Australian Government
Australian Institute of Criminology

AIC reports
Research Report 03

Criminal misuse of the Domain Name System

Tony Krone and Russell G Smith

ISSN (Online) 2206-7280

Published by the Australian Institute of Criminology
GPO Box 1936 Canberra ACT 2601
Tel: (02) 6268 7166
Email: front.desk@aic.gov.au
Website: aic.gov.au

Please note: Minor revisions are occasionally made to publications after release. The online versions available on the AIC website will always include any revisions.

All publications in the Research Report series are subject to peer review–either through a double-blind peer review process, or through stakeholder peer review. This report was subject to double-blind peer review.

Disclaimer: This Research Report does not necessarily reflect the policy position of the Australian Government.

General editor: Dr Rick Brown, Deputy Director, Australian Institute of Criminology

Edited and typeset by the Australian Institute of Criminology

A full list of publications in the AIC Reports series can be found on the Australian Institute of Criminology website at **aic.gov.au**

Contents

Boxes

Figures

Tables

Acknowledgements

This research was funded by the auDA Foundation Pty Ltd. Dr Alice Hutchings, former Senior Research Analyst at the AIC, helped develop the study in 2013. The views expressed in the paper are those of the authors and may not reflect the position of the auDA Foundation or the Australian Government.

Foreword

This report presents the findings of a preliminary inquiry into the nature of and the risks arising from misuse of the Domain Name System (DNS), and how criminological and regulatory approaches can assist in minimising risks of such misuse. Criminal misuse of the DNS has received relatively little academic attention, falling as it does between the disciplines of law, information technology, regulation, criminology and public policy. Solving the problem requires an understanding of how users and infrastructure and service providers use and contribute to the internet, and an appreciation of the complex legal and regulatory framework that governs the DNS. A deterrence-based approach based on criminal prosecution and punishment is unlikely to be effective against a cross-border problem that affects both the public and private sectors.

Internet governance reached an important milestone in 2016 when the United States devolved the functions of the Internet Assigned Numbers Authority (IANA) to the Internet Corporation for Assigned Names and Numbers (ICANN). This report on the misuse of the DNS and cybercrime is a timely contribution to the debate around internet regulation – it is certain that Internet governance will be intensely scrutinised in the years ahead.

I commend the authors for their research and the auDA Foundation for its initiative in funding the study.

Michael Phelan APM
Director, Australian Institute of Criminology

Acronyms

AIC	Australian Institute of Criminology
APWG	Anti-Phishing Working Group
ARPANET	Advanced Research Projects Agency Network
ASO	Address Supporting Organisation
auDA	.au Domain Administration
BBC	British Broadcasting Corporation
BGP	Border Gateway Protocol
CCNSO	Country Code Name Supporting Organisation
CCTLD	Country Code Top Level Domain
DDoS	Dedicated Denial of Service
DNS	Domain name system
DNSSEC	Domain name system security extension
DoS	Denial of Service
EU	European Union
EUROPOL	European Police Agency
FNC	Federal Networking Council
GAO	Government Accounting Office (US)
GNSO	Generic Names Supporting Organization
gTLD	Generic Top Level Domain
HCI	Human-Computer Interaction
HTTP	HyperText Transfer Protocol
IAB	Internet Architecture Board
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
IDN	Internationalised Domain Name
IETF	Internet Engineering Taskforce
IGF	Internet Governance Forum
IIFS	Internet Infrastructure Foundation of Sweden
IOC	International Olympic Committee
IOS, MA	International Organization for Standardization, Maintenance Agency
IP	Internet Protocol
IRTF	Internet Research Task Force

ISOC	Internet Society
ISP	Internet Service provider
ITU	International Telecommunications Union
IXP	Internet Exchange Point
NDN	Named Data Networking
NWG	Network Working Group
OFAC	Office of Foreign Assets Control
OSI	Open Systems Interconnect
RIR	Regional Internet Registry
RPKI	Resource Public Key Infrastructure
SLP	Statement of Licensing Policy
SCIC	Standing Committee on Infrastructure & Communications
TCAM	Tertiary Content Addressable Memory
TCP	Transmission Control Protocol
TLD	Top Level Domain
TLS	Transfer Layer Security
TOR	The Onion Router
TSIG	Transaction Signature
UDRP	Uniform Dispute Resolution Policy
UNESCO	United Nations Educational, Scientific and Cultural Organization
UNODC	United Nations Office on Drugs and Crime
VPN	Virtual Private Network
W3C	World Wide Web Consortium

Executive summary

The DNS is a naming system for resources, such as personal computers or other devices, that connect to the internet via the World Wide Web. It coordinates internet addresses and domain names—the two kinds of unique identifiers that make internet connection possible.

The study was funded by the auDA Foundation, which was established by the .au Domain Administration (auDA), the policy authority and industry self-regulatory body for the .au domain space in Australia. The aim was to support the objective of the Foundation by 'promoting and encouraging educational and research activities that will enhance the utility of the Internet for the benefit of the Australian community' (auDA Foundation 2015).

Methodology

Public source, non-technical literature was comprehensively reviewed to identify instances of DNS misuse, the risks that led to the commission of these instances, and the crime prevention and regulatory measures available to address the problem. The study was particularly focused on exploring existing legal and criminological frameworks that could be used to conceptualise the problem of DNS misuse and provide a framework for developing effective control strategies.

The literature review was international and examined English-language resources including academic sources, legal databases and relevant policy documents. The review primarily focused on the risks of misuse of the DNS from an Australian perspective although, due to the global nature of the internet, all legitimate users would benefit in many ways from a more secure and trusted domain name system, both as domain name owners and consumers.

Scope

The results address current identified risks, but they could also inform further and more detailed cross-disciplinary research into the nature of the problem and appropriate solutions. The research was not intended to be an overly technical examination of the problem and does not address the architectural or programming features of particular examples of misuse. Rather, it explores the issue from a policy perspective that will be beneficial in devising appropriate legal and policy responses.

The research looks at the connections that exist between various forms of misuse and DNS governance. The discussion explores the internet as a network of networks based on an addressing system known as the Internet Protocol (IPv4 and IPv6), which creates IP addresses for resources within the DNS and is focused on what might be called the 'open web' or the World Wide Web (the public internet) most users commonly access when using the DNS.

Resources which are accessed via the public internet, but located behind a barrier such as a paywall or an account login for hosted services, are included in the research. These hosted resources are from the DNS core and so are not directly subject to DNS regulation, but rather are immediately subject to any regulation the host imposes or any conditions imposed on the hosting service. Regulation at the level of a hosting service varies, and debate about whether service providers are responsible for the online activities of those who use their services continues.

The report deals briefly with resources that are essentially invisible to or hidden from the open internet, or that cannot be accessed directly from the public internet. While these parts of the internet present the majority of regulatory challenges and are of significant concern for law enforcement, they are not analysed in detail in this report as they are too far removed from the limited scope of regulation through the operation and governance of the DNS.

Research questions

These questions formed the basis of the current research.

- What is the DNS and how does it operate within the framework of internet governance?
- How has the DNS been misused for criminal purposes?
- What is known about perpetrators of DNS misuse? That is:
  - What are their motivations and what benefits did they obtain?
  - What are their countries of origin?
  - Do they operate alone or with others?
  - Why did they select the targeted domain name?
  - How have instances of DNS misuse been dealt with and what were the outcomes of any investigations?
- What crime prevention strategies do domain name owners, DNS server owners and registrars currently use to prevent DNS misuse?
- What other crime reduction strategies could be implemented to prevent misuse of the DNS?

Findings

Background

This section explains the internet's development and operation and reviews the environment in which criminal misuse of the DNS has emerged. It explains the internet's infrastructure and discusses the operation and governance of the DNS, highlights weaknesses in the regulatory framework that increase the potential for misuse, and identifies the strengths that may help prevent misuse. The internet's nature and its governance structures result in weak regulatory responses to misuse of the DNS.

Criminal misuse of the DNS

This section explores criminal misuse of the DNS by firstly considering illegal acts that do not amount to cybercrime offences, including property offences like the theft of hardware and domain names, and, secondly, misuse that falls within the general classification of cybercrime. It presents a tentative analytical model that relates forms of misuse to particular aspects of the DNS, namely to:

- the DNS architecture;
- domain names (or domains);
- domains as virtual spaces; and
- other layers at some remove from the DNS.

This model helps to explain misuse occurring within the architecture of the internet (software engineering) as well as misuse facilitated through human interaction (social engineering).

The section then examines opportunities for misuse in terms of the DNS' primary purpose, which is to overcome restrictions created by the internal architecture of the early internet. This misuse concerns how machines use internet addressing to make connections between resources. Misuse through software engineering is further classified according to whether the DNS is itself the target of misuse or is used to facilitate other offending; facilitating other offending may involve misusing the DNS as a mechanism to do harm, a vector to transmit harm or a platform from which to commit harm.

The outward appearance and presentation of internet for human users is then considered. A division can be drawn between misuse intended to manipulate machines through software engineering and misuse intended to manipulate people through social engineering.

To distinguish between abuses of the DNS and abuses that exploit applications layered above the DNS, DNS misuse may also be categorised according to the architecture of the internet. This helps identify who could potentially prevent misuse and potential points for regulatory intervention.

Perpetrators of misuse

The many and varied forms of DNS misuse identified in this study make it difficult to describe a typical offender or criminal justice response, particularly given the absence of criminological research in this area. The limited research so far conducted has found a high incidence of organised crime activity. This often involves loose groups of people, usually young men with limited technical abilities who rely on online guidance. Perpetrator profiles also differ according to the extent of the perpetrator's involvement in the darkweb. There is limited evidence to indicate where those misusing the DNS are located.

Legal responses to DNS misuse

Although some instances of misuse can be addressed through the criminal justice system, there are many impediments to harnessing the criminal courts as a regulatory response. Few conventional crime categories are relevant apart from, arguably, some property crime offices such as theft of domain names, or the criminal infringement of intellectual property rights. Of greater relevance are specific offences created under cybercrime legislation that governs unauthorised access to networks, data interference and acts of online dishonesty associated with domain name misuse. There are also criminal offences arising from social engineering, including identity misuse, misleading and deceptive conduct, and fraud. To date, these have not been used due to problems of evidence and proof, jurisdiction, and the limits of law enforcement resources in identifying suspects, seeking mutual legal assistance and mounting prosecutions. Over time, as the jurisprudence of DNS criminality develops, criminal proceedings may be more successful. Whether this would deter criminals from committing DNS crime remains conjectural.

In addition to criminal justice responses to DNS misuse, there are a number of avenues for redress through the use of the civil laws relating to obligations and intellectual property. 'Webjacking', and disputes about the registration of domain names that could lead to legal action about 'cybersquatting' or 'domain name squatting', can be resolved by taking action under the Uniform Domain-Name Dispute-Resolution Policy (UDRP) adopted by domain name registrars. In appropriate cases of infringement of contractual rights or intellectual property related to registered names, where economic loss can be quantified and proved, civil action can be taken in relation. Where business interests are at stake, injunctive relief can also be useful.

Preventing misuse of the DNS

A number of environmental crime prevention strategies could be used to reduce the harms associated with DNS misuse, including routine activities theory, crime pattern theory and rational choice theory. Crime prevention is considered by reference to various regulatory touchpoints within DNS regulation. Importantly, these regulatory touchpoints often lie outside the scope of national laws, which creates opportunities for exploiting regulatory weaknesses for criminal purposes. Some strategies to reduce the risk of DNS abuse include:

- enhancing identification checks when registering domain names;
- using Domain Name System Security Extensions;
- making DNS abuse less profitable by coordinating reporting mechanisms and controlling online profit centres;
- neutralising offender rationalisations; and
- improving user education on the risks of DNS misuse.

Conclusions

The DNS is fundamental to the functioning of the internet, and its potential for misuse is one of the most important legal and regulatory challenges facing internet governance in the years ahead. A failure of the DNS would impede machine-to-machine communication, and make it difficult for users to navigate the internet.

However, the capacity to regulate possible misuse of the DNS is limited. While the DNS requires centralised authority, no single global entity is responsible for the regulation of all its aspects. This is because regulation of the DNS, like other aspects of the internet, occurs under a multi-stakeholder model of governance and a distributed administration model. It is also a result of the fact that much of what happens on the internet is beyond the jurisdictional reach of the criminal law of individual nations.

Nonetheless, regulating DNS registration and addressing the security weaknesses of internet architecture would provide some limited means of controlling the environment to prevent criminal misuse of the DNS and the internet. Although there will always be a place for criminal justice responses to internet abuse, in the global regulatory environment in which the DNS operates prosecution of DNS misuse will be difficult, and is likely to be reserved for the most serious and obvious infringements. As with other online crime, enacting a uniform set of policies to prevent misuse before it arises is likely to be the most effective strategy.

Introduction

In the twenty-first century we are all increasingly dependent on the internet. At the same time, the internet's global reach and the density of possible connections continue to expand, despite evidence of some tapering of growth in 2015 (ITU & UNESCO 2015:9). Major developments include the growth of mobile and wireless technologies (ITU 2014); increased reliance on cloud services (Burt et al. 2014:10); and the emergence of 'the internet of things' where everyday objects become part of the internet (Evans 2011). Not surprisingly, the CSIRO identified the development of the virtual world as one of six interlinked global megatrends that will shape how we live in the 20 years from 2012 (Hajkowicz et al. 2012). The other megatrends are resource depletion, loss of biodiversity, shifting economic power, ageing populations and increasing expectations about service delivery.

The DNS is a naming system for resources that connect to the internet via the World Wide Web. It allows internet addresses and domain names to be coordinated. Two kinds of unique identifiers make it possible to connect with particular resources across the internet. However, the DNS entails more than just domain registration; it provides the key that allows machines and people to make connections using the protocols (IPv4 and IPv6) on which the internet is currently based. As a system, the DNS transforms the method for addressing resources on a network to create wholly new possibilities for misuse, such as the 'territorialisation' of the internet; the exploitation of common security risks at the software engineering level; and opportunities to reach, target and manipulate internet users.

The DNS was introduced by the Network Working Group (NWG) in 1983 in Request for Comments 882 (Mockapetris 1983). Two years later, <symbolics.com> became the first second-level dotcom domain (Attalah 20-15: 1). This granting of ownership over a new second-level domain marks the beginning of the modern internet (Atkinson et al. 2010). The DNS is now more than 30 years old, and it is hard to imagine how the internet would work or how people would navigate it without the DNS.

In the first 30 years of the DNS there was enormous growth in the scale, range and operation of the internet, driven by demand beyond the control of those who collectively govern it. The response has been evolutionary, with both the original nature of internet governance and its fundamental architecture (made up of standard protocols and software) persisting as templates to be adapted, rather than discarded.

These developments in information and communications technologies greatly enlarge the enormous opportunities and possible risks associated with the internet. While not all of these risks are the subject of cybercrime laws, global concern about cybercrime continues to increase (USDOJ 2004; Jakobsson 2012; Europol 2015; Malby et al. 2013; House of Commons Home Affairs Committee 2013; Rusmussen & Vixie 2015).

However, the role of the DNS as a target or facilitator of cybercrime offending has been given limited attention. In Australia, the responsibilities of domain registrars were examined by a Commonwealth parliamentary committee, which recommended the adoption of a best practice code for handling maliciously operated domains (Standing Committee on communications 2010). Europol (2014) drew attention to the use of malicious and bad-faith domain registrations to facilitate criminal activity and repeated similar comments in 2015, raised concerns about how some <.onion> domains associated with criminal activity —which can only be accessed using The Onion Router (TOR) software—could be located using the DNS (Europol 2015:65). This issue was also reported by Thomas and Mohaisen (2014). This study helps to situate criminal misuse of the DNS within the existing framework of national cybercrime laws.

Malicious or criminal exploitation of the DNS can vary considerably and can target any of the principal features of the DNS, as illustrated in Table 1. The DNS can be misused via the creation of malicious domains. Domain names can be registered specifically to facilitate malicious activity—for example, domain names can be registered in bulk for fast-flux hosting of phishing attacks (ICANN-SSAC 2008). Alternatively, the DNS can be abused by compromising existing legitimate domains or using DNS-based software exploits to manipulate the DNS as a system for data transmission and exchange. Not all forms of exploitation are necessarily criminal in themselves, but they may form part of a current or future criminal enterprise.

Table 1: A categorisation of malicious or criminal exploitation of the DNS	
Nature of DNS exploitation	**Example**
Non-cyber offending involving domain names as territory or property	Stealing a domain name
Registration of domains specifically to engage in malicious activity	Registering domains for direct phishing attacks
Cyber offending through attacks on the operation of the DNS	Root server attacks
Cyber offending through software engineering with direct pathways—single-step misuse	Hacking directly into a database
Cyber offending through software engineering with indirect pathways—multi-step misuse	Phishing to gain access to compromised computers to create a botnet to launch other forms of misuse such as a denial-of-service attack
Cyber offending through social engineering using the DNS	Registering and operating a domain name to be falsely represented to other users or to impersonate another legitimate domain name
Using the possibilities of the DNS to create a platform for offending	Running a criminal enterprise using the possibilities offered by the internet to hide illegal behaviour or identity, or evade jurisdiction

It is important to note these divisions are not clear in practice, and that offending may involve one or more of these features, or possibly all of them, in any given case. Instances of exploitation that, for whatever reason, lie beyond the reach of national cybercrime laws should be examined; by examining DNS misuse as a phenomenon in itself, rather than simply as a subset of existing national cybercrime offences, this report identifies other regulatory frameworks that may aid in the development of more effective crime prevention responses. At the same time, this study highlights those attributes of the internet that limit the reach of governance.

The DNS and the internet

The internet is a rule-based engineering construct that connects resources to become a network of networks, comprised of billions of resources. The internet works as long as each resource can be identified and located correctly at any time. Identification and location of resources at a machine level currently relies on IP addresses, following specifications developed in 1981. While we speak of locating resources, what currently happens is that the internet connects between hosts where resources are located. Jacobson et al. (2009: 1) described how the current method for locating resources using the DNS relies on resource-sharing between two machines acting as hosts, and internet traffic involving conversations between pairs of hosts. This identifies where content is located. IP addressing and the DNS are simply the dominant modes of identifying and locating these resources, but other ways of

networking resources are possible. Examples include bulletin boards, peer-to-peer networks and the darknet.

One proposed engineering alternative is Networking Named Content. This would establish connections based on what data are to be exchanged, rather than their location (Jacobson et al. 2009:1). The National Science Foundation (2015) funded the Named Data Networking (NDN) Project to investigate this possibility (Zhang et al. 2010). The possible transition from 'a host-centric network architecture (IP) to a data-centric network architecture (NDN)' is showing some promise and is thought achievable without discarding all elements of the DNS (Zhang et al. 2014:1).

Internet protocols (Internet Protocol Version 4, or IPv4, and Internet Protocol Version 6, or IPv6) are the machine-readable addressing systems that identify and locate resources electronically on networks including the internet. In simple terms, the DNS enabled the transformation of the original ARPANET into the current internet by unlocking the potential of non-hierarchical addressing. However, the DNS is not used for networking the entire Internet, and it is not the same as the Internet.

The internet

Before discussing internet and DNS governance, it is important to consider the conceptual framework to be applied. MacLean (2004) noted that governance of the public internet involves disparate interests with distinct views about the scope and means of governance. One important issue is how different interest groups define the internet and governance.

As noted by DeNardis (2012:1), the internet (and the DNS) is engineered according to internet invariants set out by the Internet Society. The invariants divide into those that principally affect the internet's architecture (global reach, potential connectivity of end devices and interoperability) and those that principally affect human interaction with the internet (freedom to innovate without consent, general purpose support and governance invariants). It is important, therefore, to recognise that more is engineered into the internet than its basic architecture, and that the internet encompasses a liberal and open approach to human interaction and cooperative regulation.

However, as Rutkowski (2004) pointed out, common legal definitions, such as that of the United States Code, are narrow and infrastructure-centred. This code defines the internet as the 'international computer network of interoperable packet switched data networks' 'based on ARPANET and using the Internet protocol suite comprising the Transmission Control Protocol (TCP) and the Internet Protocol (IP)' (Title 47, Section 230).

There has been some criticism of legal definitions of the internet. One issue is that resources that are not part of the internet may, however, use its addressing protocol. For example, the Cybertelecom Project critiqued a focus on network infrastructure, noting that the TCP/IP method of network operation is not unique and is used by other networks that are not part of the internet use it (Cybertelecom 2014a). A focus on infrastructure may also divert attention from the role played by private sector ownership of global decentralised networks and

infrastructure which has important implications for finding points for regulation or control (Kruger 2013).

