CIGI

CHATHAM HOUSE
The Royal Institute of International Affairs

Global Commission on Internet Governance

ourinternet.org

PAPER SERIES: NO. 8 — MARCH 2015

Understanding Digital Intelligence and the Norms That Might Govern It

David Omand

UNDERSTANDING DIGITAL INTELLIGENCE AND THE NORMS THAT MIGHT GOVERN IT

David Omand

CHATHAM HOUSE
The Royal Institute of International Affairs

Published by the Centre for International Governance Innovation and Chatham House.

CIGI

67 Erb Street West
Waterloo, Ontario N2L 6C2
Canada
tel +1 519 885 2444 fax +1 519 885 5450
www.cigionline.org

CHATHAM HOUSE
The Royal Institute of International Affairs

10 St James's Square
London, England SW1Y 4LE
United Kingdom
tel +44 (0)20 7957 5700 fax +44 (0)20 7957 5710
www.chathamhouse.org

TABLE OF CONTENTS

ABOUT THE GLOBAL COMMISSION ON INTERNET GOVERNANCE

The Global Commission on Internet Governance was established in January 2014 to articulate and advance a strategic vision for the future of Internet governance. The two-year project conducts and supports independent research on Internet-related dimensions of global public policy, culminating in an official commission report that will articulate concrete policy recommendations for the future of Internet governance. These recommendations will address concerns about the stability, interoperability, security and resilience of the Internet ecosystem.

Launched by two independent global think tanks, the Centre for International Governance Innovation (CIGI) and Chatham House, the Global Commission on Internet Governance will help educate the wider public on the most effective ways to promote Internet access, while simultaneously championing the principles of freedom of expression and the free flow of ideas over the Internet.

The Global Commission on Internet Governance will focus on four key themes:

- enhancing governance legitimacy — including regulatory approaches and standards;
- stimulating economic innovation and growth — including critical Internet resources, infrastructure and competition policy;
- ensuring human rights online — including establishing the principle of technological neutrality for human rights, privacy and free expression; and
- avoiding systemic risk — including establishing norms regarding state conduct, cybercrime cooperation and non-proliferation, confidence-building measures and disarmament issues.

The goal of the Global Commission on Internet Governance is two-fold. First, it will encourage globally inclusive public discussions on the future of Internet governance. Second, through its comprehensive policy-oriented report, and the subsequent promotion of this final report, the Global Commission on Internet Governance will communicate its findings with senior stakeholders at key Internet governance events.

www.ourinternet.org

ABOUT THE AUTHOR

Sir David Omand was the first UK security and intelligence coordinator from 2002 to 2005 as permanent secretary in the Cabinet Office. Previously, he was permanent secretary of the UK Home Office and director of Government Communications Headquarters (the UK signals intelligence and cyber-security agency). He has a degree in mathematics and theoretical physics and a master's in economics. He is a fellow of Corpus Christi College Cambridge and is senior independent director of Babcock International Group PLC. His book *Securing the State* is published by Hurst (United Kingdom) and Oxford University Press (United States).

ACRONYMS

DGSE	Direction générale de la security extérieure
DPI	deep packet inspection
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
FBI	Federal Bureau of Investigation
GCHQ	Government Communications Headquarters
IP	Internet Protocol
NATO	North Atlantic Treaty Organization
NSA	National Security Agency
SIGINT	signals intelligence
UNSC	United Nations Security Council
WMD	weapons of mass destruction

EXECUTIVE SUMMARY

This paper[1] describes the nature of digital intelligence and provides context for the material published as a result of the actions of National Security Agency (NSA) contractor Edward Snowden. Digital intelligence is presented as enabled by the opportunities of global communications and private sector innovation and as growing in response to changing demands from government and law enforcement, in part mediated through legal, parliamentary and executive regulation. A common set of organizational and ethical norms based on human rights considerations are suggested to govern such modern intelligence activity (both domestic and external) using a three-layer model of security activity on the Internet: securing the use of the Internet for everyday economic and social life; the activity of law enforcement — both nationally and through international agreements — attempting to manage criminal threats exploiting the Internet; and the work of secret intelligence and security agencies using the Internet to gain information on their targets, including in support of law enforcement.

INTRODUCTION

The Snowden material has exposed — to unprecedented and uncomfortable international gaze — the world of digital intelligence and the technical success of US agencies and those of its close intelligence allies in adapting their processes to the opportunities the Internet provides. The protection of personal information from unlawful exploitation, and the legality, proportionality and adequacy of regulation of digital intelligence access and intelligence sharing have become major international political issues. This paper looks at the dynamic interaction between demands from government and law enforcement for digital intelligence, and at the new possibilities that digital technology has opened up for meeting such demands. Inevitably, the paper has an "Anglo-Saxon" bias, given that American influence on the Internet so far has been so great, an understandable situation given the origins of the Internet and the sources of investment and innovation that have driven it thus far. The Snowden allegations have highlighted what many nations see as this US "home field" advantage in economic terms, as well as in the scale and reach of modern digital intelligence giving the United States a "hard power" advantage. The alleged range of targets of US intelligence included the chancellor of Germany and the president of Brazil and set off firestorms of diplomatic protests led by those nations. The disclosures also put the long-standing "Five Eyes" (the United States, the United Kingdom, Canada, Australia and New Zealand) partnership in signals intelligence (SIGINT) under unparalleled scrutiny and became an issue in the New Zealand general election. The debate in the European Union over personal privacy in a data-rich world in which the private sector harvests significant amounts of personal information was already complex,[2] but the Snowden allegations have made this and other international debates intense and at times toxic.[3] That, in turn, has led to some nations exploiting the issues for protectionist purposes to benefit their domestic industry in terms of data localization and procurement restrictions from US suppliers. Overall, the adequacy of the previous regimes of legal powers and governance arrangements is seriously challenged just at a time when the objective need for intelligence on the serious threats facing civil society is apparent. This paper suggests areas where it might be possible to derive international norms, regarded as promoting standards of accepted behaviour that might gain widespread, if not universal, international acceptance, for the safe practice of digital intelligence.

