https://www.oaic.gov.au/resources/individuals/privacy-fact-sheets/general/privacy-fact-sheet-17-australian-privacy-principles.pdf

Reiner, R. (2010). *The Politics of the Police (4th Edition)*. Oxford: Oxford University Press.

Surveillance Devices Act 2004 (Cth). Retrieved fromhttp://www.austlii.edu.au/au/legis/cth/consol_act/sda2004210/

Sveen, B., & Ockenden, W. (2015, July 10). Hacking team: Australian Government agencies negotiating with notorious surveillance company, leaked emails show. *Australian Broadcasting Corporation*. Retrieved from http://www.abc.net.au/news/2015-07-10/leaked-emails-expose-australian-government-agencies-hacking-team/6609276

Telecommunications (Interception and Access) Act 1979. Retrieved from http://www.austlii.edu.au/au/legis/cth/consol_act/taaa1979410/

United Kingdom Government. (2016). Investigatory Powers Bill: Targeted Equipment Interference Fact Sheet. Retrieved 18 June 2016 from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/505516/Targeted_Equipment_Interference_factsheet.pdf

Williams, G. (2014). The Legal Assault on Australian Democracy. *QUT Law Review*, *16*(2), 19-41.

Wyden, Blaze, and Landau. (2016, September 14). The feds will soon be able to legally hack almost anyone. *Wired*. Retrieved from https://www.wired.com/2016/09/government-will-soon-able-legally-hack-anyone/

Yates, S.Q, (2015, May 4). Acting Deputy Attorney General Sally Q. Yates Delivers Remarks at the Association of State Criminal Investigative Agencies Spring Conference. Retrieved 18 June 2016, from https://www.justice.gov/opa/speech/acting-deputy-attorney-general-sally-q-yates-delivers-remarks-association-state-criminal

Zedner, L. (2009). *Security (Key Ideas in Criminology)*, 1st edition. London: Routledge.

FOOTNOTES

1. Intelligence agencies such as the Communications Security Establishment, Canada's foreign signal intelligence agency, categorise these three types of activities under a common heading. We have opted to do the same, though with a broader conceptualisation of 'operations', as those agencies. See: "CSEC Cyber Threat Capabilities - SIGINT and ITS: an end-to-end approach", https://www.christopher-parsons.com/Main/wp-content/uploads/2015/03/doc-6-cyber-threat-capabilities-2.pdf?x98114, page 22.

2. The ISA does not provide explicit constraints upon the ASD's efforts to perform CNOs (ISA, s.12) to "obtain intelligence for the purposes of national security, foreign relations, or national economic well-being" (ISA, s.11). That is to say, CNO measures (including CNE, CND, and CNAs) for all practical purposes, are unregulated when directed at persons or activities outside of Australia (ISA, 2001, s.7).

3. For a thorough review of the Australian oversight and accountability regime, see Hardy and

Williams (2016).