Another concern is that narrow definitions ignore the potential arising from increasing levels of machine and human connectivity (Hill 2013). Hill summarised the competition between narrow legal definitions based on network architecture, wider definitions that take into account applications that the network supports and, ultimately, the combined potential of networks both of machines and of people. Hill (2013: 1–2) advocated a broad definition, like the Federal Networking Council's (FNC) definition of the internet in 1995 as:

> A global information system that:
>
> (i) is logically linked together by a globally unique address space based on the Internet Protocol (IP) or its subsequent extensions/follow-ons;
>
> (ii) is able to support communications using the Transmission Control Protocol/Internet Protocol (TCP/IP) suite or its subsequent extensions/follow-ons, and/or other IP-compatible protocols; and
>
> (iii) provides, uses or makes accessible, either publicly or privately, high level services layered on the communications and related infrastructure described herein (cited in Kahn & Cerf 1999: n. xv).

In a similar vein, Cybertelecom (2014b) emphasised the internet's 'unique networked community.' It advocated recognition of the internet as 'a particular network that is neither the underlying infrastructure nor the overlying applications. It is a particular logical network, created over existing physical networks, creating a global network of interconnected devices and users' (Cybertelecom 2014b: np).

How the internet is defined depends on context. For legal purposes, a restricted architecture approach focusing on a particular aspect of legislation may be required. However, beginning with a narrow definition ignores other actual or possible attributes or values of the internet that might otherwise inform how the law responds. Considering internet architecture when using an infrastructure-based definition helps focus on where accountability may lie. References to the underlying architecture also assist in identifying how various aspects of the internet are, or may be, regulated by a variety of actors.

Less visible parts of the internet

There is more to the internet than the open or surface web. There are other, less visible parts of the web: the deep web and the dark web, or darknet. These parts of the internet are not considered in this report due to their remoteness from DNS governance; alternative networks are only considered as examples where the DNS is manipulated or adversely affected in ways that are inconsistent with the principles underpinning the DNS and internet governance.

The use of these terms is not uniform. For example, Sui et al. (2015: 6) referred to the darknet as part of the deep web, and define the deep web as resources that are not indexed, estimating this realm is four to five hundred times larger than the surface web or open internet. The authors reported that the darknet was originally 'any or all network hosts that could not be reached by the Internet' (Sui et al. 2015:6) but included the darknet as part of the deep web because of the networking between hosts.

In this report, the less visible parts of the web are defined according to the technical means required to access them. The deep web and the darknet share some aspects of the underlying architecture of the internet and could, technically, be accessed via the open web without specialist software. Both use IP addressing or functions but are not usually directly visible to internet users. The deep web refers to resources that are not indexed or that employ a barrier—such as a paywall—or another method to prevent indexing or mediate access, and these measures prevent direct connection. Deep web resources have IP addresses but do not present themselves to the network. In contrast, the darknet refers to parts of the internet accessible only via a gateway such as TOR.

As noted by Sui et al. (2015), each of these less visible spaces could be criminally misused and, accordingly, each deserves closer study. The principles underlying the internet allow for experimentation and the design of alternative networks which could be, or which may become, vehicles or platforms for criminal misuse.

The creation of alternative networks is driven by the desire to avoid content restrictions and maximise anonymity or privacy. These desires may motivate both those with criminal motives and, equally, those whose motives are not criminal. Users continue to demand ways to avoid content restrictions such as controls over breaches of civil or criminal law such as intellectual property infringement, child exploitation material, hate speech or terrorist activity. Alternative networks may also be set up to facilitate freedom of expression and political expression.

The demand for greater anonymity and privacy on the internet is driven by wide-ranging concerns. These include protecting online identity and security, and avoiding state or corporate security surveillance. Anonymity, privacy and protection from surveillance are also important factors in protecting criminal activity.

Driven by these demands, some alternative networks have come to prominence over the years. Two of the most utilised were built using peer-to-peer technology and Virtual Private Networks (VPNs). Chaudhary and Surolia (2015) described various peer-to-peer structures. Peer-to-peer networks may be centralised (eg Napster) or decentralised. The decentralised forms may be structured (eg Chord) or unstructured (eg Gnutella). Prominent examples of VPN-based alternative networks use The Onion Router (TOR) software. The Silk Road, used in part as a

marketplace for illicit drugs, was built on a TOR platform (Sui et al. 2015).

One possible threat to DNS integrity is the leakage of requests to locate TOR addresses into the global DNS resolution process, which complicates namespace management. Thomas and Mohaisen (2014) also raised concerns about the possible role of malware and attendant security risks for those unfamiliar with the use of TOR software.

The internet's layered network architecture

To understand the role the DNS plays, it is useful to consider where the DNS lies within the internet's layered structure. There is a divide between services provided by hosts above the transport layer and the services of routers and switches at or below the network layer (Yoo 2013). Within the layered model, the DNS lies at the network level relating to the IP.

How the internet and a resource are connected depends on both physical infrastructure, and various protocols for connecting the device and managing what happens while that device is connected. The result is a conceptual and practical layering of the internet, represented in different models. In general, the layered structure is made up of both the physical and non-physical components and the protocols and functions applied in each layer. The IP and the DNS map the network; the Transmission Control Protocol (TCP) allows the transport of data. The TCP/IP allows machines to connect to each other via a network, and to communicate and transfer data.

Ravali (2015) described the seven layers of the Open Systems Interconnect (OSI) model developed by the International Organization for Standardization. The layers are:

- application;
- presentation;
- session;
- transport;
- network;
- data-link; and
- physical.

The OSI model expands the application level of the TCP/IP model to application, presentation and session levels, and adds a separate physical layer. Yoo (2013) identified four levels of the model: application, transport, network and datalink. These four non-physical levels lie above the physical or spectrum-based means a device uses to access the internet. Bush and Meyer (2002) cautioned that there are profound differences embedded in the different representations of network architecture as shown in the OSI and TCP/IP models. The strict ordering of layers may also conflict with efficiency principles; Bush and Meyer emphasised the importance of keeping network architecture as simple as possible. They related simplicity to security, arguing that complexity inhibits modelling and analysis and can obscure security risks arising from change. The TCP/IP model, with the physical layer added, is shown in Table 2.

Table 2: The layers of internet architecture

OSI model	The modern TCP/IP reference model		
	Layer	Location	Protocols
Application	Application	Process-to-process	SMTP (email) HTTP (web) FTP (file transfer) Telnet (remote login)
Presentation			
Session			
Transport	Transport	Host-to-host	TCP (reliable) UDP (unreliable)
Network	Network	Router-to-router	Internet Protocol (Assignment of IP addresses) Domain Name System (DNS) Root server configuration
Datalink	Datalink	Switch-to-switch	Ethernet Connection-oriented (X.25, ATM, Frame Relay) Wireless (802.11, Bluetooth)
	Physical	Within network	Twisted pair (telephone) Coaxial cable Fibre optics Spectrum

Source: based on Yoo 2013: 1,741

Yoo described how the architectural framework has changed in response to emerging demands, uses, opportunities and threats to address resulting issues of reliability, congestion, optimisation and security. According to Yoo many responses to security weaknesses, such as the deployment of firewalls and deep packet inspection for security threats, involve network-based solutions that 'violate the principles of protocol layering' (Yoo 2013: 1,769).

Distinguishing application-level risks, threats and regulation

The DNS operates at the network level of the internet's layered structure, in router-to-router connections. The importance of this reference model is that it helps to isolate more precisely where a particular form of misuse occurs in relation to all the possible processes involved in a single internet connection between devices.

Locating a particular form of abuse using the reference model helps better distinguish how and where that abuse occurs. The reference model also helps identify where there may be capacity for regulation, or accountability implications, for internet users or service providers.

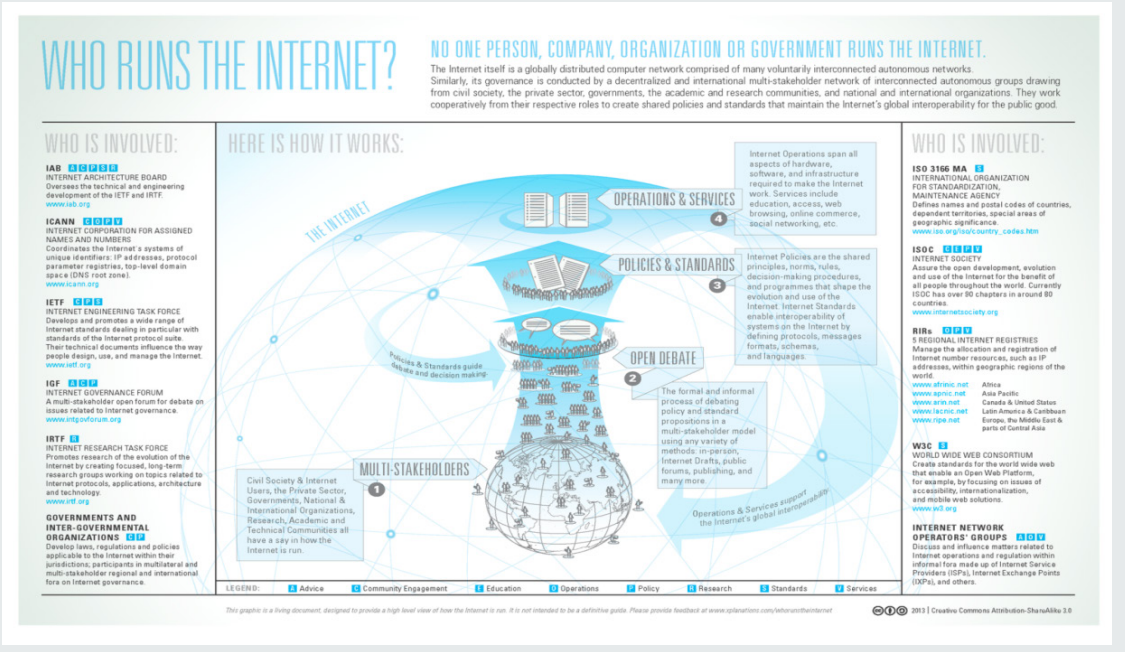
For example, registering and using a misleading domain name for a criminal purpose is tied closely to the DNS and calls for a regulatory response within the DNS. The registration and use of a misleading subdomain using a hosting service is a matter for regulation by the hosting service. A subdomain is not a new domain, but rather a web address allocated within an existing domain.

Internet governance

While no government controls the internet, the United States has had a central role in the initial allocation of names and numbers. The functions of the Internet Assigned Numbers Authority (IANA) were originally contracted by the United States Department of Defense to the Information Sciences Unit at the University of Southern California. In 1999, the IANA functions were contracted to the Internet Corporation for Assigned Names and Numbers (ICANN; NTIA 2015). However, in 2014–15, United States policy favoured formally handing over ultimate responsibility for the IANA functions as part of a commitment to a multi-stakeholder approach to internet governance.

Internet governance is dynamic and unpredictable (Weber et al. 2010). Internet governance follows a multi-stakeholder model, which places the internet beyond the control of individual nations. Various official forums and agencies play a role in internet governance; these diverse interests are indicated in the diagram shown in Figure 1 (Lipinski 2013).

Figure 1: Internet governance: Who runs the internet?



Source: Lipinski, L 2013. Who runs the internet? via Wikimedia Commons under Creative Commons Attribution-Share Alike licence https://creativecommons.org/licenses/by-sa/3.0/

Many of these entities have multiple roles. Weber et al. (2010) argued that the nature of the internet and a multi-stakeholder approach to its governance mean that effectively all users

have a stake in regulatory responses. They argued that technical issues such as the change from one internet protocol to another are not just technical matters but involve significant public policy choices about how the web functions. All users and non-users have both a stake in the internet and a right to consideration and engagement in its governance.

While the multi-stakeholder model applies at a global level, governments may impose internet controls at a national level (Murdoch & Roberts 2013). These authors describe a battle for control of the internet and note that potentially high levels of connectivity may be constrained, particularly at a national or local level, by network infrastructure limits to do with 'hardware implementation,' or by socio-political limits imposed by 'the politics of control' in different countries.

Weak regulatory capacity

There is little capacity for regulatory responses to the misuse of the internet because of its nature and governance structures. Internet regulation depends on high levels of national and international cooperation between governments, service providers, industry and users. For some, increased internet regulation is completely at odds with the principle of openness, and others consider regulation of the internet to be technically impossible. Authority is decentralised and regulatory capacity limited, with a primary focus on ensuring the interoperability and functionality of the network of networks that makes up the internet. The Internet Architecture Board (IAB), the Internet Engineering Taskforce (IETF), the International Organization for Standardization, Maintenance Agency (ISO 3166 MA) and the World Wide Web Consortium (W3C) set the standards for internet functionality.

The Internet Governance Forum (IGF) and the Internet Society (ISOC) exercise high-level functions. The Internet Network Operator's Groups include various forums for internet service providers (ISPs), internet exchange points (IXPs) and others. The Internet Research Task Force (IRTF) promotes research of importance to the evolution of the internet by creating focused, long-term research groups to work on issues related to internet protocols, applications, architecture and technology.

The domain name system

The DNS and the IP are related, and a discussion of DNS misuse inevitably requires consideration of the underlying IP address system as well. The IP allows electronic resources to be identified whether they are connected to the internet or not. The DNS uses this convention to create a naming system for resources that connect to the internet via the World Wide Web.

The DNS coordinates IP addresses and domain names (the two forms of unique identifiers that make it possible to connect with particular resources across the Internet). The DNS is, therefore, sometimes likened to an 'address book' for the internet (Gersch 2007: 5).

The DNS was introduced to overcome two problems that emerged as the early internet began to expand rapidly. The first problem was the difficulty of managing the table of IP addresses because they were assigned non-hierarchically. The second problem was that human users found it difficult to navigate across resources using IP identifiers that consist of strings of numbers. To overcome these issues, the DNS provides two address books for locating all devices connected to the internet, which is now integral to how most people interact with it.

Engineering

The first DNS address book organises addresses written in IPv4 and IPv6. The DNS was designed to enable network connection between a rapidly growing number of IP addresses. Before the DNS, the method of identifying each resource on the ARPA Internet used a non-hierarchical table of numbers to relate host names to ARPA Internet addresses. The size of the table and the frequency of updating it were 'near the limit of manageability' (Atkinson et al. 2010: 1). The engineering objective was to overcome the problems arising from accelerating growth in the number of resources and resource locations across multiple administrative boundaries and locations.

The example in Box 1 illustrates the hierarchical nature of the DNS. A simple three-level domain name places a resource within a top-level domain such as .au, followed by a subdomain such as .gov, then the specific domain name, such as aic.

Box 1: Navigation by domain name

The 32-bit IPv4 address rendered in a human-readable format for the AIC homepage is 113.20.25.130. IP addresses are read from left to right—from the highest level in the hierarchical organisation to the lowest.

A user can also navigate to the same site by typing the domain name address aic.gov.au into your browser. The URL for a domain name such as aic.gov.au is read from left to right—from the lowest hierarchical level to the highest.

A US Government website, such as that of the National Institute of Justice with the IP address of 149.101.16.39, appears as nij.gov. There is no top-level designation for the United States because the assignment of names and numbers for the internet was first contracted there.

The hierarchical framework of the DNS allows IP addressing to be scaled, and internet routers now use a hierarchical table of IP addresses to connect devices. Scalability means increasing numbers of available resources can be connected; a web browser can be used to access any one of the billions of resources accessible via the World Wide Web in an instant.

The creation of internet topography is a by-product based on the allocation of addresses within the table. Resources on the open internet are located using IP addresses, most of which were allocated after the DNS was introduced. With the DNS, IP addresses are distributed hierarchically from top-level domains (TLDs) down. Information is carried in the IP address according to the TLD's heirarchy for allocating IP addresses and domain names. IP addresses, therefore, carry information about the top-level domain (TLD) and any lower-level domain in which they were issued.

Where IP addresses and domain names fall under a country code top level domain (ccTLD) such as .au, the IP addresses and domain names can be associated with the country code of the country of issue. How accurately an IP address or domain name is associated with a ccTLD depends on whether there are any obstacles (formal or informal) to obtaining an IP address or domain name from outside the geographical remit of a particular ccTLD. Also, various applications may be used to mask the true IP address or associated domain of a particular resource.

Importantly, while resources require an IP address and IP addresses are issued within a particular domain, this does not mean that all resources require a domain name. There are many more IP addresses than there are domain names, and not all users require a personal domain name. Nor is every IP address assigned to a unique domain; rather, only a few IP addresses indicate a particular domain name.

Human interaction

The second DNS address book converts machine-readable IPv4 and IPv6 code into a natural language that people can read. In doing so, the DNS aids human navigation of the internet as well as allowing parts of cyberspace to be named, creating virtual territories that can generate value.

The DNS allows users to create territories in cyberspace, beginning with the various TLDs that include country-based domains or named domains such as .com, .net, org and .xxx. The clustering of domains that fall under national domain registries such as .au forms a topography of virtual space that, at least in part, is analogous to physical geography. However, there are exceptions such as US-based domains that do not require the US to be identified as the TLD. For example, the website of the Bureau of Justice Statistics in the United States appears as bjs.gov. Some country-based TLDs, such as .tv (Tuvalu), have been sold to private interests unrelated to the assigned nation, and some allow buyers to purchase domains without demonstrating a connection to the physical territory of the country.

The places claimed and used for all manner of purposes and interests in the generic TLDs such as .com, and more specific interests in named TLDs such as .xxx, create an additional topography of virtual space. It costs money to register and maintain these cyberspace territories created under the DNS. They have an added value beyond the cost of registration, arising from exclusive usage rights to the use of that particular domain name. Examples of the value of such territories are the prices paid for particular domains. The TLD .blog was reportedly purchased for US$20m (McCarthy 2015a)and the domain 558.com for US$1m (Berkins 2015).

The creation of platforms for online activity that may or may not be in breach of national laws, in some or all of the nations where that platform is accessed, is related to the territorialisation of cyberspace. The DNS allows users to navigate the internet using human-readable characters that form words or readily understood letter combinations or symbols, instead of the underlying binary or decimal IP addresses used by software in network communication. The identity of a resource may be interpreted by a person using language or symbols typically represented in a web browser address bar. The DNS makes it possible to go to, search for or see, a domain (for example .gov.au) using letters. Within each level of a domain name, resources may be identified using letters representing words, trademarks, acronyms or shortened words, rather than numbers. Once a domain name is allocated, the owner of the domain may organise resources in that domain so that specific pages appear in a URL either before or after the domain name, such as http://www.aic.gov.au/crime_types/cybercrime.html.

The DNS is simple to use and readable, and the process of resolving IP addresses to matching domain names is seamless and invisible to the ordinary user. Millions of computers work to resolve user requests. As Simon (2006: 43) put it: '[T]he genius of the DNS is how the list gets refreshed. Those millions of local servers don't need to keep a persistent memory of every name-to-number pairing, just the address of at least one server in the root zone. In turn, each root server contains a list of top level domains (TLDs) servers.'

While the DNS was designed to overcome engineering limits and facilitate human interaction, it also created wholly new possibilities. One was the ability to identify IP addresses and domain names within a hierarchical framework that in many instances maps to the physical world. Another was to give non-geographical territorial dimension to 'virtual space.' As a result, cyberspace could be marked out by domains representing individuals, organisations, governments or things. These new territories enabled by the DNS have created new forms of identity, property and place.

The DNS also creates an internet landscape of locatable resources across the internet where domains function as virtual places. These places can foster misuse or criminal activity in different ways: as spaces for offenders to inhabit or as platforms to launch criminal activity, or as targets for criminal activity. The DNS allows human users to read web addresses with characters other than the underlying software-designed numerical IP addresses. For domain owners, the use of natural language and symbols (initially in English) means that domain owners can name parts of the internet, and this has created wholly new virtual spaces. Some individuals and many corporate users have come to rely heavily on ownership or control of a particular domain name. However, not every device or user requires (or has) its own domain name. There are costs associated with establishing and maintaining domain name ownership, and ordinary users are perhaps unlikely to obtain one. Also, where a domain name is allocated, it does not necessarily have to be used or made available on the internet.

In 2010, the introduction of internationalised domain names allowed the use of non-Latin scripts in the top-level domain—a major development in the availability of domain names (Al Helou & Tilley 2010). The number of TLDs available has also been expanding since the announcement in 2013 of up to 1,000 new generic top-level domains (gTLDs). More than 500 of these were allocated by early 2015 (Attalah 2015).

DNS governance

More than at any other time in the last 30 years, DNS governance is at a critical point, with the whole model of governance at issue and wide-ranging implications for the future of the internet as a single global platform.

ICANN, the co-operatively organised institution that manages the DNS, is currently contracted by the United States Government to perform the functions of IANA, including supervising the allocation of IP addresses and coordinating the IPv4 and IPv6. ICANN directly controls the creation of TLDs. ICANN delegates authority to local domain name authorities at the TLD level to organise domain name registries within those TLDs.

As ICANN (2007) indicated, in addition to IP addresses and domain names, the DNS relies on authoritative root servers to ensure that resources connect correctly. There are thirteen addresses globally for the root servers; these operate autonomously to ensure internet traffic is directed accurately by the index of addresses for each TLD kept by ICANN. The root servers ensure that IP addresses match the correct server hosting the index for a particular domain at the TLD level.