1 The contents of this paper and opinions given in it are the sole responsibility of the author in his capacity as visiting professor at King's College London. They should not be taken as an expression of the views of the British government, which continues neither to confirm nor deny allegations made in the media about the operational activity of British intelligence in the light of the material leaked by Edward Snowden.

2 Discussion of a controversial new draft European Union Regulation on Data Protection and a specific new Data Protection Directive for law enforcement continues. See http://ec.europa.eu/justice/data-protection/.

3 The European Parliament, for example, has called for suspension of the "safe harbour" arrangements for sharing data on European citizens with the United States and the suspension of the US/EU Terrorist Finance Tracking Programme that had generated significant intelligence, helping to detect terrorist plots and trace their authors.

ORIGINS OF DIGITAL INTELLIGENCE

The interception of written communications — and, when necessary, their decipherment — and the monitoring of patterns of communication are practices of considerable antiquity. SIGINT derived from electromagnetic emissions developed during World War II and the Cold War into a recognized major intelligence capability. The Internet is a major source of comparable intelligence power today.

Recent years have seen the development of powerful tools of digital intelligence driven by the dynamic interaction of two coincidental developments: on the one hand, the increasing public, corporate and government use of the Internet and digital data, making possible an unprecedented supply of information about individuals and their activity, movements and location; and on the other hand, the evolution of national demands for intelligence on non-state actors, in particular for the United States and its allies on terrorists after the attacks on New York and Washington, DC on September 11. Supply and demand have interacted dynamically with technological advances and popular apps, making possible new opportunities for accessing information, helping to meet insistent demands for information about suspects that have in turn driven the development of more ingenious uses of digital data to derive intelligence. This dynamic interaction is set to continue.

SUPPLY-SIDE CONSIDERATIONS

The digital revolution has wrought profound changes in the technological environment in which intelligence agencies operate, in particular, the growth in global communications with the network of packet-switched networks[4] that comprises the Internet and carries the World Wide Web. The adoption of open Internet and network protocols allowed rapid innovation in applications attractive to business and consumers alike and the development of public key cryptography[5] made online monetary transactions feasible. The resulting popularity of the Internet as a means of personal communication as well as business, the development of the Web (and, more recently, the so-called dark Web[6]) and the ability to cheaply transfer, store and mine digital data have all transformed the opportunities for obtaining secret intelligence. Understanding the changing nature of the potential *supply* of intelligence from the Internet thus involves recognizing the potential represented by:

- the digitization of communications and the advent of packet-switched networks to carry all forms of digital communications;
- the availability of relevant data (such as communications traffic records and Internet metadata[7]) already in digital form, which means that it is economically viable to store data in bulk and to examine it and combine it with other datasets to identify matches and patterns of interest to an intelligence analyst seeking to discover new leads on a target;
- the growth in voice and video communications carried over the Internet, with Voice over Internet Protocol applications (such as Skype and FaceTime) replacing many terrestrial telephone calls using subscriber dialing;
- the widespread use of mobile devices to access the Internet and their impact on the interception of "data in motion";[8]
- the impact of cheap data storage and processing on the digitization of back offices of both companies and government departments (such as passports, national insurance records, bank account details, airline reservations and so on), making "stored data" a valuable source of digital intelligence;
- the use by governments and armed forces of Virtual Private Networks using the Internet Protocol (IP) carried on the Internet and mixed with other packet-switched communications, rather than traditional

4 Packet switching describes the type of digital communication network in which relatively small units of data called packets are routed by computers (servers) through a network based on the destination address contained within each packet, normally directed to take the least congested and therefore cheapest route at that instant.

5 Public key encryption was first discovered by mathematicians at the UK signals intelligence agency, Government Communications Headquarters (GCHQ). See www.gchq.gov.uk/history/Pages/Recent-History-technology-challenges.aspx.

6 The dark Net, or dark Web, describes networks that are only accessible by trusted peers, with measures to ensure that the addresses and identities of participants are not discoverable, for example, to allow markets for narcotics and other criminal transactions to be operated with transactions in Bitcoin.

7 Packet-switched networks rely on "headers" being attached to data packets that identify their destination and routing and enable the entire message to be recomposed on arrival, even when individual packets have taken different routes through cyberspace. Traffic data is normally defined by an analogy with old-fashioned telephone billing that lists who called whom, when, from where and for how long. The Internet age extends the metadata to include such information as the browsing history of an individual or their digitized list of contacts.

8 A useful, if crude, distinction can be drawn between intelligence agencies intercepting communications and information about communications — data in motion — and agencies accessing data held in digital data bases, including in the Cloud — stored data.

dedicated high-frequency/very high-frequency/ ultra high-frequency wireless networks;

- the commercial use of strong encryption in enabling secure financial transactions and communications and in securing mobile devices from unauthorized access;
- the use of a range of technologies that can provide locational data on mobile devices;
- the use of Cloud services both for storing consumer-related information and for enabling mobile devices to use advanced programs such as mapping, aerial photography and street views too large to be stored on the device itself; and
- the widespread use of social media, texting, tweeting and blogging, all of which may provide information on the identity and associations of suspects.

No doubt, in the near future, digital "wearables" will also be popularized as consumer goods (an example is the bracelet that takes pulse and heart rate measurements and links to the owner's mobile phone — and, in the future, possibly directly to the doctor's office to warn of impending trouble). In the future, the Internet will be connected to a wide range of other devices (the so-called "Internet of things" or, more recently, "the Internet of Everything"), again increasing the stock of information that is relatable to an individual and from which useful intelligence might be derived.