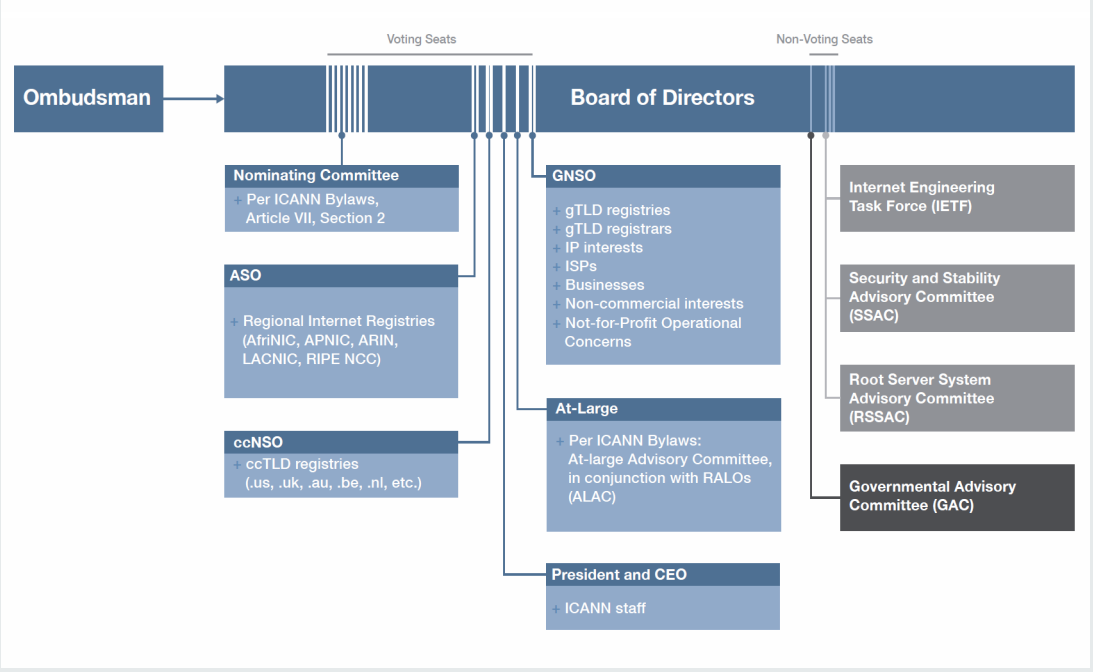
The DNS is not simply about the allocation of domain names. The DNS put forward in RFC 882 has three components: the domain namespace, name servers and resolvers (Mockapetris 1983). These remain the core elements of the DNS, used to connect resources to the internet (Internet.nl 2015). Strong central coordination is required to maintain the accuracy of IP addresses, domain name registries and the server indices at the root and domain levels. However, this does not translate into a strong regulatory authority as day-to-day control is distributed hierarchically across the levels of the DNS and the scope of centralised regulation is limited. The multi-stakeholder model of internet governance creates many divisions and levels of governance, within which strong coordinating principles of access and openness apply. This arrangement limits the power of agencies and governments to regulate the internet. In this context, national cybercrime offences play an important but limited role.

The administration of IP addresses and domain names follows a hierarchy with the central global authority of ICANN and regional, national and individual domain registries. The hierarchy of the DNS flows from top-level domains to second-level domains and subdomains within domains. ICANN (2012) set out its coordination responsibility for the first two components of the DNS: it is responsible for the allocation and assignment of three sets of unique internet identifiers—domain names, IP addresses and autonomous system numbers, and protocol port and parameter numbers. ICANN also has overall responsibility for the operation and evolution of the DNS root name server system distributed across 13 root server authorities.

Other aspects of internet software and physical infrastructure are not centrally controlled but require a degree of central coordination. Software protocols must be coordinated to resolve or look up domain names. Coordination is also required for the physical infrastructure of the Internet including root servers and resolvers to handle DNS queries.

The ICANN organisation chart (ICANN 2012) shown in Figure 2 sets out the related entities with voting or non-voting seats on the ICANN board. The Nominating Committee (NomCom) 'is an independent committee tasked with selecting eight (voting) members of the Board of Directors and other key positions within ICANN's structure'.

Figure 2: ICANN organisation chart



Source: (ICANN 2012)

Other voting seats are for the Address Supporting Organisation (ASO), which represents the five Regional Internet Registries (RIRs; ASO 2015). The RIRs service different regions globally, managing the allocation and registration of internet number resources at a regional level. Australia is covered by the Asia-Pacific RIR (APNIC 2015a).

Beneath the RIRs, ICANN recognises top-level domain authorities responsible for the management of resource allocation within that domain. Australia's top-level domain manager is auDA. This level of governance is represented on the ICANN Board through the Generic Names Supporting Organization (GNSO) 'which fashions (and over time, recommends changes to) policies for generic TLDs (eg .com, .org, .biz). The GNSO strives to keep gTLDs operating in a fair, orderly fashion across one global internet while promoting innovation and competition' (GNSO 2016: 3).

The Country Codes Name Supporting Organisation (CCNSO) is a 'forum for country code Top Level Domain (ccTLD) managers to meet and discuss topical issues of concern to ccTLDs from a global perspective' (ccNSO 2015: np).

The DNS war

Since the DNS's inception, its governance has been subject dispute; this has been termed the 'DNS war.' Mueller (2002), Pare (2003), Simon (2006) and Pavan (2012) have examined the DNS war in detail. Pare (2003) pointed to the complexity of competing interests involved in the DNS

war. Arguments raised include concerns about the internet as a whole involving architecture and function and governance at a global level. Other concerns focus on the individualised benefits of domain names, such as intellectual property.

According to Simon (2006) disputes were driven by those who promoted control by narrow interests such as the market, engineers or nations and those who argued for distributed control with a new 'global constituency:'

> …an overarching goal shared by most participants was to organize an accountable, deliberative body capable of governing the administration of key DNS resources. A central point of contention was how to constitute a legitimate organization whose officers would, on one hand, be expertly conscious of the Internet's technical constraints and, on the other, be directly responsive to the as yet unarticulated interests of a legitimating global polity (Simon 2006: vi–vii).

DNS governance has been the subject of vigorous debate from the beginning. Since 2000, the following IANA functions have been contracted to ICANN by the US NTIA (2015):

- coordinating the assignment of technical internet protocol parameters;
- administering certain responsibilities associated with root-zone management;
- the allocating internet numbering resources; and
- other services related to the management of the ARPA net and .int (international) TLDs.

The long-running arguments about governance assumed greater urgency in 2014 when President Obama set out to transfer full responsibility for the functions of IANA currently contracted to ICANN. The United States Government confirmed the formal transfer of IANA functions to ICANN as part of the privatisation of IANA functions. However, the initial time frame was amended in October 2015, when the United States Government renewed its contract with ICANN for another year as the transition process became mired in disagreements (McCarthy 2015b). The Assistant Secretary of the NTIA set out the conditions sought by the United States Government for transfer Strickling 2014). These included commitments to 'supporting and enhancing the multi-stakeholder model of governance'; maintaining 'the security, stability, and resiliency of the domain name system', meeting 'the needs and expectations of the global customers and partners of the IANA services' and maintaining 'the openness of the internet.' Strickling emphasised that oversight by 'a government or group of governments would not be acceptable' (Strickling 2014: 6).

auDA

Initially, the administration of the .au domain was assigned by IANA to one person— namely, Robert Elz, a computer programmer at the University of Melbourne. In October 2001, ICANN signed a ccTLD sponsorship agreement with .au Domain Administration (auDA) which sets out the commitments of both ICANN and auDA. The agreement records that both desire that 'the Government of Australia assume responsibility for overseeing the interest of Australia and its internet community', and that the agreement between auDA and ICANN represents an allocation of responsibility between the Australian Government and ICANN (ICANN 2001: 2). Prior to entering this agreement, auDA reported on how it would meet Australian Government objectives for self-regulation, and thereby secured government endorsement as Australia's domain authority. Government endorsement was subject to conditions, including that auDA recognise that the DNS 'must be administered in the public or common interest' and 'management and administration of the .au ccTLD is subject to the ultimate authority of the Commonwealth of Australia' (Alston 2000:1).

Earlier in 2000, the Australian Government amended the *Telecommunications Act 1997* (Cth) and the *Australian Communications Authority Act 1997* (Cth). The amendments clarified that any Australian domain authority was subject to Telecommunications Act provisions that allow for intervention by the national communications regulator or the national competition regulator to preserve the public interest. The statutory scheme allows the communications regulator to declare an electronic addressing service to be 'a manager of electronic addressing' for the purpose of giving directions to rectify problems concerning competition or consumer protection or unsatisfactory management of the addressing system (Senate 2000: 2).

auDA effectively operates under a self-regulatory model on condition that it continues to satisfy expectations of the Australian Government and ICANN. Debates about governance of the .au domain space reflect both the global nature of the internet and national concerns about managing the .au domain.

auDA commissioned an independent review of .au governance (Westlake Consulting Ltd 2011) at least partly in response to issues raised by the parliamentary report on cybercrime (Standing Committee on Infrastructure & Communications (SCIC) 2010). The Committee recommended that the 'Australian domain registration industry be subject to a code of conduct consistent with' APWG recommendations and that a further inquiry be conducted into the domain name registrations industry (SCIC 2010: xxviii). The Westlake review referred to the growth in the probability and severity of cybercrime and found that the .au domain was well managed and worked particularly well. However, the review made a number of recommendations to maintain broad-based stakeholder support in the areas of accountability and transparency, relationships with the Australian Government, and internal governance. The auDA Board accepted the majority of the Westlake review recommendations (auDA 2012a).

In December 2012 auDA published an *Accountability and Transparency Framework* (auDA 2012c). auDA also published a review of the .au domain name dispute resolution policy in 2014 (Christie 2014).

In relation to security issues, auDA introduced the Information Security Standard (ISS) for all auDA accredited registrars in October 2013 (auDA 2013). Lim and Chen (2015: 1) report that five potential registrars in the process of becoming accredited 'opted to voluntarily terminate their accreditation' and they argue that implementation of the ISS has:

> …increased security mindfulness and built greater capability across all accredited registrars to respond to and remediate potential attacks, reinforcing instilled trust and confidence in the .au [Domain].

In 2014 auDA published the *Interim DNSSEC Policy and Practice Statement (DPS)* for the .au domain (auDA 2014).

Misuse of the Domain Name System

The internet attracts offenders for many different reasons related to a variety of forms of misuse and crime types. Jakobsson (2012: xix; xvii) warned that the internet is at risk of becoming 'useless and dangerous', that criminal misuse of the internet takes many forms 'commonly to make money' and that 'internet crime is both profitable and safe for criminals to engage in.' Jakobsson (2012) summarised the internet's attraction as a platform for criminal misuse as its scalability and speed, the difficulty of both identifying abuse and the difficulty of tracking down offenders. Blocking detected offenders does not prevent them resurfacing in a new guise.

Criminal misuse of the DNS is a subset of more general internet offending and the DNS's attraction for criminals, like that of the internet as a whole, includes the relatively low costs (in time, effort or expense) and risk for offenders, and the prospect of comparatively considerable rewards . Offenders are often driven by similar motives to commit non-internet offences; however, the calculus of risk and reward for online crime is likely to be skewed towards low risk and high reward. Crime attractions can arise from the inherent challenge of hacking the system or from using the online environment as a platform for protest or expression.

Attempts to measure the costs of cybercrime present many methodological problems and draw attention to the lack of data (Center for Strategic and International Studies 2014; Anderson et al. 2012; Anon 2015a). Armin et al. (2015) argued that responding to cybercrime is made more difficult by the lack of consistent definitions and regular data collection. As a result, both the costs of cybercrime and the cost-effectiveness of security responses cannot be clearly assessed.

Despite these measurement difficulties, the reported estimated cost of phishing offences in the United States in 2007 varied from US$320m to US$2b (Moore & Clayton 2007). In Australia, in October 2013, one industry estimate put the cost of cybercrime to be at least $1b over the previous 12 months (Symantec 2013).

Theoretical approaches to misuse

Smith (2010, 2015) examined the applicability of criminological theory to cybercrime and found that routine activity theory and opportunity theory provide useful insights into why this form of crime is attractive. These theories were also shown to provide better insight into the development of cybercrime over time. Beebe and Rao (2005) noted that situational crime prevention strategies are applicable to information system security. Choi (2011) applied similar theoretical constructs to a study of crime prevention strategies for users. For a review of scholarship that relates criminological theory to cybercrime and some of the avenues for further research, see (Holt & Bossler 2014).

Smith (2010, 2015) referred to routine activity theory stemming from the work of Cohen and Felson (1979), who argued that the convergence in space and time of three elements—a motivated offender, a suitable target and the lack of an effective guardian—precipitates predatory physical crime. Smith applied this perspective to cybercrime to determine what conditions precipitate it. As Smith noted, computers and the online environment (and the DNS) can be manipulated to give effect to well-known offline motives such as greed or revenge, as well as new motives like curiosity or status.

Williams (2015) applied routine activity theory to online identity theft (defined as identity fraud committed by duplicating digital information or hijacking online accounts). Williams described three types of security behaviours that represent guardianship for users, which he labelled passive physical, active personal and avoidance personal. Passive physical measures address hardware and software security and include using a single computer with inbuilt security and antivirus protection. Active personal measures include user vigilance and secure online behaviours such as the use of strong passwords. Avoidance personal means users do not engage in online transactions. These divisions help to illustrate for users the range of individual protective behaviours possible. Williams compared Eurobarometer data on online identity theft for 27 European countries and found that two routine activities, public internet access and online auction selling, presented a high risk of identity theft.

Wall (2005: 2–3) described the dual nature of six transformative impacts of internet technology on deviant behaviour:

- the globalisation of opportunity and 'glocalisation' of law enforcement jurisdiction;
- distributed networks and grid technologies that enhance opportunities to commit offences while increasing the complexity of regulation;
- the capacity of offenders to target victims from a distance, and the possibility of detecting offending activity from patterns of behaviour;
- the multiplication of asymmetric relationships, such as small impact victimisations, on a large scale
- data trails and the potential to obscure data relevant to cyber offending; and
- changes in the organisation of criminal activity (exemplified in the segmentation and distribution of tools and skills that allow individual offenders to act with the sophistication of a group.

The internet attracts criminals because it underpins so many aspects of life including banking, finance, data storage and communication, thus offering valuable targets (De Vey Mestdagh & Rijgersberg 2007). Those motivated to offend can access these services, or the people using them, through the internet. This offending may successfully exploit large targets or aggregate the proceeds from many smaller targets.

Finally, both the scope of cybercrime and the capacity to police it are limited. Exploitation of the DNS is poorly addressed in criminal law and other areas of legislation and regulation. Where criminal provisions apply, offenders may reduce the risk of offending by using various measures to evade detection or identification. Where DNS exploitation lies beyond the reach of criminal law enforcement, or other forms of law and regulation, the capacity to respond depends on the international framework that regulates the DNS. In this context, the relevant aspects are a general lack of regulatory capacity, low requirements for user identification, and software and social engineering measures that make it possible to 'hide' online.

The internet, IP addressing and the DNS have been developed according to principles of openness and interoperability, and in circumstances that favour utility over security. The internet's early development can be modelled as a response to the discovery of emerging vulnerabilities: security patches are devised and implemented after a security weakness is detected or exploited. The most dangerous security flaw would be a zero-day vulnerability exploiting a previously unidentified security gap for which there is no ready fix. This would result in an extended latency period between discovery and remediation, thus offering greater opportunity to cause harm (Albon et al. 2014). Similarly, software in the application layer of the internet can develop in the same way—with a cycle of fixes applied to emerging vulnerabilities. Smith (2010: 214) also showed how crime develops and changes in response to technological change. The development of cybercrime activity follows the stages identified by Felson et al. (1998) for criminal conduct related to mass-produced consumer goods. These stages are

- innovation;
- growth;
- mass market; and
- saturation.

As Smith (2010: 246) argued, the insights gained from applying criminological theory to misuse of the internet can be used to help develop crime prevention strategies 'that seek to modify the online environment to make the commission of crime less attractive to potential offenders.'

Prior research into DNS misuse

Cheung (2006) examined the vulnerability of the DNS to various forms of denial of service (DoS) attacks. Cheung presented an attack tree describing three main forms of attack. These were:

- attacking resolver hosts, including exploiting resolver vulnerabilities, corrupting resolver configuration and attacking resolver hosts;
- disrupting communications, including by packet flooding and attacks on routers or firewalls; and
- attacking name servers by injecting incorrect DNS data, mounting DoS attacks on name servers and damaging name servers.

At the time, best-practice countermeasures included using multiple name servers; deploying Anycast routing; overprovisioning capacity; implementing various DNS software to avoid exposure to single vulnerabilities; using the Transaction Signature (TSIG) scheme; and dedicating separate machines to name resolving functions. Cheung also described the development of new countermeasures such as the now widely used DNS security extension, DNSSEC, and the possibility of peer-to-peer DNS. The drive to develop peer-to-peer-based DNS alternatives is sometimes characterised as a response to actual or perceived threats that certain sites will be shut down, or that user privacy may be compromised (Storm 2010).

In 2010, the Commonwealth House of Representatives Standing Committee on Communications reported on its inquiry into cybercrime (Standing Committee on Communications 2010). The Committee made recommendations relating to the need for data collection, domestic and international coordination, cybercrime reporting and other law enforcement coordination efforts. The Committee did not undertake a detailed inquiry into domain name registration in Australia and suggested a parliamentary inquiry be conducted on this. However, the Committee did recommend that the Australian domain name registration industry be made subject to a code of conduct consistent with the *Best Practices Recommendations for Registrars* of the Anti-Phishing Working Group (APWG; Alperovitch & MacFarlane 2008. The recommendations cover collecting and retaining data relating to domain name registration, employing processes to identify fraudulent activity in domain registrations and developing clear guidelines for the rapid takedown of malicious sites.

In 2013, the Congressional Research Service reported on internet governance and the DNS (Kruger 2013). This report detailed the most important areas for debate about multi-stakeholder model of internet governance. In particular, the report addressed the contentious issue of whether the United States should continue to relinquish authority for IANA functions to ICANN. The Research Service noted that Congress had to weigh the consequences of attempting to control aspects of the internet and domain governance through domestic legislative action against maintaining the multi-stakeholder model's long-term viability.

The risk of undermining the current arrangements for network governance are detailed by Hill (2012), who reported six concerns that could lead to the fragmentation of the internet. The first of these is the possibility of countries creating national root servers and 'seceding' from the internet.

Conventional legal framework

Before discussing the relationship between DNS misuse and cybercrime, it is important to note that domain names may also be subject to conventional (non-cyber) crime. Examples include fraud or theft of domain names, or sabotaging the hardware of a computer.

Hardware

On the official Microsoft blog (http://blogs.microsoft.com/blog/2012/09/13/microsoft-disrupts-the-emerging-nitol-botnet-being-spread-through-an-unsecure-supply-chain/#sm.0000fl3y86ulde2hzps1ednvhpohx), (Meisner (2012) described how the Microsoft Digital Crimes Unit detected malware preloaded on new computers sold in China. The problem involved supply-chain interference that may have occurred at any point between manufacture and delivery to the purchaser. During Operation b70, Microsoft detected pre-installation of software that propagated the Nitol botnet, which Microsoft says was 'operating on a domain linked to malicious activity since 2008.' The domain was 3322.org, a site alleged to hold '500 different strains of malware hosted on more than 70,000 subdomains.' The malware was capable of

> …remotely turning on an infected computer's microphone and video camera, potentially giving a cybercriminal eyes and ears into a victim's home or business. Additionally, we found malware that records a person's every keystroke, allowing cybercriminals to steal a victim's personal information. (Meisner 2012: np)

Microsoft took action in a United States court to take over the domain and shut down the malicious components (Meisner 2012).

Domain name theft

Whether or not a domain name can be 'stolen' according to criminal law depends on the circumstances of each case, and there may be competing principles to consider. These include that:

- domain names are subject to a non-criminal law regime for initial allocation and resolving disputes about allocations;
- domain names may also be considered immaterial, and not things that can be stolen; and
- stealing a domain name is an action beyond the cybercrime framework unless it involves criminal manipulation of a network or computer.

A domain name may be stolen where title to the domain name is acquired through fraud or criminal data manipulation. If data manipulation is involved, that may be separately prosecuted as a cybercrime offence; but the completed act of stealing the domain name may be prosecuted under the general criminal law.

In March 2015, cases of domain stealing were reported in the United States (Simon 2015). The cases involving targeted phishing to gain access to the computer system of a domain owner, followed by manipulating the target computer to transfer the ownership of the domain to an account owned by the scammer. The scammer may be motivated 'to hold the domain name for ransom, resell it, or use the information to access data.' A stolen domain name might also be used to 'display pay-per-view advertisements, display a website that downloads malware, or… to send legitimate looking emails containing spam, viruses or phishing' lures.