On the other hand, the Internet and its digital applications also offer added potential for those who wish to *hide* their communications:

- The huge growth in the volume of data[9] carried by global communications networks reduces the probability of interception of any given email, text or other message[10] and packet switching means that only parts of a message may be recovered. Microsoft has over a billion users of its Cloud services with 1.3 billion email addresses sending four billion emails a day and uploading 1.5 billion photographs a month. Skype calls via the Internet are taking up two billion minutes per day.
- There is a wide choice of social media platforms, chat rooms, drop boxes and other apps, not just the most well-known ones, and many are hosted overseas, complicating the surveillance task, especially if it becomes known which are less able to be accessed by the authorities.
- The provision of communications channels in multiplayer role games enables virtual "meetings" inside games.
- The availability to the user of very strong commercial encryption such as Pretty Good Privacy that, if implemented correctly, means that for all practical purposes the content of an encrypted message does not represent a cost-effective target for the authorities.
- The development of anonymizing software, such as Tor,[11] which hides the IP address of the user's device from an intercepting agency.
- The ease with which, given digital communications, steganography[12] can be used to conceal messages or malware even when the communication is intercepted.

The public is only now beginning to recognize — stimulated by the controversy over digital privacy that the Snowden affair has generated — the business model that makes the Internet economically viable, and cheap to the user, indeed largely free at the point of use. Personal information of users can be collected and monetized, and sold for marketing and other purposes. This complex metadata ecosystem has driven the massive take-up of easily available software applications (now universally just called apps) for mobile devices and the rapid adoption of social media (of which there are thousands of different variants available worldwide). Such developments have transformed the ease and variety of ways of interacting digitally between individuals and within groups, and have made multimedia ubiquitous — video, photograph, graphic and text all combined. A further relevant development has been the provision of Cloud services, not just for easily accessible data storage, but also to enable mobile devices to access very powerful software programs too large to fit on individual devices, such as search and inference engines able to recognize context and thus be faster and more efficient, translation to and from multiple languages and voice-activated inquiries. The benefits to the

9 According to an NSA document revealed by Snowden, the NSA touches about 1.6 percent of total Internet traffic, estimated at 1826 petabytes of information a day. However, of the 1.6 percent of the data, the document states that only 0.025 percent is actually selected for review, so the net effect is that NSA analysts look at 0.00004 percent of the world's traffic in conducting their mission (less than one part in a million) (Ball 2013).

10 Examples include financial and commodity market trading, streaming video services (such as Netflix, as well as educational services) and massively multiplayer online role-playing games.

11 Tor, or The Onion Router, was developed by the US Navy to make impractical the identification of the sender of communications traffic, and its use by dissidents under repressive regimes such as in Iran has been encouraged. It is now a main route to the criminal websites to be found on the dark Web.

12 The hiding of messages from plain sight, for example, concealed at very small scale beneath digitized photographs or graphics or in the code of instructions for a program.

consumer are faster, more appropriate responses to search engine requests, relevant "pop-up" advertisements on websites and apps and free or cheap services. The private sector is thus expert at harvesting, for its own commercial purposes, data on the Internet usage of its customers, which is of considerable interest to intelligence and law enforcement for the reasons explained in the demand section below.

DEMAND-SIDE CONSIDERATIONS

The basic purpose of intelligence is to improve the quality of decision making by reducing ignorance. Secret intelligence achieves that purpose in respect of information that others are trying their best to prevent from being discovered. The traditional requirements for secret intelligence drawn up by governments for their intelligence agencies were dominated by security concerns over potentially (or actually) hostile states. The priorities were acquiring intelligence on the military capabilities (organization, order of battle, equipment and doctrine) and intentions of states and their armed forces, and providing early warning of emerging threats. National security, including counter-intelligence and counter-subversion work, has been the staple diet of intelligence and security agencies around the world. These demands for military and diplomatic intelligence of course continue, in particular to support current military operations and where national enmities and rivalries persist. To a large degree, however, meeting even these traditional tasks nowadays requires, for the reasons stated earlier, access to and understanding of digital communications and Internet use.

Most intelligence services around the world have also experienced a sea change over the last decade toward helping improve decision making for the purpose of public safety and security. Agencies have increasingly been called upon to target individuals, so-called non-state actors, to help counter international and domestic terrorism, proliferation of weapons of mass destruction (WMD),[13] narcotics and people trafficking, pedophile networks and other serious international crime including, most recently, cybercrime. The emergence of al-Qaeda and violent jihadist groups as a global phenomenon has created widespread public concern in many nations and a need for governments to reassure their publics over their management of the terrorist threat. Digital intelligence has proved invaluable in providing leads, such as identifying the contacts of terrorist facilitators, part of an intelligence chain that can allow the disruption of a terrorist plot[14] and as a tool after an attack to identify others in the conspiracy.[15]

For many nations, such intelligence work is reflected in a broadening of how national security is perceived in terms of anticipating threats to everyday life in addition to the traditional preoccupation with defence from external attack.[16] This shift has been described[17] as that from "the Secret State" to "the Protecting State," where it is the direct security of the public rather than that of the institutions of the state that is the focus of national security. Some relevant implications of these changes in demand include the following:

- secret intelligence becoming (for the democracies at least) a legitimate and avowed arm of government, regulated by legislation;
- a wider "customer"[18] base for secret intelligence than in the past, including local as well as national police forces, border and immigration authorities, revenue and customs, and domestic homeland security planners;
- a much higher proportion of effort[19] than hitherto going on analysis relating to terrorists and other individuals of intelligence interest to establish their identities, associations, activities and intentions, movements, and financing;
- erosion, from the point of view of the customer, of intelligence of the traditional distinctions between domestic and overseas spheres for intelligence collection since, for example, a terrorist plot may well

13 Although there are many instances of states being behind proliferation of WMD, individuals have also been important, such as AQ Khan and his global commercial network of technology suppliers. See Corera (2006).

14 The director general of the British Security Service has publicly given credit to the invaluable nature of such intelligence that frustrated a number of terrorist attacks in the United Kingdom in the latter half of 2014, but has emphasized the "jigsaw" nature of the intelligence work (Parker 2015).

15 See www.theguardian.com/world/live/2015/jan/09/charlie-hebdo-manhunt-kouachi-terrorist-links-live-updates.

16 The United States, India, the United Kingdom, France, Switzerland, the Philippines and Singapore, to take a range of examples, have brought together at the highest levels responsibility for policy on external national security and internal domestic or "homeland" security (including the response to civil emergencies) into a National Security Council.