Box 2 presents a US criminal case that involved the theft of a domain name. The offender hacked into the registration account of a domain name and transferred ownership to himself, subsequently selling the domain name for a considerable amount of money.

Box 2: Stealing P2P.com

In New Jersey in 2010, Daniel Goncalves was convicted of 'theft by unlawful taking, theft by deception, and computer theft.' Goncalves pleaded guilty to the charges involving stealing the domain name P2P.com. He 'illegally accessed the GoDaddy account belonging to P2P.com and initiated a transfer of the domain name to his personal GoDaddy account.' Goncalves had then sold the domain name on eBay for US$110,000. Goncalves was convicted and sentenced to five years in state prison.

Source: Dow 2010

Where a domain name is fraudulently taken, damage may accumulate while the domain owner seeks to recover control of the name through formal processes. It is unlikely an offender would be identified or could realistically be sued for any damage caused.

The legal cybercrime framework

The Council of Europe's *Convention on Cybercrime* forms an international regulatory framework for the creation of offences against 'computer data and systems' and for computer-related offences (Council of Europe 2016). It sets out requirements for gathering and sharing electronic evidence of cybercrimes (and other crimes) where a computer was used to facilitate offending. Under this framework cybercrime can be divided into three categories: crimes against computers (target); crimes using computers (tool); and crimes involving incidental computer use (incidental; see, for example Clough 2010 and Rasmussen & Vixie 2015).

Wall (2007) focused on crimes committed substantially online, and refers to target offences like computer integrity crime and tool offences as computer-assisted crime. He effectively sets aside the category of incidental cybercrime offences as too broad, and separates computer content crime—including online child exploitation material and intellectual property offences—from other computer-assisted crime.

Gordon and Ford (2006:1–2) defined cybercrime by first distinguishing between the terms

cybercrime and crimeware. Their definition of crimeware includes 'trojans, viruses, bots, spyware and worms which are instrumental in facilitating certain cybercrimes'. The authors argued that the term cybercrime unrealistically indicates a distinct sphere of criminal behaviour, whereas cyber activity is part of the repertoire of means to commit or facilitate the commission of criminal acts. They proposed a two-part definition, with type I offences consisting of discrete crimeware victimisations, often based on the exploitation of software vulnerabilities. Type II offences are based on interaction with a victim and characterised by the use of software other than crimeware, usually involving repeated contact. Others have emphasised that cybercrime laws have jurisdictional limits that constrain the investigation or prosecution of offences, as the offender and victim could be physically located anywhere or highly mobile (Speer 2000).

An example of a cybercrime target provision from the Commonwealth *Criminal Code Act 1995* is shown in Box 3 below. The matters set out in paragraph 477.2 (1) (d) establish a basis for the exercise of Commonwealth jurisdiction, including under the telecommunications power in the Constitution or Commonwealth ownership of a computer or data. The physical elements of the offence are that a person causes data held on a computer to be modified without authorisation. The fault elements lie in the person knowing that the modification is unauthorised and is reckless to whether the modification impairs (or will impair) access to, or the reliability, security or operation of, any such data.

Box 3: Section 477.2 of the *Criminal Code Act* 1995 (Cth)

477.2 Unauthorised modification of data to cause impairment

(1) A person is guilty of an offence if:

(a) the person causes any unauthorised modification of data held in a computer; and

(b) the person knows the modification is unauthorised; and

(c) the person is reckless as to whether the modification impairs or will impair:

(i) access to that or any other data held in any computer; or

(ii) the reliability, security or operation, of any such data; and

Penalty: 10 years imprisonment.

The definition of cybercrime encompasses crimes against the confidentiality, integrity and availability of computer systems. Importantly, the provision is framed around 'a computer' and 'data held', and the impairment issue is tied to 'any computer' or 'any such data.' There is no reference to the DNS, a network or networks, and no specific offences based on DNS misuse were identified. Despite this, the cybercrime provisions are sufficiently broad to capture most offending directed at, or based on, abuse of the DNS.

Obviously most internet offending involves some form of DNS misuse, but not all examples of misuse of the DNS would be considered criminal. The absence of specific DNS offences may be explained by the following factors:

- the general description of crimes against computer systems is thought to provide adequate protection for the DNS;
- the DNS lies beyond the regulatory sphere of nation states either in fact, in law or in principle;
- DNS governance has been so contentious that it is too hard to define offences specific to it;
- it is tacitly accepted that the DNS is a matter for multi-stakeholder governance; and
- questions of DNS misuse are seen as best dealt with as civil cases, applying normative principles derived from the rules and structure of the DNS.

Nations do not control the internet and national cybercrime laws are subject to territorial limits, with the effect that some internet activity is beyond the reach of national cybercrime provisions (Brenner 2007). Despite this, there has been a high degree of international police and law enforcement agency cooperation in coordinating responses to cyber threats.

A tentative model of criminal DNS misuse

Figure 3 presents a tentative model for considering criminal misuse of the DNS with typical cybercrime offences . DNS misuse may involve manipulating machines (software engineering) or people (social engineering). The twin purposes of the DNS create a simple framework for examining criminal misuse, depending on whether it exploits the attributes that support engineering purposes or those that support human interaction.

However, misuse cannot always be divided neatly into the categories of software or social engineering, and some forms of misuse combine both. The model incorporates the concept of using the DNS as a virtual platform for criminal activity or a place in which to commit offences.

Figure 3: A tentative model for considering criminal misuse of the DNS

Type of cybercrime using Convention on Cybercrime types	Primary mechanism	Offence	Principal attribute of DNS relied on			
			DNS architecture	Domain name	Domain as virtual space	Application in a layer removed from the DNS
Target	Software engineering	Illegal access				
		Illegal interception				
		Data interference	☑	☑		☑
		System interference				
		Misuse of devices				
		Attacks on the DNS itself	☑			
Tool	Social engineering	Computer-related forgery				
		Computer-related fraud				
		Offences related to child pornography	☑	☑	☑	☑
		Offences related to infringements of copyright and related rights				
Incidental	Platform for misuse				☑	☑

This model is used in the following discussion of the various types of cybercrime-related misuse of the DNS.

Software engineering misuse

In addition to the landscape the DNS adds to the internet, every internet activity involves one or more layers of the software architecture that supports the internet as a whole. There is an added dimension to consider in locating criminal activity on the internet: identifying the engineering layers of the internet that support, or are exploited by, misuse helps to identify more precisely the pinch points for regulation and regulatory weaknesses. Software engineering misuse can arise in two contexts: that in which the DNS is a target for misuse and that where the DNS is a vector for misuse.

The DNS as a target for misuse

Network architecture

Rasmussen and Vixie (2015) described the threat posed to the DNS by attacks on DNS record publishing. This occurs where DNS registry information is altered by hacking into the accounts of domain owners, or of domain registrars or registries. Attacks on registrars may compromise the records of domain owners. The compromised data could include passwords that enable the hacking of owner accounts. Certificate signing authorities may also be hacked, which could give the hacker access to secure networks. For this reason, one organisation's security may depend on that of its partner or service organisations.

Alternative root systems

Mueller (2002) identifies alternative root systems such as Pacific Root, ORSC, New.net, Name.space and CN-NIC. Some current examples include Open NIC; dotpirate.org; Namecoin; .bit,OpenDNS; and the Open Root Server Network. Marks (2010) reported Peter Sunde's announcement of a plan to establish an unregulated alternative internet registry. Sunde was convicted and sentenced to imprisonment in Sweden in a prosecution related to the Pirate Bay site.

In 1997, Eugene Kashpureff hijacked the InterNIC website as part of a personal protest against the monopoly of Network Solutions (NSI) over the root registry. Kashpureff and others established AlterNIC in 1995 as an alternative root server (Cuff 1997). The hijack involved DNS poisoning and diverted users attempting to connect to internic.net to alternic.net. On alternic.net, users could click through to internic.net or read a protest message created by Kashpureff (Kornblum 1997).

In a press report at the time, Cuff (1997) downplayed the harm caused by the redirect while acknowledging the enormous commercial and political significance of both this demonstrated vulnerability and the ongoing debate over internet governance. Cuff argued that the symbolic importance of the Kashpureff hack on the root servers greatly exceeded the actual damage done.

Root zone attack

Some cyber attacks have focused on the root zone. Relatively recently, in 2012, the online activist group known as Anonymous threatened the root zone—as described by Gallagher (2012). The proposed attack—which did not eventuate—was alleged to be based on a DDOS attack on the root servers. However, as Gallagher points out, there are not literally only thirteen root servers, but many more that replicate the root server and the prospect of a successful DDOS attack on the root servers in the manner threatened was unlikely.

In 2007, a root zone attack that did affect internet operations took place. and was reported by ICANN (2007) and Kristoff (2007). On 6 February 2007, the internet's core DNS servers were subject to a serious distributed denial of service attack (DDoS). The attack consisted of two denial of service bursts of about two and a half hours and five hours, with a break of three and a half hours between bursts.

ICANN (2007: 2) described how 'billions of worthless data packets are sent from thousands of different points on the internet to specific computer servers in order to overwhelm them with requests and so disrupt the smooth running of the internet' (2007:1). ICANN revealed that six root servers were attacked and 'two of them were noticeably affected: the "g-root", which is run by the U.S. Department of Defense, and the "l-root" run by ICANN and physically based in California. These two were particularly badly affected as they had not installed Anycast (three root servers without Anycast were not attacked this time).' BGP Anycast is a Border Gateway Protocol (BGP) which allows 'the same address space (to be) used and announced in the normal way but from multiple locations on the Internet. Within the BGP routing system, multiple routes to the same address space will be seen, and the shortest route is given preference in the normal way' (APNIC 2015b).

Routing via the border gateway protocol (BGP)

Anycast software added to the resilience of the root servers targeted in the 2007 attack. However, the Internet Society (2014b: np) noted the potential for error or misuse given that BGP 'does not directly include security mechanisms, relying on trust between network operators that they will secure their systems correctly and not send incorrect data.' The Society noted that 'mistakes happen, and problems could arise if malicious attackers were to try to affect the routing tables used by BGP.'

One example of BGP misuse is a Bitcoin-stealing offence committed using the compromised administrator account of a Canadian ISP. According to Litke & Stewart (2014: np),, an attacker used the administrator account to 'inject BGP routes that redirected traffic from machines mining Bitcoins to the attacker's compromised host.'An estimated $83,000 worth of Bitcoins, Dogecoins, HoboNickels, and Worldcoins were stolen over a period of four months. The Internet Society (2014a: np) said 'there are two obvious technologies that would have prevented this attack. The first…is Border Gateway Protocol (BGP) security. Something like BGP Resource Public Key Infrastructure (RPKI) would have prevented the receiving BGP peer from accepting bogus routes. The second is Transfer Layer Security (TLS) connections between the hosts controlling the coin miners, and the miners themselves'.

The application of BGP is a separate technical issue not because the BGP itself is limited but because the older servers that support it have limited capacity. Brooks-Pollock (2014) reported disruption to eBay and other services in August 2014. Anthony (2014) explained how these problems related to the limited processing capacity of older servers on the network which had been configured to accept just over 500,000 entries in Tertiary Content Addressable Memory (TCAM). The number was 2^{19} or 524,288 entries. Anthony reported that once the number of routes on the Internet exceeded this number some routers crashed, and some ignored new routes, creating instability.

Huston (2014) considered the limitations of BGP and addressed some questions concerning how they might affect the operational capacity of the DNS.

- If facing a major problem with routing scalability, should alternative architectural models of identity and location separation be examined, to build truly massive and highly diverse networks; or

- is the scaling of routing an intractable problem within the confines of the current architecture, and do we need to alter the internet's architecture to a different routing architecture with radically different scaling properties?

Huston concluded that there was no need to change the basic routing architecture if the internet. For IPv4 addresses, the increased density of connections will overcome the number of possible connections:

> The density of inter-AS interconnection continues to increase. The growth of the Internet is not 'growth at the edge' as the network is not getting any larger in terms of average AS path change. Instead, the growth is happening by increasing the density of the network by attaching new networks into the existing transit structure and peering at established exchange points. This makes for a network whose diameter, measured in AS hops, is essentially static, yet whose density, measured in terms of prefix count, AS interconnectivity and AS Path diversity, continues to increase (2014: 5).

According to Huston, the expected number of IPv6 addresses is much lower, and the number of routing entries will be much less than that required for existing IPv4 addresses.

What is most interesting in terms of how the internet may be used or misused is the observation by Huston that BGP does not create a single authoritative view of the routing table (a data table that routes to particular destinations). As a consequence, routers can be set up to share routing information in different ways. Huston noted that changes in routing might flow from 'transit arrangements within the interior of the network that may expose, or hide, collections of routes.' (Huston 2014: 4) The result is that routes that are made visible or shared can be limited in one-sided arrangements, where a router uses routes made visible by other routers but limits those it shares in return. Huston suggests that this may be considered a form of 'misuse' of the DNS, which he likens to the notion of the 'tragedy of the commons' (Huston 2014: 4). :

> In the absence of enlightened self-interest, some form of authority or federation is needed to solve the collective action problem. This appears to be the case in the BGP realm, where there is an extensive reliance on enlightened self-interest to be conservative in one's own announcements, and the actions by a smaller set of actors are prominent because they fall well outside of the conventional "norm" of inter-domain routing practices (2014: 4).

DNS hijacking

Malicious phishing and DNS hijacking activities are often committed for financial gain. One example reported in 2011 involved offenders hijacking ChronoPay.com, Russia's largest payment processor, and one of the largest payment processors in Europe, for several hours on December 25 and 26 via DNS hijacking (Anonymous 2011).

Cache poisoning

Karrenberg (2010: 5) described cache poisoning attacks (or 'spoofing') as 'particularly dangerous.' Infection with malicious code can affect all future requests by an infected computer, which will keep redirecting itself to an incorrect IP address. He highlighted the combined threat of manipulating network and user trust:

> Cache poisoning is especially dangerous when hackers target well-known and trusted websites, where users may be inclined to enter personal details and passwords. Last year, for example, a prominent Brazilian bank suffered a cache poisoning attack that redirected customers visiting its website to fraudulent portals that attempted to steal passwords and install malware. Alarmingly, attacks of this type are becoming increasingly common (Karrenberg 2010: 5).

The DNS as a vector for misuse

Misuse of the DNS may enable a cybercrime or other crime but not be an offence itself. It is, therefore, important to consider the role of the DNS as a threat vector—for example, through phishing. Rasmussen and Vixie (2015) described how the DNS has become a threat vector for internet crime, and identified DNS-based threats including in-transit attacks, attacks using domain generation algorithms, DNS tunnelling and reflective DNS amplification DDoS attacks.

Misuse of the DNS can be categorised as threats that lead directly to an intended harm and threats that represent steps towards causing an intended harm. The example given by Rasmussen and Vixie (2015) of an in-transit attack can be considered a form of single-step misuse because the attack on data during transit is completed directly. The examples of domain generation algorithms and DNS tunnelling can be characterised as multi-step misuse although these techniques are not by definition criminal as they may also have legitimate purposes. Reflective DNS amplification DDoS attacks are categorised here as multi-step misuse because they enlist authoritative and recursive name servers to answer DNS queries, usually generated by botnets, where the query is spoofed so that it appears to be coming from the server or site of the attack's target. The targeted site or server is thus overloaded and will crash, as a result of being bombarded with answers to the false DNS query that apparently came from the target.

Cross-site scripting (single-step misuse)

Saharan (2007: 2) gives a 2006 example of cross-site scripting involving the social network site Orkut, reported by Rajesh Sethumadhavan. A vulnerability in the site allowed 'members to inject HTML and JavaScript into their profile. In November 2006, Rodrigo Lacerda used this vulnerability to create a cookie stealing script known as the "Orkut Cookie Exploit" which was injected into the site's profiles of the attacking member(s). By merely viewing these profiles, unsuspecting targets had the communities they owned transferred to a fake account of the attacker.' The operators of Orkut fixed the vulnerability in December 2006.

Hacking (single-step misuse)

The websites of corporations remain particularly vulnerable to hacker attacks (Yu 2013). Hacking has the potential to cause enormous damage and hacks are instituted for a variety of malicious purposes. Some hacks are committed with less obvious malicious intent, or with the intention not to cause harm but to help improve overall internet security by detecting and proving security defects. Haggard and Lindsay (2015) detailed the Sony hack, a significant hacking incident in late 2014 that Fortune Magazine described as the 'Hack of the Century' (Elkind 2015: np). Domain names are usually prefaced by an indication that hypertext transfer protocol (HTTP) is being used; this is written as http (or https for secure connections); sometimes it is written as www. Most browsers default to read an entry as an http-based connection, although the user may insert other prefixes to access other resources. For example, a user may type 'email', plus a relevant identifier, to go directly to an email server. Internet resource addresses can be manipulated to create a hack that gets around access restrictions, such as for a wi-fi service behind a paywall. Geisendorfer (2006) describes this hack, which involves inserting a domain name preface that suggests access has already been obtained.

Botnets (multi-step misuse)

Botnets are networks of computers that have been compromised by malicious software that allows someone to take command of infected machines and direct their tasks, often without the knowledge of the owner of the compromised computer (Cheung 2006). Khattak et al. (2014) examined how botnets were organised and argued that responses must be tailored to the specific nature of each threat. Macnair (2008) described the increasing ease of exploiting botnet technology, attributing a spike in 2007 in 'pump and dump' spam to the increased use of botnets. Botnet-generated spam has been blamed for SQL injection attacks on websites that cause legitimate web pages to be swapped for malicious sites.

Messmer (2009: np) considered the problem of domains being farmed out for 'botnet-controlled SQL injection attacks against websites in India, United States and China.' Turning from the particular instance in which GoDaddy domains were used, Messmer (2009: np) argued that the underlying issues to be addressed 'encompass the entire domain name registration system' and the 'faulty Whois database of registrant information'. She makes the point that much online criminal activity itself depends on the stability of the DNS. For example,

bots need to be able to map dynamically to a particular IP address while the botnet controller seeks to evade being blocked or taken down. Messmer quotes Dean Turner, director of Symantec's global intelligence network, as saying 'criminals today can be seen making clever use of what's known as fast-flux to rotate a botnet through thousands of IP addresses using a single domain or group of domains to defeat IPblacklists' (Messmer 2009: np).

Lawton (2007) argued that spam is dangerous because it can be used to transmit malicious code that takes over target computers to form 'botnets of zombie machines' to deploy DDoS attacks. Lawton pointed to factors that can minimise adverse impacts, including 'DNS security measures and quick, coordinated responses by Internet engineers, including the filtering of hackers' messages' (Lawton 2007: 14).

Denial of service attacks (multi-step misuse)

A denial of service (DoS) attack involves using DNS architecture to overload a site or server by inundating it with dummy requests—whether to resolve a routing request or to respond to a supposed user request. DoS attacks and Dedicated Denial of Service (DDOS) attacks require many requests to be made at once for a sustained period. The actual period of overloading may not last long, depending on whether the source of the dummy requests can be identified and blocked. DoS attacks are increasingly committed using botnets.

DoS attacks may be motivated by revenge, to extort, or to embarrass, harass or ridicule. DoS attacks are unlikely to bring the internet to a halt because they can often be circumvented, even if after some time. The possibility of illegally making money from a DOS attack is related to the prospect of the attack lasting for a limited period. As a result, extortion attempts may focus on time-sensitive applications such as internet gambling sites, or be timed to coincide with key announcements or to inflict maximum damage to reputation.

In some instances, DoS-like conditions occur when many legitimate users seek to use a service at the same time, such as during a well-publicised online sale or an important sporting event.

Spam (multi-step misuse)

In Australia, spam is a matter for civil regulation. Despite continued efforts by spammers, the amount of spam that reaches users is limited. Macnair (2008) reported a transition away from pharmaceutical promotions to the sale of counterfeit products. Rafiee et al. (2012) acknowledged that spam has been a serious problem for a long time, noting that 'automated strategies are required' (2012: 1) to deal with spam traffic, and warning that:

> …while IPv4 networks offer a variety of solutions to reduce spam, IPv6 networks' large address space and use of temporary addresses—both of which are particularly vulnerable to spam attacks—makes dealing with spam and the use of automated approaches much more difficult. IPv6 thus poses a unique challenge (Rafiee et al. 2012: 1).

Social engineering misuse

Krombholz et al. (2014) pointed to the enormous growth in opportunities to exploit increasing levels of connectivity across multiple platforms where private life, work and other domains are increasingly blended. The authors provided a taxonomy of social engineering and described a range of threats involving what they labelled physical, technical, social and technical–social methods.

In this section, two forms of social engineering are considered. Both aim to defraud users or have users take actions with unintended consequences, or that otherwise compromise the security of their computer. The first is appearance-based and uses domain names registered through the DNS or otherwise use the DNS to manipulate the presentation of Internet resources for malicious purposes. An example is provided in Box 4 below.

Box 4: Social engineering case study

In 2013 Whitehaven Coal Limited (Whitehaven) was preparing to construct a coalmine at Maules Creek in New South Wales. The project relied on funding from the ANZ Banking Group Limited (ANZ). Jonathan Moylan opposed the mine construction and sent an email purporting to be from the ANZ to a number of media outlets, to the effect that a $1.2b loan facility for the project had been withdrawn.

Moylan sent the email from the email account named media@anzcorporate.com. He had purchased the domain name anzcorporate.com for $27. The email included a false name but Moylan's own phone number. When contacted by someone seeking verification, Moylan admitted the email was false.

Reports of the email negatively affected Whitehaven's share price until share trading was blocked at Whitehaven's request. The email was sent at 11.44 am on 7 January, and trading was halted at 12.41 pm. The volume of shares traded increased significantly from around 12.18 pm, following unverified reports of the supposed ANZ decision. Whitehaven's share price dropped, with a potential loss on all stock of $316m. The potential maximum loss from actual trades after 12.18 pm, using the lowest price for all shares traded at the time, was more than $878,000. However, apart from transaction costs, only those who sold their shares and did not repurchase at the lower price before the trading halt experienced an actual loss in share value.

Moylan was prosecuted under section 104E(1) of the *Corporations Act 2001* (NSW) which prohibits knowingly distributing 'false information likely to induce persons in Australia to dispose of financial products.' Moylan was convicted and sentenced to one year and eight months imprisonment, suspended on entering into a recognisance to be of good behaviour for two years.

Source: R v Moylan [2014] NSWSC 944

The second form of social engineering is interest-based, and is not dependent on a particular name or the manipulation of the DNS; it directly engages user interest in a way that is designed to trick other users.

Phishing

Phishing is very closely related to DNS abuse. Since 2008, the Anti-Phishing Working Group (APWG) has published a biannual global phishing survey (APWG 2015).

The APWG identifies three categories of phishing attack sources:

- maliciously registered domains;
- hacked domains; and
- the abuse of subdomain services, virtual hosts, or URL changers.

They report the prevalence of phishing by top-level domain (TLD) and show the incidence of phishing domains and phishing attacks as a ratio of the total number of registered domain names in a TLD per 10,000.

Toward the end of 2009, phishing attacks began to be primarily sent from hacked domains rather than from maliciously registered domains. Hacked domains continue to be the primary source of attacks.

The hacking of shared virtual servers is a high-yield activity for phishers. It involves breaking into a web server that hosts many domains, which allows the phisher to update the web server configuration or use automation tools to add phishing content to each domain hosted on the virtual server.

Another area of concern is the use of subdomain services for phishing. The APWG (2015) defines subdomain registration services as 'providers that give customers subdomain hosting accounts beneath the domain name that the provider owns' (APWG 2015: np).' These subdomain services are challenging 'because many of the services are free, offer anonymous registration, and only the subdomain providers themselves can effectively mitigate these phish.' The APWG noted the launch, in January 2014, of the first of some 1,200 new TLDs. They cautioned that the malicious use of new TLDs will require ongoing monitoring.

The APWG reports confirm, in line with findings made consistently since 2008, that phishers and spammers do not often register domain names referencing brand names. This is because using a brand name can indicate the domain is malicious; and phishing can be effective without using a brand name in the domain name. While the domain names used by phishers do not generally feature brand names, the APWG reports the use of URL shorteners to obfuscate phishing URLs.

The APWG survey reports indicate threats to major targets including the banking sector, e-commerce sites, money transfer sites, social networking sites and email. The APWG measures the damage caused by a particular phishing attack and the success of anti-phishing mitigation efforts by the time the attack remains live. The APWG reports highlight the role of registrars in malicious phishing. The report for the first half of 2014 included new data from China; nine of the top 10 registrars, by malicious domain name score, were located there. Ke et al. (2015) analysed the elements of a sophisticated social engineering attack that specifically

targeted Australian users.

Online pharmacies

Online pharmacy scams involving fraud or the supply of prescription drugs without authority are commonplace. The demand for drugs like Viagra has been exploited by malicious operators to entice users to respond to phishing emails and interact with online pharmacies.

Mackey and Liang (2013) studied the operation of online pharmacies using social media platforms such as Facebook, Google+, Twitter and MySpace. They were able to create illicit direct-to-consumer advertisements on each platform. The advertisements referred users to dummy websites that gave an error message if a user attempted to access them. They found this could be done using 'commercially available internet tools and services, including website hosting, domain registration, and website analytic services' Mackey and Liang (2013: 45). Once the advertisements were posted they were not taken down Mackey and Liang (2013) claimed that these 'fictitious advertisements promoting illicit sale of drugs generated aggregate[d] unique user traffic of 2,795 visits over a 10-month period' (2013: 45). Their conclusion was that there were few barriers to creating these advertisements, and the advertisements created a global market for the advertised product. The authors concluded that cybercrime strategies must focus on the threat online pharmacies pose to effective global e-health governance.

Tech support scams

Tech support scams are one apparently effective variant of social engineering that combine code manipulation with personal interaction by phone. The offender calls people and identifies themselves as a representative of a reputable computer company, ISP, or other technology and technology service providers. They offer to help the user remove or otherwise deal with a malicious virus or similar that has been remotely detected on the user's computer.

In 2012, the US Federal Trade Commission took action to shut down six telemarketing scams where users were called, by someone pretending to be from a company such as Microsoft, and told that their computer was infected with malware. The users were charged hundreds of dollars by the scammer to have the 'problem' fixed remotely. The scams originated in India, and targeted users in Australia and elsewhere (Anon 2013: 12). The latest survey of consumer fraud victimisation by the Australian Institute of Criminology found that 65 percent of the fraudulent invitations received by those who responded to the 2014 survey related to computer support scams. They were the second-most common type of scam and resulted in the loss of personal information or money for 0.5 percent of those who received an invitation (Jorna 2016).

The DNS as a platform for misuse

Many aspects of the internet can be used in the commission of cybercrime offences. This section outlines some of the ways offenders use the DNS as a platform for offending. Lavorgna (2015) documents how criminals use the internet to support their criminal activity. It is difficult,

however, to collect data on this and keep up with the pace of change in this area.

A platform can include those parts of the DNS that can be manipulated by software and social engineering, from which malicious activity is launched, hosted and controlled. These sites may be used exclusively for malicious activity, or they may have shared functions relating to legitimate activity. They may be exclusively owned by offenders or jointly owned with legitimate users; or sites owned by legitimate users may be maliciously hijacked. Each of these possibilities presents distinct challenges in responding appropriately when malicious activity is detected from a particular site on a site-hosting service.

The concept of platform also includes the use of domains for any action that supports criminal behaviour before, during or after a cybercrime is committed. Possible preparatory site uses include discussing or exchanging the tools and techniques required to support malicious activity. Individual criminals or criminal organisations may operate sites that appear legitimate or that arenot directly associated with the commission of cybercrime offences but that enable communication about, control of and support for cybercrime.

One downstream use that acts as a first step in monetising cybercrime is the creation of a marketplace for compromised data or hacks; another is the creation and exchange of systems for payment and the transfer of values that are difficult for law enforcement agencies to trace. It should be noted, however, that such sites are more likely to be located on the darknet.

Geolocation misuse

At least four potential actors are involved when a user accesses the internet. These are:

- the user;
- the ISP;
- the telecommunications carrier; and
- the internet router or host that establishes a connection.

Connection implies interaction with some other part of the internet. The potential fifth actor is the host of any particular part of the internet accessed by the user.

To connect to the internet, an ordinary user requires both an ISP and access to a telecommunications platform. The IP addresses of ordinary users are likely to be dynamically assigned for a particular internet connection session by an ISP from the suite of addresses allocated to it. Dynamic assignment is seamless and no direct user input is required.

Users do not need their own domain name to access the internet, but most users gain access through a dedicated server or a service provider. A user accesses the internet via an IP address allocated to the server or service provider's domain. This locates the user in the domain through which they entered. However, this does not anonymise a dynamic IP address session. The ISP may link the dynamically allocated IP address to the particular account used to connect through it at a particular time. In addition, when a device is connected it may directly transmit identifying information; or the programs or applications used may transmit identifying

information either automatically or through direct user input.

The APNIC homepage (www.apnic.net) displays the IP address of the device used to access the internet at the top right of the screen. The address contains hypertext that links to the APNIC Whois Service showing the entry associated with the given IP address at that time.

The ability to match an IP address to a domain has given rise to a variety of legal issues across a range of interests. There are numerous examples where providers of digital media wish to limit the availability of that media to users from a particular geographic location or to specifically exclude users from another. The antecedents for territorial restrictions on copyrighted material lie in pre-internet models for dividing the world into distinct markets for the licencing of intellectual property. For example, Clark and Phillips (2008: 124-5) described how the global market for English language books was divided between US and UK publishers and how this came to be undone. The history of territorial control of the book trade was recounted by the Copyright Law Review Committee (1988) in its report at *Appendix D*.

Geoblocking international coverage

Olympic coverage (or coverage of any other major international sporting event) is an example of a situation where a content owner wishes to control access to digital material on a geographical basis, thus making it available only to users accessing the web via the domain of one country and blocking users from other national domains. Limiting access to content by geographic location is known as geoblocking.

During the London Olympics, the BBC streamed extensive live and recorded coverage of events over the web; this was available only to users with a UK IP address. In this case, geoblocking was intended to protect nationally segmented worldwide licencing rights for Olympic coverage.

The sale of licensing rights to Olympic coverage, and to coverage of other international sporting events, is worth a considerable amount of money. The IOC (2013) revealed that the broadcast revenue for the London Summer Olympics was worth US$2.569b.

Other geoblocking issues

A government may wish to selectively geoblock material to restrict the flow of information to or from a particular domain. An issue of this nature arose in connection with the sanctions imposed by the United States on the Islamic Republic of Iran (Box 5).

Box 5: United States sanctions against the Islamic Republic of Iran

The United States has in the past imposed trade sanctions on various countries.

To foster private access to the internet for Iranians, the US Office of Foreign Assets Control clarified the trade sanctions applicable to the Islamic Republic of Iran:

Consistent with United States current foreign policy to enable private persons in Iran to better and more securely access the Internet, OFAC is clarifying its existing Statement of Licensing Policy (SLP) that establishes a favourable licensing policy through which U.S. persons can request OFAC approval to export to Iran services and software not covered by section 560.540 of the ITR that directly benefit the Iranian people.

Source: Office of Foreign Assets Control (2012: 2)

An internet user's geographical location may trigger closer monitoring of the traffic they generate, or it may influence how much attention law enforcement pays to the activities of users who access the internet from a particular domain.

Fraud detection

Where internet-based transactions originate from a domain known to be a source of high levels of fraudulent or suspicious activity, this may trigger manual or other checks on the authenticity of transactions from that domain. The use of a credit card via a domain other than the home domain of the account holder may flag potentially suspicious account activity.

Marketing

Marketers often target users who access the internet from a particular domain. In addition, legal restraints in one domain may mean that a service—for example, online gambling—may be inaccessible by users who access the internet from that domain.

Pricing differentials

Many products such as software, services, or music or video files can be sold and delivered online. The supplier may apply different pricing structures depending on where the item is being sent (see Box 6).

Box 6: Standing Committee on Infrastructure & Communications inquiry into online pricing

Online pricing was examined by the Standing Committee on Infrastructure & Communications in 2013 in response to concerns about the 'significantly higher prices paid by Australians in Australian dollars for IT products obtained online', at a time when the Australian dollar had appreciated greatly against the United States dollar.

The public's enormous interest in viewing events such as the Olympics or episodes of popular programs—whether without delay or without paying for content—motivates some people to circumvent geographical location restrictions to be able to access the material if it is available in another domain. For example, some Australians attempt to make it seem they are located in another country—typically the United States—to purchase products or services online at cheaper rates than they would if they bought the same product or service from an Australian IP address.

The committee noted that it is relatively easy for users to circumvent geoblocking software by using a VPN or proxy browser to make it appear as though they are accessing the internet from a particular domain (2013: 103):

Consumers may use a proxy server or a virtual private network (VPN) to bypass IP address-based geoblocking. Proxy servers and VPNs create an encrypted tunnel between a customer's computer and a server elsewhere, usually in another country. The customer's internet traffic is routed through that server and, as a result, the vendor's site recognises the IP address of the routing server, rather than that of the customer, which may allow consumers to access content that would otherwise be geoblocked.

The Committee discussed the distinction between a technological protection measure (TPM) and geoblocking technology. The Attorney-General's Department advised the Committee that it may be unlawful to circumvent a technological protection measure (TPM) that is protected under section 10(1) of the Copyright Act, for a measure that is used (2013: 98):

in connection with the exercise of the copyright;

by or with the permission of the owner or exclusive licensee of the copyright in the material, and

to control access to the work or other subject matter.

While the Committee did not support geoblocking, it concluded that the legalities of avoiding geoblocking were unclear. They made two recommendations to effectively defeat geoblocking (2013: 108):

Recommendation 5

The Committee recommends that the Australian Government amend the Copyright Act's section 10(1) anti-circumvention provisions to clarify and secure consumers' rights to circumvent technological protection measures that control geographic market segmentation.

Recommendation 6

The Committee further recommends that the Australian Government investigate options to educate Australian consumers and businesses as to:

the extent to which they may circumvent geoblocking mechanisms in order to access cheaper legitimate goods;

the tools and techniques which they may use to do so; and

the way in which their rights under the Australian Consumer Law may be affected should they choose to do so.

In its submission to the Australian Government's Competition Policy Review, Choice (2014: 4)

reviewed continuing issues with the 'Australia tax' and the price differentials that affect digital products. Choice described the significant pricing differentials of goods in the Australian market, and made a detailed submission suggesting reform in response to the impact of digital technologies.

Circumventing identification or geolocation

This discussion refers to peer-to-peer file sharing of material that has been made available for free elsewhere via the internet. The enormous public interest in viewing material for events such as the Olympics or for episodes of popular programs, quickly and for free, motivates some people to circumvent geoblocking by accessing the material from another domain. The Standing Committee on Infrastructure & Communications (2013) noted that, in these circumstances, it is relatively easy for users to use a virtual private network or proxy browser to make it appear as though they are accessing the internet from a particular domain:

> Consumers may use a proxy server or a virtual private network (VPN) to bypass IP address-based geoblocking. Proxy servers and VPNs create an encrypted tunnel between a customer's computer and a server elsewhere, usually in another country. The customer's Internet traffic is routed through that server and as a result vendor websites recognise the IP address of the server, rather than that of the customer, which may enable consumers to access content that would otherwise be region-blocked (Standing Committee on Infrastructure & Communications 2013).

Perpetrators of DNS misuse

Initial research for this project showed it is not possible to assess the number of cybercrime offences committed, let alone instances of criminal misuse of the DNS. Specific cybercrime offences and potential DNS misuse may remain undetected or, if detected, may not be prosecuted; or, if prosecuted, the prosecution may not be successful.

Perpetrator profiles

Only a fraction of cybercrime offending ends with the successful prosecution of an offender. Gathering information on prosecutions is difficult, because ordinarily cases are only officially reported when a legal point is decided in a higher court on appeal. Where offenders are prosecuted, the bulk of cases are finalised by the trial court; these may or may not be reported via the press or some other outlet. It is therefore not feasible to survey the range of cases successfully prosecuted, and caution is required when drawing on reported cases for information about cybercriminals.

Despite these difficulties, the United Nations Office on Drugs and Crime (UNODC) collated information about perpetrators in its *Comprehensive study on cybercrime* (Malby et al. 2013). The UNODC report argued that it is important to understand more about the perpetrators of cybercrime, and about cybercrime as a 'socio-technological phenomenon' (Malby et al. 2013: 39) The report also acknowledged the lack of research into organised criminal activity in cyberspace. While a comprehensive typology of cyber offenders is unlikely to be developed given the limited data available, the UNODC drew on the work of Lu et al. 2006; Li 2008; Detica and London Metropolitan University 2012; and McGuire 2012) (The references to Detica and London Metropolitan University and to McGuire (2012) appear to relate to the same report. Links to that report are no longer active and neither of two versions of the reference could be located. They are referred to here as sources used by others although copies were not obtained for verification or clarification.)

Key findings derived from these studies were that:

- perpetrators need fewer IT skills as they can access malware toolkits;
- almost 80 percent of cybercrime is organised;
- the kind of organisation required to commit many cybercrime acts is said to lend itself to small groups, loose networks or large-scale organised crime;

- young men in developing countries, in particular, are increasingly associated with online fraud; and
- the typical offender was a young male, although child exploitation material offending generally involves an older male cohort; on the whole, offenders do not have specialised education.

Broadhurst et al. (2014) review possible models for presenting the characteristics of organised online offenders. The authors draw primarily on the work of McGuire (2012 – original source could not be located) and Chabinsky (2010) on cybercrime offender characteristics. Their review presents two basic levels of organised crime across three possible degrees of interaction with the internet. The levels of organisation are classed as loosely organised to more highly organised, and either wholly online, a mixture of online and offline, and wholly offline. The authors cite a variety of motives including a desire to expose faults; seeking celebrity, reprisal or monetary gain; or to feel involved in keeping the internet 'open'. The basic elements of the typology are the level of organisation and the degree to which a criminal activity takes place offline or online.

Tropina (2012: 159–160) viewed digital networks as enabling cybercrime by giving rise to an ecosystem with distinct business models. The business models include 'crime-as-service', where criminals provide other criminals with cybercrime tools such as viruses, Trojans or keyloggers. Another model involves the provision of money laundering and mules to monetise the results of cybercrime activity. Tropina concluded that much more was known about what cybercrime groups can do than about who they are and how they are organised.

Lusthaus (2012: 71) drew attention to the apparent conflict between the organised nature of cybercrime and the 'large deficit of trust' that exists online, and which might be supposed to inhibit cooperation among criminals. According to Lusthaus, this trust deficit is overcome by a range of mechanisms that build trust within the context of online anonymity. Trust is established through mechanisms allowing criminals to establish a cybercriminal identity; demonstrate their expertise; and impose forms of extra-legal governance—principally by naming and shaming those cybercriminal identities that cannot be trusted, for whatever reason, by cybercrime networks.

Wall (2015: 84–85) strongly critiques existing models used to describe organised internet crime. He proposes a distributed model of organised crime that is much flatter than a mafia-like command and control model. Wall argues that many forms of cybercrime 'do not display the classic signs of organised crime' but have distinctive traits, including an ephemeral nature and stealth. Wall concludes that cybercrime 'can never be eradicated and can only be regulated and managed to minimise its impacts.' Interestingly, Wall writes that sending cybercriminals to general prisons is itself dangerous because this brings together cybercriminals and traditional organised crime offenders.

The current study suggests that it is worth adding to this framework by distinguishing more clearly between the platforms for criminal activity and the actors who make use of those platforms. For example, between the Darknet site Silk Road as a platform for unguided

collective action, and Ross Ulbricht, the individual who was convicted of offences committed as founder and operator of Silk Road. It is also important to note that there are major differences between activity on the surface web versus the Deep Web or the Darknet.

Finally, it is useful to distinguish between the activities of states, organised crime, corporations and individuals. This enlarged framework indicates the potential for further research into whether, and how, the additional categories for analysis may help provide a complete picture of cybercrime.

Country of origin

It can be extremely difficult to determine who is responsible for an act on the internet. Indeed, much attention has been given to finding ways for users to remain anonymous or hide their physical location. Aside from the anonymity of the darknet, geographically based IP addressing can be manipulated to hide the actual physical location of a user. Techniques such as DNS tunnelling and IP spoofing make it hard to determine where an offender is physically located, even in terms as simple as nationally. It can also be much more difficult to identify the offender. For example, McCombie (2011) makes a detailed study of Eastern European involvement in phishing scams in Australia.

The APWG (2015) has conducted global surveys of phishing activity on the internet for more than a decade. The APWG global survey for the second half of 2014 estimates more than 95,000 phishing domains were observed in the period. Of these, just over 27,000 were maliciously registered and just over 68,000 were compromised domains.

It was estimated that approximately 75 percent of malicious domain registrations were located within five TLDs. These were two generic TLDs, .com and .net, and three country code top level domains (CCTLDs): .tk (Tokelau), .pw (Palau), and .cf (Central African Republic). Of the three CCTLDs, .tk and .cf offer free domain registration. Tokelau was described as the 'cybercrime centre of the world' by the Commonwealth Secretariat (2014: 515). The APWG (2015) reported that Chinese phishers registered most of the malicious domains.

The APWG surveys illustrate the emergence of phishing activity launched from subdomains (Piscitello & Rasmussen 2008), where a domain is made available within another domain; this means the management of the subdomain is a step further removed from the host domain's regulatory framework.