17 See, for example, Omand (2010).

18 The term customer is used in this paper to cover the varied recipients of intelligence reporting. The term does not imply the need for any financial relationship between customer and the supplier of intelligence.

19 For example, on September 11, 2001, only about 1,300 Federal Bureau of Investigation (FBI) agents, or six percent of the FBI's total personnel, worked on counterterrorism. By 2003, that had risen to 16 percent. By 2003, over 70 percent of British Security Service effort was devoted to countering terrorism. See National Commission on Terrorist Attacks (n.d.) and Manningham-Buller (2003).

have both domestic and external components, leads about which need to be brought together;[20]

- in both criminal and civil cases, the prosecution's use in court of evidence derived from intelligence and consequent issues over disclosure of sensitive operational details;
- the value of mutual sharing of intelligence-derived leads and tip-offs, and threat warnings with partners overseas to a much greater extent than in the past, both through police channels such as the International Criminal Police Organization and the European Police Office and between national intelligence agencies and counterterrorism analysis centres — this sharing now also includes the development of arrangements for supporting UN requirements for intelligence for their peacekeeping and peace enforcement missions;
- greater influence for the customers over intelligence collection priorities focused on intelligence reporting that could provide opportunities to take early action to protect the public or deployed armed forces, as against more traditional strategic intelligence analysis;
- especial interest in the identification (including biometrics) of individual suspects who are using the Internet under multiple aliases, and the geo-location in near-real time of individuals of counterterrorism interest; and
- the growth of interest in intelligence to support economic well-being, including anticipating key natural resource scarcities[21] and identifying corruption, fraud and detection of market rigging including by cyber means.

The growth in cyber threats, both malicious and criminally inspired, has made nations much more aware of the value of digital intelligence techniques to:

- help detect, classify and, where possible, attribute cyber attacks, including the theft of intellectual property;
- understand the nature of advanced persistent cyber threats (advanced since they involve exploiting vulnerabilities in software that firewalls will not detect, and persistent since the attacks will continue until there is a successful penetration) — such threats include the potential for disruptive cyber attacks on the critical national infrastructure and on systems essential for the effectiveness of military operations; and
- provide the means for designing and launching offensive cyber operations[22] to support military operations and for covert actions carried out in cyberspace.

THE RESULTING DIGITAL INTELLIGENCE ENVIRONMENT

The coincidence of the modern digital communications and storage revolution and the post-September 11 demands for intelligence on suspects and their networks will be familiar to all modern intelligence agencies. It is less a question of how many terrorist attacks, criminal plots and cyber attacks have been stopped because of specific interception of terrorist intent in their communications and much more the unique contribution digital intelligence sources make to the intelligence jigsaw and the painstaking process of "discovery" of terrorist cells and involved individuals. This dynamic interaction between supply and demand forms the background to the allegations of Edward Snowden[23] about the advanced digital intelligence capabilities of the NSA and its many overseas partners.[24]

Two issues have often been conflated in the subsequent controversies over the scale and intrusiveness of digital intelligence activity both in relation to international human rights and in intelligence activity apparently

20 A number of nations, including the United States, the United Kingdom, France and Germany, have created counterterrorism analysis centres where police and internal security and external communications intelligence analysts can work together to uncover terrorist plots, advise on threat warnings and alert states.

21 An example is the group of rare earth minerals essential for electronic devices used in the defence, alternative energy and communications industries, and where 97 percent of world production is in China (Chapple 2012).

22 A number of nations, including the United States and the United Kingdom, have admitted to seeking offensive cyber capabilities; others such as Russia, China and Iran have already implicitly demonstrated capabilities, either governmental or by so-called "patriotic hackers" based in those nations.

23 An indexed guide to the material published as a result of Edward Snowden's actions can be found at www.lawfareblog.com/catalog-of-the-snowden-stored/#.UuBEdxDTk2w, and commentary at www.schneier.com/blog/archives/2014/01/catalog_of_snow.html.

24 The long-standing Five Eyes partner agencies of the US NSA are the UK GCHQ, Canadian Communications Security Establishment, Australian Digital Signals Directorate and New Zealand Government Communications Security Bureau. In addition, Snowden has revealed networks of bilateral and multilateral digital intelligence relationships with countries such as the "SIGINT Seniors": the Five Eyes plus France, Germany, Sweden, Italy, Spain, Belgium, the Netherlands, Norway and Denmark, and others in Africa, South America and Asia, involving shared access to global communications and exchanges of technical information and techniques.

directed at friendly states.[25] The first issue concerns what legal authority there should be for the state to compel (and subsidize) an Internet company to create and retain digital records of customer activity and furnish the authorities with data about the use of the service. An example would be the issue of a subpoena or warrant to an Internet Service Provider or Internet company for access to data in the Cloud or real-time transmission. The second issue concerns the ability of intelligence agencies to collect digital data without the knowledge or cooperation of the companies, in other words, as classic secret intelligence collection activities. An example would be an intelligence survey using cyber exploitation to place secretly, without the assistance of a third party, a harvesting tool on a device or network to identify the members of a child abuse network.

After the first round of publicity over the Snowden material, US President Barack Obama was forced to order an immediate "blue ribbon" inquiry into the conduct of the NSA and, subsequently, to make a major public statement and publish for the first time his directive to the NSA[26] to govern SIGINT collection. The President's Commission and the US Privacy and Civil Liberties Oversight Board both aired arguments over the potential unconstitutionality of certain domestic collection programs. The US Congress has continued to debate reforms in the relevant intelligence legislation, but the outcome is uncertain.