Legal responses to DNS misuse

Criminal action

The UNODC 2013 study on cybercrime found traditional criminal law did not provide sufficient protection from online offences, and that cybercrime laws that criminalise certain actions and outline procedures to support law enforcement and international cooperation are needed (Malby et al. 2013: 81). The authors noted there was general agreement on the need to harmonise laws, largely driven by the need to immediately eliminate safe havens and facilitate evidence gathering. Penalty regimes were significantly different, indicating quite different perceptions of the seriousness of online crime (Malby et al. 2013: 86). Areas where cybercrime laws varied or coincided were noted across five main regional instruments shaping cybercrime (the EU, the Commonwealth of Independent States, African organisations, the League of Arab States and the UN; Malby et al. 2013: 93). Despite a lack of global uniformity, these multilateral cybercrime instruments positively influenced non-state parties and non-member states (Malby et al. 2013: 102).

As well as arguments for greater consistency and uniformity in addressing the problem of cybercrime, the fundamental differences between jurisdictions that prevent the adoption of a completely standardised approach should be considered (Naziris 2014).

Malby et al. (2013) found there were areas of widespread agreement on core cybercrimes, or criminalising offences 'against confidentiality, integrity and accessibility of computer systems'. The cybercrime laws of European nations were considered the most sufficient. Overall, it was agreed that spam, the misuse of tools, hate or racist speech and the grooming of children should be criminalised (Malby et al. 2013: 107). The report argued that differences in criminalisation can have profound effects on regulatory scope and the capacity for international cooperation. For example, what was protected by criminalising illegal access to computers and data—that is, data, system or information—differed from jurisdiction to jurisdiction; different jurisdictions also differed in whether mere access was sufficient to be cybercrime, or whether there must also be malicious intent or a breach of security measures (Malby et al. 2013: 111).

The report found that most cybercrime offending comes to the attention of law enforcement through victim reports. A private sector survey commissioned for the report suggested that 80 percent of individual victims do not report cybercrime to police. The law enforcement response to the under-reporting of cybercrime included increasing public awareness, as well as focusing on crime markets and criminal scheme architects (Malby et al. 2013: 117).

Procedural laws encouraging investigation and prosecutions in support of investigation and prosecution were least likely to be uniform. Special evidence laws were enacted in many jurisdictions, but in many of these places the police lacked the capacity to enforce them (Malby et al. 2013:152). Overall, prosecutions were constrained by legal frameworks, problems of attribution, problems with evidence and delays in international cooperation (Malby et al. 2013: 168). Brenner and Schwerha (2004) showed that procedural laws were critical to the investigation and prosecution of cross-jurisdictional cybercrimes. Brown (2015) drew attention to the continued need for, and importance of, collecting, exchanging and using electronic evidence to prosecute cybercrime.

The report found that private sector security was most weak for small and medium enterprises. Private industry, including ISPs, can play a key role in bolstering security and improving responses to emerging threats. Help from the private sector was required in logging internet activity, identifying compromised computers, blocking malicious content and communicating with users (Malby et al. 2013: 239).

Hu et al. (2013) conducted a comparative analysis of law enforcement outcomes for cybercrime offences in media reports from the US, the UK, a number of European jurisdictions, Australia and China. They found most cybercrime prosecutions were for credit card fraud, child exploitation material, social networking-based crime and 'juvenile delinquency.' Juvenile delinquency was defined as hacking by people under the age of majority that was not committed for financial or other benefit. There are substantial difficulties in using media sources to infer crime rates, and media coverage is unlikely to be representative of all cases prosecuted; the number of cases studied was also small. Despite these limitations, the authors found differences between jurisdictions that increased the likelihood detection and prosecution for criminal activity. For example, there was less likelihood of being charged in the US and a greater likelihood of imprisonment for credit card fraud offences in China. The authors concluded that economically advanced jurisdictions had more comprehensive cybercrime laws. They also argued that greater reliance on specific cybercrime offences in common-law jurisdictions, as opposed to adapting existing criminal law in civil law jurisdictions, better addressed cybercrime.

Civil action

Domain name disputes

ICANN and other internet governance agencies have spent much time addressing controversy around what principles should be applied in regulating the allocation and registration of

domain names. For example, McGillivray and Lieske (2001) referred to the problem of 'webjacking', and described how victims need to work with the relevant domain name registrar, as well as considering taking action under the Uniform Dispute Resolution Policy (UDRP) adopted by all registrars. They described this as 'a relatively quick and inexpensive way to resolve domain name disputes' (McGillivray and Lieske (2001: 1). Potential problems associated with domain name registration that may lead to legal disputes about 'cybersquatting' or 'domain name squatting' are generally addressed by registration requirements and facilities for the settlement of domain name disputes.

In Australia, auDA's (2012b) rules for domain name registration set a number of requirements for registration under different TLDs. These arrangements were reviewed favourably by Roache-Turner (2013) and are set out in Box 7 below.

Box 7: Domain name allocation rules

First come, first served

Domain name licences are allocated on a first come, first served basis. Domain names cannot be pre-registered or otherwise reserved.

Registrants must be Australian

Domain name licences may only be allocated to Australian registrants, as defined under the eligibility and allocation rules for each second level domain (2LD).

Composition of domain names

Domain names must:

a) be at least two characters long;

b) contain only letters (a to -z), numbers (0 to 9) and hyphens (-), or a combination of these;

c) start and end with a number or a letter, not a hyphen; and

d) not contain hyphens in the third and fourth position (eg ab--cd.com.au).

Domain name licence period

The domain name licence period is fixed at two years. It is not possible to license a domain name for a shorter or longer period.

Renewal of a domain name licence at the end of the two-year period depends on the registrant continuing to meet the eligibility and allocation rules for the relevant 2LD.

Number of domain names

There is no restriction on the number of domain names that may be licensed by a registrant.

auDA's Reserved List

auDA's Reserved List contains names that may not be licensed. The list is available on auDA's website.

Prohibitions

Registering domain names for the sole purpose of resale or transfer to another entity is prohibited.

Source: auDA (2012b:np Schedule A)

Disputes in the United States

The *Anticybersquatting Consumer Protection Act* (ACPA), 15 USC § 1125(d), was enacted in the United States in 1999 and established a legal basis for the owner of a mark (including a personal name) to take civil action to seek injunctive relief and to secure the forfeiture, cancellation or transfer of an infringing domain name. The relevant provision is presented in Box 8.

Box 8: *Anticybersquatting Consumer Protection Act* **15 USC §1125(D), Cyberpiracy prevention (extract)**

(1) (A) A person shall be liable in a civil action by the owner of a mark, including a personal name which is protected as a mark under this section, if, without regard to the goods or services of the parties, that person

(i) has a bad faith intent to profit from that mark, including a personal name which is protected as a mark under this section; and

(ii) registers, traffics in, or uses a domain name that—

(I) in the case of a mark that is distinctive at the time of registration of the domain name, is identical or

confusingly similar to that mark;

(II) in the case of a famous mark that is famous at the time of registration of the domain name, is

identical or confusingly similar to or dilutive of that mark; or

(III) is a trademark, word, or name protected by reason of section 706 of title 18 or section 220506 of

title 36.

Piscitello (2012) pointed out the complexity and time-consuming nature of pursuing a domain name dispute and provided comprehensive guidance for taking civil action under US law to obtain domain name orders, seizures and takedowns. One aspect of the cybersquatting problem in the United States is described by the executive chairman and founder of GoDaddy, Bob Parsons (2016). Parsons refers to 'add/drop schemes' (or 'domain tasting'), where domain names are registered in bulk and put up for sale immediately. If the domain name is not sold within the free five-day grace period before payment is required, the registration is withdrawn. The scheme operators would therefore only pay a registration fee for those domains that they had sold in the grace period. McNamara (2006) described how pernicious this conduct was in effectively rorting the domain name registration system. Thibodeau (2007) described the cost to established businesses of monitoring and responding to potential domain name trademark infringement.

Fahey and Murphy (2009) provided an overview of the law on domain tasting, with particular reference to the case of *Verizon California, Inc. v. Navigation Catalyst Systems, Inc* 568 F. Supp. 2d 1088 (C.D. Cal. 2008). In that case, it was found that domain tasting by the defendant had targeted existing trademarks and created confusingly similar domain names. Judgement was awarded to the plaintiffs, with orders for the surrender of the domain names at issue in that case. However, the court refused to restrain the defendant's domain tasting business. Sloan (2012) also reported on the apparently profitable domain tasting businesses operated by people in the US. Parker (2007) detailed a case in which an election candidate registered multiple domain names for sites that might have been used by an opponent to run their campaign. Rodenbaugh (2009) pointed out the low cost of registering a domain name compared with the cost of pursuing UDRP action to have a confusing or misleading domain name taken down, which reportedly resulted in 'literally millions of clearly infringing domain names currently registered by cybersquatters' (Rodenbaugh (2009: 9).

Godfread and Dorrain (2010) surveyed cases brought under the *Anticybersquatting Consumer Protection Act* (ACPA) in 2009 and 2010. They summarise the cases for 2009 as being 'decidedly defendant-friendly' and quote three 2010 cases; in the first, the plaintiffs secured the maximum available damages; in the second, actual and punitive damages; and in the third an award of over US$33m.

IP infringement

Domain names and domain name administrators are, arguably, not amenable to regulation by existing criminal law. The Swedish case of Pirate Bay (piratebay.se) involved substantive and procedural aspects of the criminal law of Sweden. The case arose following Pirate Bay's return to Sweden following its movement in quick succession through other domains where de-registration followed soon after registration.

The Internet Infrastructure Foundation of Sweden (IIFS) is the top-level domain name administrator responsible for the Swedish top-level domain .se. In 2013, the Swedish prosecutor commenced proceedings against the IIFS under section 53 of the Swedish *Copyright Act* and Chapter 36 section 3 of the Swedish Penal Code to obtain forfeiture of the domains piratebay.se and thepiratebay.se.

In May 2015, the Stockholm District Court ruled that, while the IIFS knew that the Pirate Bay domains were being used to facilitate criminal copyright infringement, it was not obliged to block or forfeit the domain names and was not responsible for the actions of those using the domains. However, the court did order the IIS to hand over ownership of the domains to the Swedish state (Anon 2015b).

Elisabeth Ekstrand (2013: np), General Counsel for IIFS, argued that 'the degree of responsibility that .se can be deemed to possess in its capacity as top-level domain administrator is uncertain, and it is also uncertain whether a domain name can be considered equivalent to an object or property. The position of .se was effectively to resist the prosecutor's claim until the court clarifies the legal situation.

Ekstrand (2013: np) indicated that the Copyright Act action was based on the assertion that .se (the IIFS) is 'an accomplice to crime' as its domain name operations promote copyright infringement (through the piratebay.se website) and this justifies a forfeiture order should .se be considered as abetting the crime; Ekstrand stated that this would be framed in terms of 'de facto promotion of crime' rather than 'intentional abetting of crime. (2013: np)'

Injunctive relief

Microsoft has also taken private court action against domain name misuse. Microsoft's Digital Crimes Unit focused on three main areas where the company could make a direct impact. These were technology-facilitated child sexual exploitation crimes, content piracy and other intellectual property infringements, and malicious software crimes, particularly botnet-driven internet attacks.

In court documents filed in an ex parte action against Vitalwerks (or No-IP), Microsoft Corporation (2014) said that, in early 2014, it identified the top malware threats affecting its consumers. A significant amount of malware was programmed to connect to internet domains leased by Vitalwerks (or No-IP). Microsoft was seeking a temporary restraining order to 'stop the harm' by 'blocking traffic between infected computers and malicious No-IP subdomains, through which the Malware Defendants (Mutairi, Benabdellah, and Does 1-500) communicate with the infected computers' Microsoft Corporation 2014: np).

Microsoft argued for the ex parte order on the basis that it had a good chance of ultimately winning its case for computer abuse and common-law action. Microsoft alleged that the abusive conduct was enabled by the dynamic DNS service provided by Vitalwerks and that this caused 'irreparable harm including the loss of goodwill, brand integrity, and resources expended to investigate and combat this abuse.' The claim states that 'defendants are able to control user computers and steal sensitive information from unknowing and unsuspecting Microsoft customers and the public at large causing them untold harm' Microsoft Corporation 2014: np).

In setting out the relative harms of granting ex parte injunctive relief, Microsoft asserted that the defendants' criminal activities served no legitimate purpose; that only traffic to the malicious subdomains was to be blocked; and that Vitalwerks offered a free service and would not lose income. Microsoft argued that advanced notice would permit the defendants 'to disappear without a trace, thus rendering Microsoft's efforts fruitless'. After Microsoft obtained ex parte injunctive relief, it emerged that a number of users of the No-IP service who were not targeted in the Microsoft civil claim had lost access to their subdomains (Goodin 2014).

Goodin (2014: np) explained the popularity of the dynamic service provided by Vitalwerks, which provided a free subdomain that mapped to whatever IP address the user was using at any time. These qualities were noted as attracting online gamers and Linux user groups, and likely to 'be popular with criminals running command and control servers that manage large numbers of infected computers' (Goodin 2014: np).

While critical of the number of untargeted users affected in this case with the temporary take-down of Vitalwerks, Goodin noted the difficulty of taking action against sophisticated schemes:

> By creating a sprawling series of redundant servers with a variety of hosts, IP addresses, and domain names, the malware operators can elude takedowns by shuttling compromised end-user computers from one to another. Microsoft's technique relies on stealth to disconnect virtually all of a campaign's malicious servers at once before the operators have a chance to respond. (Goodin 2014: np)

Preventing DNS misuse

DNS misuse can be prevented and controlled by applying a number of general criminological theories of situational crime prevention. In essence, these aim to prevent the occurrence of crime by making it more difficult and risky to commission crime, or making crime less rewarding or excusable (Clarke 1997). More specifically, situational crime-prevention approaches attempt to influence individual behaviour through five key mechanisms (Morgan et al. 2012):

- increasing the effort involved in offending—eg decreasing access to a desired item through the use of physical security;
- increasing the risk associated with offending—eg increasing formal surveillance in high-risk areas;
- reducing the rewards that come from committing a crime—eg decreasing the value of assets obtained through crime by interrupting illicit markets;
- reducing the situational factors that might influence an individual's offending—eg discouraging individuals from imitating the criminal behaviour of their peer networks; and
- removing excuses for offending behaviour—eg raising awareness of the harms associated with specific types of offences;

Situational crime prevention approaches are underpinned by three dominant theories: namely routine activities theory; crime pattern theory; and rational choice theory. Rational choice theory proposes that offenders are rational actors who weigh up the benefits and drawbacks associated with proposed course of illegal conduct before making a decision to commit a crime (Vold, Bernard & Snipes 2002). Crime pattern theory seeks to understand how people encounter or experience crime as part of their everyday lives, and the role that communities and neighbourhoods play in this process (Morgan et al. 2012). Finally, routine activities theory suggests that crime can be reduced by addressing the three essential requirements for the commission of crime: 'a motivated offender, a suitable target and the absence of a capable guardian' (Morgan et al. 2012: 13).

A large body of evidence supports a situational approach to preventing a range of different criminal behaviours. Although developed for use in preventing property and street crime, situational approaches are also applicable to technology-enabled crime (Smith 2015). Beebe and Rao (2005: 10) claimed that situational crime prevention strategies concentrated too much on affecting the perceived cost of crime with far less attention being given to reducing the

perceived benefit of cybercrime. Situational crime prevention deals primarily with financially-motivated crime by increasing perceived effort and risk, decreasing perceived reward and removing excuses for criminal behaviour. The specific model for dealing with possible attacks on data talks of 'deception, assumption and experience' focused on reducing perceived benefits for potential offenders (Beebe and Rao (2005: 15). However, this is described in terms of questionable actions like attempting to deceive would-be offenders about the nature or value of data repositories. The experience category was described in terms of 'encryption, automatic data destruction mechanisms, separation (compartmentalization) of information, and data hiding' (Beebe and Rao (2005: 16).

Increasing effort

Registration systems

Registries authenticate those obtaining domain names in varying ways, which is a major issue with domain name registration (Molnar 2005). It is more difficult to impose authentication requirements in generic TLDs or openly available Country Code Top-Level Domains (ccTLDs) that do not limit registrations to a country-level domain.

Problems with registration accuracy can have a long-term impact as the information provided at registration becomes the Whois entry. Whois is a searchable registry that allows domain name owners to be identified, but Whois information may be deliberately false, misleading or inaccurate. In 2005, the United States Government Accounting Office (GAO) reported on the accuracy of contact information provided during domain name registration in the three TLDs .com, .org, and .net, and found just over eight percent of domain registrations involved incomplete or patently incorrect details (GAO 2005). In some cases, domain owners may opt to withhold identifying information due to privacy concerns. When a domain is wittingly or unwittingly misused, the lack of reliable Whois information can be a major impediment to any response.

This variation in arrangements for domain name registration makes authentication and registry accuracy difficult to achieve. It would also be considerably difficult to authenticate the ownership details of existing domain names, except perhaps when re-registration may be required; however, ICANN requires generic TLD registrars to verify registrant contact information regularly. ICANN is also considering developing a next-generation gTLD Registration Directory Service (RDS) for Whois data (ICANN-GNSO 2015). Interestingly, scammers have thought of using false Whois registration update requests in phishing. One scam reported in Australia in January 2014 involved false notices asking .com domain owners to update their Whois registry entries (Pongas 2014).

IT security

Gont (2008) canvassed the security limitations embedded in the architecture of IPv4. The TCP/IP protocols were created with a focus on operational requirements for sharing large service machines on ARPANET. Gont explained there was no central coordination of knowledge about known security flaws that had been poorly documented or patched over. The lack of official, documented responses to security problems meant not all vendors implemented fixes, and some fixes were developed without consideration of their effectiveness. Gont concluded that the failure to adopt fixes to the official TCP/IP specifications means that we lack a security roadmap, and that this makes the task of securing TCP/IP implementations very difficult.

IT security approaches to protect the DNS include the introduction of the Domain Name System Security Extensions (DNSSEC; Microsoft 2014). Those who fail to follow the most basic recommended security procedures are most at risk and are ongoing targets. The standard IT security measures for protection against malware are set out by Chichonski et al. (2012). These require action across the key areas of preparation, detection and analysis, containment, eradication and recovery. Following these guidelines is probably not enough, given that offenders are continuously working to overcome these security measures.

Where targets have hardened IT security in place, software engineering approaches can be combined with social engineering to circumvent protections—for example by spear-phishing, or the crafting of phishing attempts specifically targeting key members of an organisation. Spear-phishing can also involve offenders targeting organisations or service providers with weak security protocols to gain access to the data or systems of an ultimate target organisation.

Reducing rewards

The period during which an exploit or data derived from cybercrime can be used significantly influences the profitability of cybercrime. A persistent piece of malicious code can be exploited for longer, and the longer compromised data can be used or goes undetected, the more likely it is to be monetisable.

The *Computer security incident handling guide* (Chichonski et al. 2012) was drafted, at least in part, to reduce the time available to offenders to exploit a vulnerability or monetise a particular cybercrime. The APWG is an example of strong, coordinated action by multiple partners to reduce the persistence of a threat using the measure referred to as ‘phishing by uptime’.

Removing excuses

Removing excuses that may underpin offender behaviour is unlikely to apply to DNS misuse in general; however, this approach is advocated for particular forms of offending, where offending may be justified on the basis of supposed right, grievance or disregard for victims (Wortley 2001).

Other crime reduction options

It is increasingly recognised that internet security threats are most likely to emerge on platforms like mobile devices, and from new applications and services that occur in the application, network and storage layers of internet architecture. to the critical factor in social engineering is user behaviour; in software engineering, there is a tension between utility and security. The background to this is a potentially dramatic shift in governance arrangements or movement towards a fragmentation of the internet.

User education

Criminal activity—particularly organised criminal activity—relies on trust. Criminals (and legitimate users) must trust each other or, at least, must balance their degree of confidence in another against any risk they are exposed to through that person.

Misuse of the DNS seeks to exploit users' belief that they can navigate the internet successfully and with acceptable levels of exposure to risk. Criminal activity will often involve some form of social engineering to establish sufficient user trust for a crime to be committed against them, or using them. Unless someone is seeking to destroy the internet—which may well be impossible—any use, whether legitimate or illegitimate, depends on perceptions of the reliability of the system as a whole.

Collective action

As more and more people connect to and make use of the internet, clashes occur between different interest groups; sometimes the medium has itself transformed underlying interests in ways that lead to conflict. Baloch and Cusack (2012) discussed the lack of universally enforceable rules of conduct for the internet. They claim this lack prevents adequate debate on issues such as censorship, violation of the end-to-end principle [&] intellectual rights protection. They also claim it prevents stakeholders from enforcing decisions Baloch and Cusack (2012: np) .

For many users, and particularly for those who grew up with the internet, infringing intellectual property interests is commonplace. Users who disregard intellectual property barriers may become more and more familiar with the transgressive aspects of the internet. They may become adept at using VPNs or other anonymisers; participating in peer-to-peer networks; cracking digital restraints; avoiding geoblocking; sharing their knowledge and skills with likeminded persons and, potentially, coming to see freedom of access as a right or something to champion. The ways in which criminality is attached to some forms of common internet use requires further attention.