In order to examine the implications of the Snowden allegations, the European Parliament is conducting its own inquiry into the alleged electronic mass surveillance of European citizens.[27] The United Kingdom is conducting several inquiries.[28] The German Bundestag has set up a special committee for broadly the same purpose. The German government has also announced that it will transfer its government e-services from the US carrier Verizon to the domestic provider, Deutsche Telekom, ostensibly for reasons of protecting the privacy of German citizens and fears of US intelligence access via US providers (Troianovski and Yadron 2014).[29] In 2014, the French government rapidly legislated to provide statutory legal authority for its ongoing interception activity under the *Loi de programmation militaire* adopted on December 10, 2013 by the French senate. This law enables the French secret services to intercept any electronic communication, under the direct authorization of the French prime minister or president. German legislation also allows electronic interception, but is much more restrictive.[30]

Whether the result of all this controversy and debate will be consistent, coherent and effective reform, or whether it will even be in the interests of the citizens concerned, much remains to be seen. The outcome of the different strands of investigation, inquiry and political debate following the Snowden affair may well be changes to tighten up the way many democratic nations regulate intrusive intelligence activity and legislate to protect personal data.[31] For some nations, learning about these advanced digital intelligence techniques will spur an effort to try to catch up, including increased monitoring of social media use by domestic publics. And, of course, there are major nations, such as Russia and China, that remain highly secretive about their national intelligence activity, and where it must be assumed that many of the techniques of intelligence access exposed by Edward Snowden are in regular use without the independent legal and parliamentary oversight mechanisms that are becoming common across democratic nations.

The Chinese government (along with a number of other governments) is reported as reappraising its reliance on major US Internet companies, concerns no doubt fuelled by the Snowden material.[32] And Western governments are, in parallel, examining their reliance on Chinese information technology suppliers as some of the methods of digital

25 Some care is needed in interpreting published material. The interception of the mobile telephone of Chancellor Angela Merkel of Germany was not denied, but the journalistic claims concerning the interception by NSA of large numbers of European telephone calls (for example, in France, Germany, Spain, Netherlands and Norway) turned out to be interception by the agencies of those nations themselves of calls overseas and shared with the United States. See Aid (2013).

26 See The White House (2014).

27 The evidence of Edward Snowden to the European Parliamentary inquiry can be found at www.europarl.europa.eu/document/activities/cont/201403/20140307ATT80674/20140307ATT80674EN.pdf.

28 A major review into interception is under way by the think tank, the Royal United Services Institute, at the request of the UK deputy prime minister. The UK government has also set up a statutory review to look at the capabilities and powers required by law enforcement and the security intelligence agencies, and the regulatory framework within which those capabilities and powers should be exercised. In the light of the Snowden material, the Intelligence and Security Committee of the UK Parliament has reported that the current powers of digital interception are essential, that the UK agencies operate at all times within human rights and national law, including applying the principles of proportionality and necessity, but that new consolidating legislation is now needed to provide much greater transparency for the citizen on how the law operates. Their report can be found at http://isc.independent.gov.uk/.

29 In practice, intelligence penetration has little to do with the citizenship of the network provider or the location of the data. Rather, it turns on the technical ability of the intelligence agency to penetrate the target.

30 See www.dw.de/germans-intercept-electronic-data-too-but-not-much/a-16909606.

31 See, for example, the 2013 draft EU directive, "Proposal for a Directive of the European Parliament of the Council Concerning Measures to Ensure a High Common Level of Network and Information Security across the Union," the draft EU regulation on data protection, at ec.europa.eu/justice/data-protection.

32 See, for example, http://seekingalpha.com/article/2387365-chinese-restricting-of-apple-microsoft-and-symantec-are-harbingers-of-reduced-growth and http://politics.slashdot.org/story/13/06/25/140232/chinese-media-calls-for-boycott-of-cisco2014.

intelligence become more generally known, including the United States and Australia excluding the Chinese company Huawei from critical national infrastructure-related bids.[33] The US Internet and technology companies themselves are busy reassuring their customers that their data will be made invulnerable to all unauthorized access — including the intelligence agencies of their own government. Behind this stance by the US companies lies the commercial reality that the Snowden disclosure of the scale of NSA access to communications carried by them risked hurting their business. Companies want to be able to say that their citizenship or the placement of their servers should not become a competitive disadvantage because of customer fears that they may be more amenable to or compliant with legal mandates to furnish information.

Although approximately 40 percent of the world population already has access to the Internet, most of this is in the developed world. The expected future growth in business upon which these US companies will depend will be in China and elsewhere in Asia and South Asia, South America and Africa. For some countries in these regions, there is a long-standing suspicion of the dominance of US technology companies able to extract wealth, coupled with a natural wish on the part of these countries to see the development of indigenous capability. US Internet companies are also now, following Snowden, regarded by such states as having facilitated US espionage, and, in effect, able to impose US interpretations of human rights on their citizens since decisions relating to their own law enforcement needs are being taken by private US-owned companies under US law. At the same time, most intelligence and security agencies around the world are no doubt trying to work out how to close an apparent capability gap with the United States. Meanwhile, Western intelligence agencies and law enforcement complain that the publicity given to digital intelligence means they are no longer able to gather evidence as before (Hogan-Howe quoted in Whitehead 2014) and that risks to the public are rising.[34]

For intelligence and law enforcement to be able to identify communications of interest and, where authorized, to access the content of relevant communications themselves is in fact a harder technical challenge than the many internal NSA PowerPoint presentations stolen by Snowden might suggest. Capabilities identified in the Snowden material that are said to be used by the United States (and, it must be assumed, by other leading nations) include the following:

- Access in bulk to substantial quantities of Internet traffic (although still representing a very small proportion of the total). Bulk access can be achieved by intercepting terrestrial microwave links,[35] satellite links[36] and undersea cables.[37]
- Collection and storage of intercepted metadata.[38] Saved metadata can provide information concerning when and to whom phone calls are made or emails and texts are sent. It may also reveal the location of mobile devices.
- Computerized identification of traffic[39] likely to be of potential intelligence interest (as against the bulk of Internet traffic comprising machine-to-machine trading, streaming video films, pornography and so on) using deep packet inspection (DPI)[40] techniques or equivalent.
- Advanced "front end" tools to allow analysts to efficiently access and run advanced queries on intercepted data, in particular, in order to discover new leads in their investigations.[41]
- Cooperative access with the assistance of the companies concerned to commercial digital communications networks[42] and "over-the-top" applications.

33 See Intelligence and Security Committee (2013).

34 A UK example can be seen in the comments by the Intelligence and Security Committee (2014).

35 Both the United States and the Soviet Union developed geostationary SIGINT satellites during the Cold War in order to intercept spillover from microwave links deep inside each other's territory.

36 For example, the Israeli capability. See http://mondediplo.com/2010/09/04israelbase.

37 The GCHQ program TEMPORA is said to intercept bulk traffic on undersea fibre optic cables and buffer the data to allow warranted communications to be filtered out. The French Direction générale de la security extérieure (DGSE) is said to have an equivalent capability for trans-Mediterranean cables, operated in conjunction with the NSA (Follorou 2013).

38 *The Guardian* revealed, from Snowden material, the alleged scope of the NSA's giant database, Marina, for retaining metadata. See Ball (2013).

39 An example is the NSA XKEYSCORE program. See https://edwardsnowden.com/wp-content/uploads/2013/10/2008-xkeyscore-presentation.pdf.

40 DPI is a form of filtering used to inspect data packets sent from one computer to another over a network. The effective use of DPI enables its users to track down, identify, categorize, reroute or stop packets with undesirable code or data. DPI is normally more effective than typical packet filtering, which inspects only the packet headers.

41 The NSA program ICREACH is said to be able to handle upwards of five billion records every day, store them for a year, and make the database searchable by law enforcement and other US agencies and overseas partners (Gallagher 2014).

42 According to the 2014 Vodafone law enforcement disclosure, 29 of its operating businesses around the world were required by local law to cooperate in such access either for communications data, content or both, with, for some countries, an absence of clear legal regulation and no independent oversight (Vodafone 2014). Le Monde has alleged there is a cooperative relationship between Orange and the French external service, DGSE (Follorou 2014).

- Computer network exploitation through which the networks used by targets are infiltrated digitally to extract and gather data,[43] or users' computers are spoofed into connecting into controlled servers (or base stations in the case of mobile telephones) in so-called "man in the middle" or "man on the side" attacks.

- Close-access attacks on the devices themselves and on servers[44] that are used by the target of an investigation by providing software or hardware implants that can facilitate network access to the machine, or by otherwise introducing malware.[45] So-called "watering hole" attacks use compromised websites to introduce cookies to enable users to be tracked and identified (a technique used, for example, against both child abuse and jihadist networks).

- Monitoring of social media use (such as Twitter, Facebook, Pinterest, Tumblr, Instagram, Orkut, Bebo, Qzone, Flickr and many others) with the application of computerized analytics including sentiment analysis (Omand, Bartlett and Miller 2012).

The mix of such methods exploited by nations obviously depends on ease of availability of access: for the United States, it appears from recent disclosures that access to digital data via the dominant US Internet companies has been especially important; for the United Kingdom and France, for historical and geographical reasons, undersea cable access has featured; for Germany, satellite access; for China and Russia, digital computer network exploitation appears from the cyber-security press to have been highly productive in recent years; and for many smaller African and South East Asian nations, cooperative access to local commercial mobile communications networks is important. The ease of access to social media also provides for any nation that feels it justified, a ready source of information on the attitudes and sentiment of local populations that would require only limited investment in interception and digital technology.

LEGAL AND SOCIETAL CONSTRAINTS

The digital intelligence tools and methods outlined above provide powerful means for a state to meet its fundamental responsibility to protect its citizens, but also, if so minded, to acquire too much information about its citizens and to interfere with their liberties. The democracies have always, to greater or lesser extent and in a variety of different ways, tried to protect respect for the rights of their own citizens. 2015 is the eight hundredth anniversary of the Magna Carta, which in turn, influenced the drafters of the US Constitution, whose Fourth Amendment (1789) prohibits for US persons unreasonable searches and seizures, and requires any warrant to be judicially sanctioned and supported by probable cause. The UN Declaration of Human Rights[46] universalized this train of thought after World War II with the prohibition that "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks." All the members of the UN General Assembly subscribed to that declaration.

The universality of the right to respect for privacy means that it must apply to modern digital as well as more traditional means of communication. Four issues in particular arise here that are not fully resolved in international debate.

The first issue concerns what regulation should apply to the greatly increased amount of personal information that the individual discloses in the course of everyday life using the Internet, and, to a great extent, *must* disclose if the full value of the Internet to the individual is to be realized. Some of that information, such as credit card details, clearly must be protected. But other information, such as a person's physical address, is likely only to be sensitive in some contexts and, in many jurisdictions, must be publicly available for voting purposes. Although great efforts are made to anonymize large datasets, which may produce useful medical research findings or public opinion data, for some time expert opinion has been warning that the number of digitized data points relating to an individual (including tagged images) are so great that too often it would be possible to re-identify individuals (Tene and Polonetsky 2002).

The second issue concerns how an invasion of privacy of digital communications is defined. Is it when the computer of an intercepting agency accesses the relevant packets of data along with the rest of the streams of digital information on a fibre optic cable or other bearer? Or is it when a sentient being, the intelligence analyst, can actually see the resulting information about the communication of the target? Perhaps the most damaging loss of trust from the Snowden allegations has come from the common but unwarranted assumption that access in bulk to large volumes of digital communications (the "haystack") in order to find the communications of intelligence targets

43 Widespread use of this approach is said to be responsible for large-scale theft of intellectual property from the United States and Western nations by the Chinese People's Liberation Army (Mandiant n.d.).

44 See, for example, the allegations against both the NSA (https://edwardsnowden.com/2014/05/14/update-software-on-all-cisco-ons-nodes) and Huawai (www.technologyreview.com/news/429542/why-the-united-states-is-so-afraid-of-huawei/).

45 Russian government hackers are suspected of creating a highly sophisticated malware program, code-named Uroburos, designed to steal files from nation states' digital infrastructure (Brewster 2014).

46 Article 12 of the UN Declaration of Human Rights is available at www.un.org/en/documents/udhr/.

(the wanted "needles") is evidence of mass surveillance of the population, which it is not.