Payment systems

Thomas et al. (2015: 1) set out to systematise our understanding of the underground economy of the internet and set out a simplified model of 'profit centers' and 'support centers.' The profit centres allow for the monetisation of online crime, and the support centres provide the

tools and knowledge needed to commit online crime. The authors argue for a 'drastic departure' from protecting users and system security to focus on disruption of the profit and support centres. It is argued that the greatest disruptive effect will come from concentrating on 'frail underground relationships' Thomas et al. (2015: 1).

The continuing development of online payment systems also raises the possibility of creating more secure systems for legitimate payments; see, for example, Islam 2015. New payment systems that are integrated with the 'internet of things' open up significant opportunities for global commerce. Krishna (2015) describes how block chains might be used to join payment systems and digital information needed to verify or document a transaction. Cuomo (2015) writes about the potential to broadly use block chain technology (as used by the cryptocurrency Bitcoin) across many forms of value transfer, to extend to record keeping for transactions with multiple parties: block chain technology, however, is not suitable for all transactions. A practical application of these ideas was announced at a global entrepreneurship summit hosted by President Obama in Kenya in July 2015 (Batty 2015). IBM will work with Bitsoko, which provides a mobile platform for Bitcoin payments, to foster business growth and innovation. Bitsoko was also supported by the Bill and Melinda Gates Foundation in April 2015.

Conclusions

The internet's potential does not simply lie in machine connectivity. As well as the possibility of connecting literally billions of devices, the internet offers us the capacity to interact with and exploit this potential in directed and meaningful ways. The internet is nothing without connectivity or the means to exploit it. Under the DNS, domain names mark an exclusive identifiable virtual space for the use of the domain name owner.

The capacity to regulate potential misuse of the DNS is limited. While the DNS requires centralised authority, no single global entity is responsible for regulating all its aspects. This is because regulation of the DNS, like other aspects of the internet, follows a multi-stakeholder governance model and a distributed administrative model. Also, much of what happens on the internet lies beyond the jurisdictional reach of individual nations' criminal law.

An initial review of DNS operations suggests that, like other aspects of the internet, it is loosely governed and subject to limited centralised control; its misuse is therefore likely to be difficult to regulate. Overall, the multi-stakeholder model of governance promotes open access and minimal restraint, and offers little capacity to regulate the internet. Efforts are made to accommodate demands for increased accessibility while maintaining functionality.

The formal mechanisms for control and governance of the DNS provide limited scope for the exercise of regulatory authority. The architectural standards of the internet and the DNS offer a less direct form of regulatory control. The most obvious and, perhaps, strongest control point is the allocation of IP addresses and the registration or renewal of domain names, which are centrally coordinated under the internet's multi-stakeholder governance model.

The global exercise of these central roles is beyond the control of any particular state. The administration of these assignment functions is distributed worldwide on a regional basis, down to a national level. The capacity to regulate DNS registration and address the security weaknesses of internet architecture provides limited means to control the environment for criminal misuse of the DNS and the internet. In this context, states or agencies may seek to control or influence these functions at a national level.

Floridi (2014) surveys the changes in information and communications technology and rapid developments in data processing capacity, speed and affordability. Floridi argued that we are entering an era of hyperhistory, with unpredictable consequences. One feature of this age of hyperhistory is the creation and accumulation of vast amounts of data. Floridi quoted studies

estimating the amount of information accumulated in all human history before the computer age as 12 exabytes. This rises to an estimated 1,600 exabytes in 2011 (a 133-fold increase) and eight zettabytes, or 8,000 exabytes, by 2015—or 666 times more data. Floridi pointed to a countervailing trend in our capacity to store and access data over time. While data are generated rapidly, the speed of our access to that data is decreasing because of congestion, which reduces access speed; the volatility of computer memory; and increasingly redundant technological platforms.

Two aspects of global connectivity can be harnessed to minimise risks of abuse: the first is available resources and the second is people. The intensity and density of the connections between resources and between people will vary. The following indicators assume some basic level of access as a starting point.

In April 2014, the International Telecommunications Union (ITU) estimated that by the end of the year there would be 'almost three billion Internet users' with 'two-thirds coming from the developing world' (ITU 2014: 1). The ITU reported that mobile broadband connections were driving growth in internet access, with mobile connections across Africa rising from two percent of connections in 2010 to 20 percent in 2014. Overall, the ITU predicted that 55 percent of mobile broadband subscriptions would be in the developing world by the end of 2014. The number of mobile-cellular (mobile phone) subscriptions was forecast to 'reach almost 7 billion by end 2014' with a 'penetration rate of 96 percent' including more than half (3.6b) in the Asia-Pacific region. 'Fixed broadband penetration' is highest in Europe at 28 percent, or 'almost three times as high as the global average' of 10 percent (ITU 2014: 1).

Alongside this expansion the pace of development and change is accelerating; this acceleration relates to the impact of technology and how people make use of it. In between, there is also the sphere of human-computer interaction (HCI) first referred to by Card et al. (1983). It is in this sphere that the forces of technological change and human ingenuity come together to generate more possibilities than could be imagined from the first intended use of a particular technology. In this context, criminal misuse of technology can be seen as the intended (malicious) or unintended (inherent) use of technology's possibilities.

The technological drivers of change include the internet's physical architecture and its programming potential. This constant change is driven in part by technological forces such as:

- rapid technological advances;
- the continued discovery of new processes and applications;
- an exponential growth in the number and kind of devices connected to the internet;
- an exponential growth in the computing and data storage capacity of individual devices and the internet collectively;
- increasing numbers of people worldwide connecting to the internet; and
- the intended and incidental aggregation of enormous amounts of data.

These developments give rise to new technological possibilities and new ways of working with, or building on, existing technology; it can be hard to anticipate or adjust to these changes.

Human drivers of change are the result of how people use and interact with technology or, sometimes, how people are excluded from using or not involved with technology. Change is also driven by people and groups representing various interests, pushed further by the following pressures:

- rapid escalation in the number, diversity and national identity of new users;
- new open-source platforms and business models for accessing, storing and manipulating data; and
- repeated contests over the principles said to underpin the internet and how those interests may be represented or expressed.

The internet's multi-stakeholder governance model provides an arena for contest and debate beyond the immediate control of nation states. The internet's apparent paradoxes should also be considered. These paradoxes arise from how social policy has been built into the architecture of the internet and the degree to which various principles have and continue to shape it. One example is the internet's open nature and the associated paradox of finding vulnerability and survivability on an open but resilient platform, which gives rise to continued cycles of attack and the securitisation of both hardware and software elements of the internet.

Considering cybercrime from the perspective of domain name misuse provides an opportunity to question the assumptions, possible misconceptions, loose definitions and purposes of cybercrime law and literature. Placing the DNS at the heart of the discussion brings the possibilities of the internet into sharp relief. The DNS is not designed for security and is neither good nor bad. Its seemingly endless potential challenges all pre-existing state-based law and regulation. Much more discussion is required within the multi-stakeholder model about how the internet is to be managed and, possibly, regulated.

National cybercrime laws are essential to protect the internet and the broader interests of society. Internet activity must be regulated with great care to allow the promise of an open internet to be realised; at the same time, as this paper hopefully demonstrates, cybercrime must be defined with great care, and more information about the possible use and misuse of the internet must be gathered.

Identifying the characteristics of internet offenders raises intractable problems. Given the nature and scope of cybercrime, the notion of describing particular characteristics of cybercrime offenders seems unrealistic—even more so in connection with those who commit crimes against the DNS. In fact, the Internet presents us with a vast contested space with incredible potential for many different uses. There may be a congruence of interest in certain affordances created by technology, and yet other affordances may be hotly contested.

Future directions

Some of the immediate threats to the internet identified by TrendLabs (2015: 3) include:

- the likelihood that criminals will increasingly 'turn to Darknets and exclusive-access forums' as support centres;
- hacking tools and attempts will be 'bigger and more successful';
- threats will move to mobile platforms;
- targeted attacks will become more prevalent;
- new mobile payment methods will create new threats;
- open-source apps will be targeted;
- technological diversity may help insulate platforms but not data; and
- more severe threats to banking and finance will emerge.
- In short, the internet will continue to offer criminal opportunities and cannot be viewed as a benign environment.

Nonetheless, there are ways the internet's positive aspects can be preserved and built on. There would be considerable value in nuanced research into the complexities of cybercrime, accompanied by collaboration between law enforcement, providers and users. This would require focused discussion of the values and principles that ought to inform how the internet is regulated.

It seems likely that in the year ahead the subject of internet governance will be hotly debated ahead of the United States' relinquishing control of IANA. Whether and how that will take place is not certain, and the moves by the United States are surrounded by a rising clamour around internet governance. This in itself will disrupt existing arrangements, while also providing opportunities to improve internet governance.

However, debates about the open internet do not address the rise of the darknet and other online platforms that are not directly accessed from the World Wide Web. The DNS and its governance are removed from these realms, which may be used to foster criminal activity. Further work is required to relate the spheres of the open internet and the darknet in a comprehensive picture of cybercrime.

There are important questions to be resolved around internet governance, how it is used and how it may be regulated—if, indeed, it can be regulated at all. There is no doubt that increased cooperation between users, service providers and other stakeholders will be vital to the internet's continued evolution, and all will need to be involved in future discussions of governance and decision-making. Within this larger whole, the coordination of law and cooperation between law enforcement will be crucial to enforcing cybercrime provisions. Continued joint efforts by government, industry and users will be necessary to meet regulatory challenges, particularly among ASEAN nations and in the region generally (Khanisa 2013).

The issue of whether old interests and established user communities may be unfairly privileged must also be considered. The stakes involved in regulating the internet require a critical view of cybercrime—how it is defined, analysed and understood, and how laws against it are enforced. It is vital to think of the internet as a broadly conceived potentiality for humanity rather than a network of networks, series of machines or preserve for certain interests. The internet has the capacity to represent the sum of us all; it is built on a global physical platform and potentially offers both unparalleled liberty and restraint. This must be borne in mind when considering how the law intersects with this space, sometimes clumsily.

Final observations

This review shows how the DNS is fundamental to access to the open internet and how, in that sense, all cybercrimes on the open internet involve the use of the DNS. By moving away from the common taxonomy of cybercrime—that of target, tool and incidental offending—we can better identify points for regulatory intervention.

It is hard to appreciate the nature and extent of cybercrime nationally and globally. While many jurisdictions approach cybercrime in similar ways, there are also some major points of difference in how offences are defined, investigated and prosecuted and how records are kept. The knowledge base currently available when analysing cybercrime is poor, given jurisdictional differences and limited collection of cybercrime data. Data relating to phishing, however, has been consistently collected and analysed. The APWG reports are a valuable resource for tracking developments in cybercrime, and exemplify the value of tracking cybercrime over time.

The analysis of cybercrime by reference to the layers of the internet—in the sense of both the layers of an IP/ITP session and the layering of the territories of the DNS—opens up new opportunities to understand the regulatory framework cybercrime takes place in. Further defining cybercrime by whether it uses the internet as a platform for crime, or software engineering and social engineering techniques, will also provide insight into offending and crime prevention strategies.

Lack of available data makes it unfeasible to present a realistic picture of cybercrime offenders or the outcomes of criminal investigations or prosecutions. Some generalised models of offender natures are available, but these do not represent the whole of an offender's behaviour, and may be influenced more by the nature of terrestrial offending than by a full appreciation of cyberoffending. There is much more work to do in this area.

Criminological theory, particularly crime prevention theory, presents some useful insights that apply in developing crime prevention strategies. While much attention has been given to software and IT systems security, a better understanding of how software and social engineering are used together for criminal purposes must be integrated—the so-called hybridisation of online criminality. Crime prevention strategies can also be enhanced by considering an internet user's points of contact as sites for enhanced regulatory cooperation. There will also be new opportunities to extend crime prevention measures by disrupting profit and support centres (Thomas & Bursztein 2015).

References

Ablon L, Libicki MC & Golay AA 2014. *Markets for cybercrime tools and stolen data hackers' bazaar.* Santa Monica CA: RAND National Security Research Division

Address Supporting Organization (ASO) 2015. *Address Supporting Organisation and the number resource organization*. ASO webpage https://aso.icann.org/about-the-aso/address-supporting-organization-and-the-number-resource-organization/

Al Helou J & Tilley S 2010. *Multilingual web sites: Internationalized domain name homograph attacks.* New York City: Institute of Electrical and Electronics Engineers (IEEE) http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=5623562

Alperovitch D & MacFarlane R 2008. *Anti-phishing best practices recommendations for registrars*. Lexington MA: Anti-Phishing Working Group (APWG) http://docs.apwg.org/reports/APWG_RegistrarBestPractices.pdf

Anderson R et al. 2013. Measuring the cost of cybercrime, in Böhme R (ed), *The Economics of Information Security and Privacy.* Berlin: Springer-Verlag: 265–300

Business Wire 2011. New phishing tactic emerges at one of world's largest payment processors. *Business Wire* 10 February http://www.businesswire.com/news/home/20110210006567/en/Phishing-Tactic-Emerges-World%E2%80%99s-Largest-Payment-Processors

US Federal Trade Commission 2013. FTC targets computer support scams. *Information Management Journal* 47(1) 12

RT News 2015. Swedish court orders Pirate Bay key domains seized. *RT News* 19 May https://www.rt.com/news/260161-sweden-court-pirate-bay/

Anthony S 2014. Brace for the BGPocalypse: Big disruptions loom as Internet overgrowth continues. *Extremetech* 13 August http://www.extremetech.com/extreme/187954-brace-for-the-bgpocalypse-big-disruptions-loom-as-internet-overgrowth-continues

Anti-phishing working group 2015. *APWG phishing attack trend reports*. APWG Resources webpage http://www.antiphishing.org/resources/apwg-reports/

Armin J et al. 2015. 2020 Cybercrime economic costs: No measure, no solution. *10th International Conference on Availability, Reliability and Security* IEEE 701-710

Asia Pacific Network Information Centre 2015a. *APNIC serves the Asia Pacific region*. https://www.apnic.net/about-APNIC/organization/apnics-region

Asia Pacific Network Information Centre 2015b. *Root servers—FAQs*. https://www.apnic.net/get-ip/faqs/rootservers

Atkinson RD et al. 2010. *The Internet economy 25 years after .com: Transforming commerce and life*. Washington DC: The Information Technology & Innovation Foundation

Attalah A 2015. Celebrating the rise of the modern Internet: The first dot com domain name turns 30. *ICANN Blog* https://www.icann.org/news/blog/celebrating-the-rise-of-the-modern-Internet-the-first-dot-com-domain-name-turns-30

au Domain Administration (auDA) 2012a. *auDA Board response to the independent review of the governances of .au*. http://www.auda.org.au/pdf/wcl-board-response.pdf

au Domain Administration (auDA) 2012b. *Domain name eligibility and allocation policy rules for the open 2LDs*. http://www.auda.org.au/policies/2012-04/

au Domain Administration (auDA) 2012c. *Accountability and transparency framework*. http://www.auda.org.au/pdf/auda-atf-2012.pdf

au Domain Administration (auDA) 2013. *Information Security Standard (ISS) for all auDA accredited registrars*. http://www.auda.org.au/policies/2013-03/

au Domain Administration (auDA) 2014. *DNSSEC Policy and Practice Statement (DPS) for the .au domain*. http://www.auda.org.au/assets/2014-08.pdf

auDA Foundation 2015. *About the auDA Foundation*. http://www.audafoundation.org.au/about-us/

Baloch FK & Cusack B 2012. A discussion on Internet governance. Paper to the Fourth International Conference on Computational Aspects of Social Networks, Sao Paolo, Brazil, 21–23 November

Batty J 2015. IBM expands reach to African entrepreneurs with innovation space @ iHub. IBM Media Release 25 July. Available at http://www.prnewswire.com/news-releases/ibm-expands-reach-to-african-entrepreneurs-with-innovation-space--ihub-300118750.html

Beebe NL & Rao VS 2005. Using situational crime prevention theory to explain the effectiveness of information systems security. *Proceedings of the 2005 SoftWars Conference* Las Vegas NV http://faculty.business.utsa.edu/nbeebe/pubs/beebe%20and%20rao%202005_using%20scp%20theory%20to%20explain%20infosec%20levels%20v2d.pdf

Berkens M 2015. The domain name 588.com sells for $1 million dollars. *The Domains* 21 September. http://www.thedomains.com/2015/09/21/the-domain-name-588-com-sells-for-1-million-dollars/

Brenner SW & Schwerha IV JJ 2004. Introduction—Cybercrime: A Note on International Issues. *Information Systems Frontiers* 6(2): 111–114

Brenner SW 2007. Cybercrime jurisdiction. *Crime Law and Social Change* 46: 189–206

Broadhurst R, Grabosky P, Alazab, M & Chon S 2014. Organizations and cyber crime: An analysis of the nature of groups engaged in cyber crime. *International Journal of Cyber Criminology* 8(1) 1–20

Brooks-Pollock T 2014. Is the Internet full? Major sites brought down by technical problems. *Sydney Morning Herald* 13 August

Brown C 2015. Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice. *International Journal of Cyber Criminology* 9(1) 55–119

Burt D, Kleiner A, Nicholas J P & Sullivan K 2014. *Cyberspace 2025: Today's decisions, tomorrow's terrain*. Redmond WA: Microsoft Corporation http://download.microsoft.com/download/C/7/7/C7775937-748E-4E95-85FB-24581F16B588/Cyberspace%202025%20Today%E2%80%99s%20Decisions,%20Tomorrow%E2%80%99s%20Terrain.pdf

Bush R & Meyer D 2002. Some Internet architectural guidelines and philosophy. *Request for comments 3439* The Internet Society https://www.ietf.org/rfc/rfc3439.txt

Card SK, Moran TP & Newell A 1983. *The psychology of human-computer interaction.* Mahwah NJ: Lawrence Erlbaum Associates Inc

Center for Strategic and International Studies 2014. *Net losses: Estimating the global cost of cybercrime: Economic impact of cybercrime II.* Santa Monica CA: Intel Security http://www.mcafee.com/au/resources/reports/rp-economic-impact-cybercrime2.pdf

Chabinsky SR 2010. *The cyber threat: Who's doing what to whom?* Washington DC: FBI GovSec/FOSE Conference 23 March https://www.fbi.gov/news/speeches/the-cyber-threat-whos-doing-what-to-whom

Chaudhary N & Surolia J 2015. A survey on peer to peer system applications. *International Journal of Innovative Computer Science & Engineering* 2(1) 16–20

Cheung S 2006. Denial of service against the domain name system. *IEEE security & privacy* 4(1) 40–45

Choi K. 2011. Cyber-routine activities: Empirical examination of online lifestyle digital guardians and computer-crime victimization, in Jaishankar K (ed), *Cyber criminology: Exploring Internet crime and criminal behaviors.* Boca Raton: CRC Press: 229–253

Choice 2014. *Submission to competition policy review issues paper*. Marrickville: Choice. http://competitionpolicyreview.gov.au/files/2014/06/CHOICE.pdf

Christie AF, Gloster J, Kadarusman J & Lau D 2014. *auDA overview of panel views on selected auDRP questions: First Edition*. http://www.auda.org.au/policies/audrp/audrp-overview/

Cichonski P, Millar T, Grance T & Scarfone K 2012. *NIST Special Publication 800-83: Computer security incident handling guide: recommendations of the National Institute of Standards and Technology* (NIST). Gaithersburg MD: NIST

Clark G & Phillips A 2008. *Inside book publishing.* 4th Edition Abingdon Oxon: Routledge

Clarke RV 1997. Situational crime prevention: successful case studies (2nd ed). Albany: Harrow and Heston Publishers.