The distinction is between authorizing a computer to search through bulk data on the basis of some discriminating algorithm to pull out sought-for communications (and discard the rest) and authorizing an analyst to examine the final product of the material thus filtered and selected. It is the latter step that governs the extent of, and justification for, the intrusion into personal privacy. The computer filtering is, with the right discriminator, capable (in theory, of course, not in actual practice) of selecting out any sought-for communication. But that does not mean the population is under mass surveillance.[47] Provided the discriminator and selection program chosen and used by the accessing computer only selects for human examination the material that a warrant has authorized, and the warrant is legally justified, then the citizens' privacy rights are respected. Of course, if the selectors were set far too broadly and trawled in too much for sentient examination, then the exercise would fail to be proportionate (and would be unlawful, therefore, in most jurisdictions).

The third issue relates to the power of digital metadata (including revealing location, browsing history of Internet searches, and digital address, contact directories and diaries, and so on) to provide information about an individual said to be comparable in its degree of intrusion to accessing the content of communications themselves.[48] Traditionally, communications data on telephone calls was accessible in most jurisdictions on the authority of a senior police officer or investigating magistrate; access to the content of a call would require a higher level of judicial or equivalent warrant. One approach (taken by the United Kingdom in its interception legislation) is to stick to the traditional definition, and logically then to regard anything further possible from digital data (such as the browsing history) as content for which a warrant is needed.

The fourth issue is the question of extraterritoriality. Germany, for example, has put forward a number of proposals at the United Nations essentially seeking an obligation on states to respect the laws of the state where the subject of potential surveillance is located. The argument is that, at present, judgements about the necessity and proportionality of digital investigations that potentially invade their citizens' privacy are being made by judges and authorities in the United States (such as the Foreign Intelligence Surveillance Court) in accordance with US laws as opposed to German laws passed through a German democratic process. Paradoxically, for some non-democratic countries, there is an opposite concern that US privacy law overprotects US citizens and means that the US Internet companies do not have to disclose information about Internet use of their citizens that those states would want to monitor. This issue is, of course, linked to continuing and much wider arguments over the potential for there to be extraterritorial application of human rights law.

There is a separate argument about whether retention of unsorted data beyond a reasonable period, including buffering time taken to run a filtering program, constitutes mass surveillance given, the ease with which an individual's data could be retrieved (an analogy civil libertarians sometimes use is the prospect of the state installing a camera in every bedroom with the promise only to look at your camera if justified with a judicial warrant); the analogy for digital intelligence is much more akin to the ability authorities have in the most serious cases of getting a judicial warrant to install a listening device in the home of a suspect — potentially, therefore, any home. That is a serious invasion of a person's privacy, but it is not keeping the population or a substantial part of it under surveillance. So, when data is retained and held that potentially can allow privacy to be invaded, then controls over its access should be managed to the same standard as for any individual decision to conduct an act of intrusive surveillance. Just because the data is held in a digital database should not make the threshold for accessing it lower.

The caveat in the UN Human Rights Declaration that interference with privacy must not be "arbitrary" recognizes the steps a state may legitimately have to take in order to protect freedom and liberty, provided always that (in the words of Article 29), "In the exercise of his rights and freedoms, everyone shall be subject only to such limitations as are determined by law solely for the purpose of securing due recognition and respect for the rights and freedoms of others and of meeting the just requirements of morality, public order and the general welfare in a democratic society." Although the formulation predates the digital age, this need for balance within the basket of human rights, for example between the individual's right to safety and security and right to privacy, remains valid today.

47 This issue has recently been considered in respect of the Snowden allegations against the GCHQ by the statutory UK Interception Commissioner, who is a senior retired judge. He confirms in his annual report to Parliament for 2014 (available at www.iocco-uk.info/) that the GCHQ does have bulk access by computer to the Internet, but that is for the purpose of carefully targeted, highly discriminating selection of the communications of the targets where there are warrants authorizing interception with certificates attached, authorizing the targets whose communications are being sought. He has reported in the light of the Snowden allegations that everything the GCHQ does is properly authorized and legally properly justified, including under Article 8 of the European Human Rights convention regarding personal privacy. He confirmed categorically in his report that GCHQ does not conduct mass surveillance and that, furthermore, any such activity would be comprehensively unlawful. This judgement has been upheld by the UK courts. See UKIPTrib 13_77-H of December 5, 2014.

48 For example, the view of cryptanalyst Bruce Schneier (2013) that "Metadata equals surveillance; it's that simple."

Only a tiny minority that holds to the original "cyber punk" view of the Internet[49] would argue for an unqualified absolute right to digital privacy. The Snowden material, which publicized the apparent scale of US counterterrorist and other intelligence activity, has nevertheless provoked a vigorous global debate over how best to ensure respect for the right to the privacy of one's digital communications (and personal information accessible from Internet use) while meeting the state's obligation to uphold the law, protect the right to life and security for the citizen — for example, against terrorist attacks — and protect the right to own and enjoy property — for example, against the depredations of serious criminals.

An analogy can be drawn with the balancing act required to justify the use of violence by the armed forces. The "just war" approach seeks to reconcile seeming opposites: states have a duty to defend their citizens and justice — protecting the innocent and defending moral values sometimes requires willingness to use force and violence, but taking human life or seriously harming individuals is wrong. From this tradition has come the *jus ad bellum* challenge of having to justify the decision to enter a conflict and the *jus in bello* criteria for right conduct once engaged, including proportionality, necessity, right authority and discrimination (between legitimate targets and civilians deserving of protection) that are to be found in the Geneva Conventions and in customary international law. The approach has also been applied to suggest specific ethical principles for secret intelligence activity (discussed further later in this paper) (Omand 2006).

The European Court of Human Rights (ECtHR) in a number of notable cases[50] in the 1980s and 1990s gave judgments on claims that state authorities had violated the privacy rights[51] of European citizens by using unlawful methods of investigation including wiretapping and bugging of premises. In a series of judgements, the ECtHR established clear guidelines for the member states of the Council of Europe. These include the need for there not to be an unfettered discretion for executive action and for controls on the arbitrariness of that action. In essence, convention jurisprudence recognizes the need for states to defend themselves and to introduce measures in support of national security including intrusive methods of surveillance,[52] but insists that the impugned measures should have a basis in domestic law, which must be accessible to the person concerned who can foresee its consequences.[53] In its case law on secret measures of surveillance,[54] the court developed minimum safeguards that should be set out in statute law in order to avoid abuses of power: the nature of the offences that may give rise to an interception order (or warrant); a definition of the categories of people liable to have their telephones tapped; a limit on the duration of telephone tapping; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or the tapes destroyed. Such safeguards are easily adapted to the digital world. In a case[55] relating to surveillance using a covertly placed tracking device of movements in a public places, on the other hand, the EctHR established the principle that for measures that interfered less with the private life of the person concerned, the conditions could be less strict.