Clarke RV 1995. Situational crime prevention. *Crime and Justice* 19: 91–150

Clough J 2010. *Principles of cybercrime.* Cambridge: Cambridge University Press

Cohen LE & Felson M 1979. Social change and crime rate trends: A routine activity approach. *American Sociological Review* 44(4): 588–608

Commonwealth Secretariat 2014. Report of the Commonwealth Working Group of Experts on Cybercrime. *Commonwealth Law Bulletin* 40(3): 502–561

Copyright Law Review Committee 1988. *The importation provisions of the Copyright Act (1968).* Canberra: Attorney-General's Department

Council of Europe Treaty Office 2016. *Details of Treaty No. 185 Convention on Cybercrime* https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

Country Code Names Supporting Organisation (CCNSO) 2015. *CCNSO About*. CCNSO webpage http://ccnso.icann.org/about

Cuff JH 1997. Domain-name game pits ant against army. *The Globe and Mail* 6 December

Cuomo J 2015. Back on the chain gang. *IBM developerWorks blog* 22 September https://www.ibm.com/developerworks/community/blogs/gcuomo/entry/Back_on_the_Chain_Gang?lang=en

Cybertelecom 2014a. *Definition of Internet*. webpage http://www.cybertelecom.org/notes/Internet_definition.htm

Cybertelecom 2014b. *Will the real Internet please stand up?* http://www.cybertelecom.org/notes/internetreal.htm

DeNardis L 2012. Hidden levers of Internet control: An infrastructure-based theory of Internet governance. *Information Communication & Society* 15(5): 720

Detica BS & London Metropolitan University 2012. *Organised crime in the digital age.* BAE Systems Detica [source no longer accessible online]

De Vey Mestdagh CN & Rijgersberg RW 2007. Rethinking accountability in cyberspace: a new perspective on ICANN. *International Review of Law Computers and Technology* 21(1): 27–38

Dow PT 2010. *Union county man pleads guilty to stealing valuable Internet domain name.* New Jersey: Office of the Attorney General http://www.nj.gov/oag/newsreleases10/pr20101213a.html

Ekstrand E 2013. *A domain name is neither an object nor an instrument of crime.* https://www.iis.se/english/blog/a-domain-name-is-neither-an-object-nor-an-instrument-of-crime/

Elkind P 2015. Inside the hack of the century. *Fortune* 1 July http://fortune.com/sony-hack-part-1/

EUROPOL 2014. *Internet organised crime threat assessment (IOCTA) 2014*. The Hague: EUROPOL

EUROPOL 2015. *Internet organised crime threat assessment (IOCTA) 2015.* The Hague: EUROPOL

Evans D 2011. *The Internet of things: How the next evolution of the Internet is changing everything*. San Jose CA: CISCO

Fahey PM & Murphy SS 2009. The brave new world of policing trademarks. *Intellectual Property Litigation* 20(2): 1–4

Felson M, Clarke RVG & Britain G 1998. *Opportunity makes the thief: Practical theory for crime prevention*. Police Research Series Paper 98 London: Home Office

Floridi L 2014. *The fourth revolution.* Oxford: Oxford University Press

Gallagher S 2012. *How Anonymous plans to use DNS as a weapon.* 9 March http://arstechnica.com/business/2012/03/how-anonymous-plans-to-use-dns-as-a-weapon/

Geisendörfer F 2006. *Hacking a commercial airport WLAN*. 21 August http://debuggable.com/posts/hacking-a-commercial-airport-wlan:480f4dd5-50a0-40c6-aa60-4afccbdd56cb

Generic Names Supporting Organization (GNSO) 2016. Final status report and recommendations of the GAC-GNSO Consultation Group on GAC Early Engagement in GNSO Policy Development Processes GNSO Webpage https://www.google.com/url?q=https://gnso.icann.org/en/drafts/gac-status-report-rec-10oct16-en.pdf&sa=U&ved=0ahUKEwizhqrtqbHQAhWHJ5QKHbjMAsIQFggIMAE&client=internal-uds-cse&usg=AFQjCNHARaGi2QIRJRKt6PVTvZ4BnTotHw

Gersch J 2007. Protecting the DNS with DNSSEC. *FSTC Innovator* 2(1): 5–9

Godfread P & Dorrain K 2010. Developments in domain names. *Business Lawyer* 66(1): 221–229

Gont F 2008. *Security assessment of the Internet Protocol version 4*. London: Centre for the Protection of National Infrastructure

Goodin D 2014. Microsoft drops case that severed DNS hosting for millions of No-IP nodes: No-IP didn't knowingly harbor botnet operators targeted in takedown MS declares. *Ars Technica* 10 July

Gordon S & Ford R 2006. On the definition and classification of cybercrime. *Journal in computer virology* 2: 13–20

Haggard S & Lindsay JR 2015. North Korea and the Sony hack: Exporting instability through cyberspace. *Asia Pacific Issues* 117

Hajkowicz S, Cook H & Littleboy A 2012. *Our future world, global megatrends that will change the way we live: The 2012 revision.* Canberra: CSIRO

Hill JF 2012. *Internet fragmentation: Highlighting the major technical governance and diplomatic challenges for US policy makers*. Cambridge MA: John F. Kennedy School of Government Harvard University

Hill R 2013. *Information document: Defining the Internet*. Geneva: World Telecommunications/ICT Policy Forum. https://www.itu.int/md/S13-WTPF13-INF-0008/en

Holt TJ & Bossler AM 2014. An assessment of the current state of cybercrime scholarship. *Deviant Behavior* 35(1): 20–40

House of Commons Home Affairs Committee 2013. *e-crime*. London: Parliament House

Hu Y, Xi C & Bose I 2013. Cybercrime enforcement around the globe. *Journal of Information Privacy and Security* 9(3): 34-52

Huston G 2014. BGP in 2013. *The ISP Column.* January http://www.Internetsociety.org/sites/default/files/bgp2013.pdf

Internet Corporation for Assigned Names and Numbers (ICANN) 2001. *ccTLD Sponsorship Agreement (.au)* Washington DC: ICANN

Internet Corporation for Assigned Names and Numbers (ICANN) 2007. *Factsheet: Root server attack on 6 February 2007.* ICANN webpage https://www.icann.org/en/system/files/files/factsheet-dns-attack-08mar07-en.pdf

Internet Corporation for Assigned Names and Numbers (ICANN) 2012. *ICANN organizational chart*. ICANN webpage https://www.icann.org/resources/pages/chart-2012-02-11-en

Internet Corporation for Assigned Names and Numbers (ICANN) 2012. *What does ICANN do?* ICANN webpage https://www.icann.org/resources/pages/what-2012-02-25-en

Internet Corporation for Assigned Names and Numbers (ICANN) Security and Stability Advisory Committee (SSAC) 2008. *SSAC Advisory on Fast Flux Hosting and DNS* SAC 025 https://www.icann.org/en/system/files/files/sac-025-en.pdf

Internet Corporation for Assigned Names and Numbers (ICANN) Generic Names Supporting Organization (GNSO) 2015. *PDP on Next-Generation gTLD Registration Directory Service (RDS)* http://gnso.icann.org/en/group-activities/active/rds

International Olympic Committee (IOC) 2013. *Olympic marketing fact file: 2013 Edition.* IOC

International Telecommunications Union (ITU) 2014. World telecommunication/ICT development report 2010: Target 9. *Monitoring the WSIS targets - A mid-term review* Geneva: ITU 271–325

International Telecommunications Union (ITU) 2015. *The state of broadband 2015*. Geneva: ITU

Internet.nl 2015. *Internet standards*. Leidschendam: Internet.nl https://en.Internet.nl/standards/

Internet Society 2014a. *BGP Hijacker Steals Bitcoins*. Internet Society webpage http://www.Internetsociety.org/deploy360/blog/2014/08/bgp-hijacker-steals-bitcoins/

Internet Society 2014b. *Securing BGP*. Internet Society webpage http://www.Internetsociety.org/deploy360/securing-bgp/

Islam S 2015. An algorithm for electronic money transaction security (three layer security): A new approach. *International Journal of Security and Its Applications* 9(2): 203–214

Jacobson V, Smetters DK, Thornton JD, Plass M, Briggs N & Braynard R 2012. Networking named content. *Communications of the ACM* 55(1): 117–124

Jakobsson M 2012. *The death of the Internet*. Hoboken NJ: John Wiley & Sons

Jorna P 2016. *Australasian Consumer Fraud Taskforce: Results of the 2014 online consumer fraud survey*. Research Report no 1. Canberra: Australian Institute of Criminology. http://www.aic.gov.au/publications/current%20series/rr/rr001.html

Kahn RE & Cerf VG 1999. *What Is The Internet (And What Makes It Work)*, Reston, VA: Corporation for National Research Initiatives http://www.cnri.reston.va.us/what_is_internet.html

Karrenberg D 2010. DNSSEC: Securing the global infrastructure of the Internet. Network Security (6): 4–6

Ke C 2014. *Australian web threat landscape (2014): Observation of TorrentLocker attacks*. Irving TX: Trend Micro

Khanisa 2013. A Secure Connection: Finding the Form of ASEAN Cyber Security Cooperation *Journal of ASEAN Studies*, 1(1): 41–53

Khattak S et al. 2014. A taxonomy of botnet behavior detection and defense. *IEEE Communications Surveys & Tutorials* 16(2): 894–924

Kornblum J 1997. AlterNIC founder faces extradition. *CNET News* 14 November

Krishna A 2015. Blockchain: It really is a big deal. *Building a smarter planet: A smarter planet blog* 16 September http://asmarterplanet.com/blog/2015/09/blockchain-really-big-deal.html

Kristoff J. 2007. *Feb 6/7 2007 DNS Attack Recap (public archival version)*. DNS-Operations meeting [Powerpoint presentation] https://www.dns-oarc.net/files/dnsops-2007/Kristoff-Feb07-attacks.pdf.

Krombholz K, Hobel H, Huber M & Weippl, E 2014. Advanced social engineering attacks. *Journal of Information Security and Applications* 17 July 1-10

Kruger LG 2013. *Internet governance and the domain name system: Issues for Congress.* Washington DC: Congressional Research Service

Lavorgna A 2015. Organised crime goes online: realities and challenges. *Journal of Money Laundering Control* 18(2): 153-168

Lawton G 2007. Stronger domain name system thwarts root-server attacks. *Computer* 40(5): 14–17

Li X 2008. The criminal phenomenon on the Internet: Hallmarks of criminals and victims revisited through typical cases prosecuted. *University of Ottawa Law & Technology Journal* 5(1–2)

Lim & Chen L 2015. *auDA and .au registrars work together to improve* security. Computerworld 4 November. http://www.computerworld.com.au/author/2147448560/jo-lim-lujia-chen-auda/articles

Lipinski L 2013.*Who runs the internet?* https://commons.wikimedia.org/wiki/File:Who-Runs-the-Internet-graphic.png#/media/File:Who-Runs-the-Internet-graphic.png. Used under Creative Commons Attribution Share-Alike 3.0 Australia

Litke P & Stewart J 2014. *BGP hijacking for cryptocurrency profit.* http://www.secureworks.com/cyber-threat-intelligence/threats/bgp-hijacking-for-cryptocurrency-profit/ Atlanta GA: Dell Secureworks

Lu C, Jen, W, Chang W & Chou S 2006. Cybercrime & cybercriminals: An overview of the Taiwan experience. *Journal of Computers* 1(6): 11–18

Lusthaus J 2012. Trust in the world of cybercrime. *Global Crime* 13(2): 71–94

Mackey TK & Liang BA 2013. Pharmaceutical digital marketing and governance: Illicit actors and challenges to global patient safety and public health. *Globalization and Health* 9(1): 45

MacLean D 2004. Herding Schr□dinger's Cats: Some conceptual tools for thinking about Internet governance. In *Background Papers for the ITU Workshop on Internet governance.* Geneva: ITU https://www.itu.int/osg/spu/forum/intgov04/contributions/itu-workshop-feb-04-internet-governance-background.pdf

Macnair E 2008. Blacklists will be swamped by domain name explosion. *Financial Times* 22 September http://www.ft.com/cms/s/0/2f172f76-84a1-11dd-b148-0000779fd18c.html#axzz3ti1BGaCV

Malby S et al. 2013. *Comprehensive study on cybercrime*. New York City: United Nations Office on Drugs and Crime

Marks P 2010. Info pirates seek an alternative Internet. *New Scientist* 6 December

McCarthy K 2015a. So who just bought the rights to .blog for $20 million? A chap living in Panama. *The Feed* 13 February

McCarthy K 2015b. US government tweaks Internet handover—1 October 2016. *The Register* 17 August

McCombie SJ 2011. *Phishing the long line: Transnational cybercrime from Eastern Europe to Australia*. Sydney: Macquarie University [PhD thesis]

McGillivray RJ & Lieske SC 2001. Webjacking. *Computer and Internet Lawyer* 18(7) 1

McGuire M 2012. *Organised crime in the digital age*. London: John Grieve Centre for Policing and Security [source not accessible online]

McNamara P 2006. Can't find a domain name? Here's why. *Network World* 28 April

Meisner J 2012. Microsoft disrupts the emerging Nitol botnet being spread through an unsecure supply chain. *Microsoft Blog* 13 September http://blogs.microsoft.com/blog/2012/09/13/microsoft-disrupts-the-emerging-nitol-botnet-being-spread-through-an-unsecure-supply-chain/#sm.0000fl3y86ulde2hzps1ednvhpohx

Messmer E 2009. Fighting domain name abuse. *Network World* 21 September

Microsoft Corporation 2014. *Microsoft Corporation v Mutairi and others: Brief in support of application.* United States District Court: District of Nevada

Microsoft Corporation 2014. *DNSEC.* Redmond WA: Microsoft Corporation https://technet.microsoft.com/en-au/library/jj200221(d=printer).aspx?f=255&MSPPError=-2147217396

Mockapetris P 1983. Domain names - Concepts and facilities *Request for comments 882* The Internet Society https://tools.ietf.org/html/rfc1034

Molnar LV 2005. Who Owns "Invisible. com,"and "Whois" Disappearing? A Practitioner Looks for Answers. *Res Gestae* 48(26)

Morgan A, Boxall H, Dossetor K & Anderson J 2012. *Effective crime prevention interventions for implementation by local government*. Research and Public Policy Series no 120. Canberra: AIC http://aic.gov.au/publications/current%20series/rpp/100-120/rpp120.html

Moore T & Clayton R 2007. Examining the impact of website take-down on phishing. In *Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit.* Pittsburgh, PA: APWG 1–13

Mueller ML 2002. *Ruling the root: Internet governance and the taming of cyberspace*. Cambridge: MIT Press

Murdoch SJ & Roberts H 2013. *Internet censorship and control*. New York City: IEEE Computer Society

National Science Foundation 2015. NSF *Future Internet Architecture Project*. http://www.nets-fia.net/.

National Telecommunications Information Administration (NTIA) 2015. *Report on the transition of the stewardship of the Internet Assigned Numbers Authority (IANA) functions*. Washington DC: NTIA

Naziris Y 2014. 'A Tale of Two Cities' in three themes–A critique of the European Union's approach to cybercrime from a 'power' versus 'rights' perspective. *European Criminal Law Review* 3(3): 319–354

Office of Foreign Assets Control (OFAC) 2012. *Iranian Transactions Regulations (31 C.F.R. Part 560) Interpretive guidance and statement of licensing policy on Internet freedom in Iran.* Washington DC: OFAC

Pare DJ 2003. *Internet governance in transition: Who is the master of this domain?* Lanham MD: Rowman and Littlefield Publishers

Parker C 2007. DA: No crime in domain name tiff: Controller hopeful hoarded potential web sites of opponent. *Morning Call* B1 23 August

Parsons B 2006. *The add/drop scheme. How millions of .COM names are used but never paid for*. 21 April http://www.bobparsons.me/archive_article.php?entry_id=116

Pavan E 2012. *Frames and connections in the governance of global communications: A network study of the Internet Governance Forum.* Plymouth: Lexington Books

Piscitello D 2012. *Guidance for preparing domain name orders seizures & takedowns.* Los Angeles CA: ICANN

Piscitello D & Rasmussen R 2008. *Making waves in the phishers safest harbor: Exposing the dark side of subdomain registries.* APWG

Ponemon Institute 2015. *State of cybersecurity in local state & federal government.* Traverse City MI: Ponemon Institute

Pongas G 2014. *Consumer alert: WHOIS verification phishing scams hit Australia*. Melbourne: AusRegistry

Rafiee H, von Lowis M & Meinel C 2012. IPv6 deployment and spam challenges. *Internet Computing* IEEE 16(6): 22–29

Rasmussen R & Vixie P 2015. *Surveying the DNS threat landscape*. Tacoma WA: IID (Internet Identity)

Ravali P 2015. A comparative evaluation of OSI and TCP/IP models. *International Journal of Science and Research* 4(7): 514–521

Roache-Turner D 2013. *Review letter to auDA dated 31 January* Geneva: World Intellectual Property Organization Arbitration and Mediation Center

Rodenbaugh M 2009. ICANN policy developments on abusive domain name registrations. *IP Litigator* 15(5): 9

Rutkowski AM 2004. The Internet: Policy and governance, in Singh M (ed) *The practical handbook of Internet computing* Boca Raton: CRC Press

Saharan P 2007. *Host naming and URL conventions*. TKK T-110.5290 Seminar on Network Security 11–12 October http://www.tml.tkk.fi/Publications/C/25/papers/Saharan_final.pdf

Simon CL 2006. *Launching the DNS war: Dot-com privatization and the rise of global Internet governance*. Coral Gables: University of Miami [Dissertation]

Simon R 2015. Cybercriminals are misappropriating businesses' web addresses; As a result customers can't find the real companies on the web. *The Wall Street Journal* 12 March

Sloan P 2012. Meet the "Mann" who registered 14,962 domains in 24 hours. *C/Net* 21 April http://www.cnet.com/au/news/meet-the-mann-who-registered-14962-domains-in-24-hours/

Smith RG 2015. Trajectories of Cybercrime, in Smith RG, Cheung RC-C. & Lau LY-C (eds), *Cybercrime risks and responses: Eastern and western perspectives* Basingstoke: Palgrave Macmillan 13-34

Smith RG 2010. The development of cybercrime: An opportunity theory approach, in Lincoln R & Robinson S (eds), *Crime over time* Newcastle upon Tyne: Cambridge Scholars Publishing 211-236

Speer D 2000. Redefining borders: The challenges of cybercrime. *Crime, law and social change* 34: 259-273

Standing Committee on Infrastructure & Communications 2010. *Hackers, fraudsters and botnets: Tackling the problem of cyber crime*. Canberra: Parliament House

Standing Committee on Infrastructure & Communications 2013. *At what cost? IT pricing and the Australia tax*. Canberra: Parliament House

Storm D 2010. P2P DNS to take on ICANN after US domain seizures. *Computerworld* 30 November

Strickling LE 2014. *Testimony of Assistant Secretary Strickling*. Subcommittee on courts, intellectual property and the Internet 10 April 2014. Washington DC: NTIA

Sui D, Caverlee J & Rudesill DS 2015. *The Deep Web and the Darknet: A look inside the Internet's massive black box*. Washington DC: Woodrow Wilson International Center for Scholars STIP 3

Symantec, 2013. *Norton Report: Total Cost of Cybercrime in Australia amounts to A$1.06 billion* media release 13 October www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=norton-report-2013

Tropina T 2012. The Evolving Structure of Online Criminality: How cybercrime is getting organised *Eucrim* 4: 158-164

Thibodeau P 2007. Domain Name System shows signs of stress. *Computerworld* 16 April

Thomas K & Bursztein E 2015. New research: The underground market fueling for-profit abuse. *Google online security blog* 24 September 2015

Thomas K et al. 2015. Framing dependencies introduced by underground commoditization. *Workshop on the Economics of Information Security* Delft University of Technology http://static.googleusercontent.com/media/research.google.com/en/us/pubs/archive/43798.pdf

Thomas M & Mohaisen A 2014. Measuring the leakage of onion at the root. *WPES '14: Proceedings of the 13th Workshop on privacy in the electronic society* New York City: Association for Computational Machinery (ACM) 173–180

TrendLabs 2015. *The invisible becomes visible: Trend Micro Security predictions for 2015 and beyond* Irving TX: Trend Micro Security

United States Department of Justice 2004. *Special report on "phishing."* Washington DC: DOJ

United States Government Accountability Office (GAO) 2005. *Report to the Subcommittee on courts the Internet and intellectual property House of Representatives: Internet management— prevalence of false contact information for registered domain names*. Washington DC: GAO

Vold G, Bernard T & Snipes J 2002. *Theoretical Criminology* (5th ed). New York City: Oxford University Press

Wall DS 2005. The Internet as a conduit for criminals, in Pattavina A (ed), *Information Technology and The Criminal Justice System* Thousand Oaks CA 77-98

Wall DS 2007. *Cybercrime: The transformation of crime in the information age.* Cambridge: Polity Press

Wall DS 2015. Dis-organised crime: Towards a distributed model of the organization of cybercrime. *The European Review of Organised Crime* 2(2): 71–90

Weber RH Grosz M & Weber R 2010. *Shaping Internet governance: Regulatory challenges.* Berlin: Springer-Verlag

Westlake Consulting Limited 2011. *Independent Review of the Governance of .au*. Report to The Board of Directors of .au Domain Administration Limited ('auDA')

Williams ML 2016. Guardians upon high: An application of routine activities theory to online identity theft in Europe at the country and individual level. *British Journal of Criminology* 56: 21–48 (advance access publication 27 April 2015)

Wortley R 2001. A classification of techniques for controlling situational precipitators of crime. *Security Journal* 14(4): 63–82

Yoo CS 2013. Protocol layering and Internet policy. *University of Pennsylvania Law Review* 161: 1,707–1,771

Yu R 2013. "Times" attack shows soft spots in cyberdefense: Domain name systems vulnerable. *USA TODAY* 28 August

Zhang L et al. 2014. Named data networking. *ACM SIGCOMM Computer Communication Review* 44(3): 66–73

AIC reports

Research Report

Australia's national research and knowledge centre on crime and justice

aic.gov.au