There is an unresolved public policy issue for nations over how best to regulate intrusive surveillance by the authorities, drawing on arguments such as those of the ECtHR, at least for most democratic states. For example, from the point of view of the privacy interests of those individuals who are subject to investigative measures, it is difficult to draw a workable hierarchy of potential invasion of privacy through interception of digital communications data and content and other forms of highly intrusive intelligence such as the use of human agents or of

49 The classic statement is that of John Perry Barlow's (1996) "Declaration of the Independence of Cyberspace": "Governments of the Industrial World….You are not welcome among us. You have no sovereignty where we gather….Cyberspace does not lie within your borders….You claim that there are problems among us that you need to solve. You use this as an excuse to invade our precincts….We are forming our own Social Contract. This governance will arise according to the conditions of our world not yours. Our world is different."

50 Relevant ECtHR cases include *Malone v. UK* (1984) and *Hewitt and Harman v. UK* (1989). See echr-online.com/art-8-echr/introduction.

51 Article 8 of the European Convention on Human Rights (ECHR) provides that "Everyone has the right to respect for his private and family life, his home and his correspondence. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others" (available at www.echr.coe.int/Documents/Convention_ENG.pdf).

52 The relevant UK Court, the Investigative Powers Tribunal, has recently rejected legal challenges to the GCHQ and the Foreign Secretary by Liberty, Privacy International, the American Civil Liberties Union, Amnesty International and other civil liberties organizations following the Snowden allegations. In an important judgment, the court found that that there is no contravention by the GCHQ of ECHR Articles 8 (Privacy) and 10 (Freedom of Expression). See UKIPTrib 13_77-H, of December 5, 2014, at paragraph 161.

53 The ECtHR did accept, however, that the requirement of foreseeability in the special context of secret controls of staff affecting national security cannot be the same as in many other fields. Thus, it cannot mean that an individual should be enabled to foresee precisely what checks will be made in his regard. See *Leander v. Sweden* [1987] 9 EHRR 433 at paragraph 51.

54 For example, *Malone v. UK* [1985] 7 EHRR 14, *Uzun v. Germany* [2011] 53 EHRR 24 and *Bykov v. Russia* 437.8/02 21 January 2009.

55 *Uzun v. Germany* [2011] 53 EHRR 24.

bugging devices.[56] For instance, if an eavesdropping device is covertly installed in a target's home, it may record conversations between family members that are more intimate and personal than those that might be recorded if the target's telephone were to be intercepted (and this example becomes even clearer if, for instance, the telephone in question is used only by the target to contact his criminal associates).

The rule of law can be applied nationally to the world of intelligence, but there is no settled corpus of international law regulating secret intelligence activity itself, nor is there likely to be one given the universality of intelligence work (to which not all nations will admit) and the difficulties of arriving at international consensus on defining the practice (Yoo and Sulmasy 2007). All nations, on the other hand, make espionage against them a criminal offence. There is no positive obligation on a state to prevent or forestall another nation from intercepting the communications of its citizens,[57] nor is receiving the product of intelligence activity acquiescence in such activity. Nations will always do what they feel is necessary for national security.[58] Nevertheless, the world of secret intelligence need not be ethics-free any more than the world of warfare and nations can agree voluntarily to abide by standards widely accepted as representing responsible state behaviour.

A THREE-LAYER MODEL OF SECURITY AND INTELLIGENCE ACTIVITY ON THE INTERNET

Edward Snowden's allegations highlight a major unresolved public policy issue. Like all such wicked public policy issues, there are several dimensions or layers to the problem. There are interactions — and conflicts — between the requirements of these layers that cannot be wished away and can only be managed by a holistic approach that recognizes that each layer has to be considered alongside the others. Optimize the policy instruments in only one of the dimensions and the result will be unexpected and unwelcome consequences in the others. The problem needs to be tackled as a whole. To examine this proposition, the following sections discuss the nature of intelligence and security activity on the Internet in terms of three layers:

- the everyday level of normal Internet activity and the threats society faces in using and getting the most out of cyberspace;
- the law enforcement level, trying to police at least the worst criminal excesses on the Internet; and
- the secret intelligence level, with agencies working to fulfill their national security mission but also capable of supporting law enforcement.

The Everyday Level of Internet Use

In the top layer is everyday activity on the Internet: communicating, sharing, entertaining and trading. Retaining confidence in the Internet and its financial systems and transactions is fundamental for global economic well-being. This was recognized by the Organisation for Economic Co-operation and Development in 2011 when it published a recommended set of principles for Internet policy making, including: promoting and protecting the global free flow of information; promoting the open, distributed and interconnected nature of the Internet; promoting investment and competition in high-speed networks and services; and promoting and enabling the cross-border delivery of services.[59]

The appropriate norms to be worked up here relate to:

- recognition of the primary importance of the Internet for economic and social progress and for economic development;
- multi-stakeholder principles being applied to the governance of the different aspects of the efficient functioning of the Internet; and
- net neutrality, sensibly interpreted to allow effective management of high latency services.

The principal threat to Internet confidence comes from the rapid increase in malware on the Internet designed, for the most part, for criminal gain. Cybercrime of all types is the most rapidly growing form of crime, driven by highly professional gangs largely based outside their target nations that use malware to make large criminal gains from fraud, as well as simply using cyberspace to conduct classic criminal activity at scale: stealing money, organizing narcotics, WMD and people smuggling, blackmail and extortion rackets. Some of this crime exploits the characteristics of software directly. Some could be characterized as simply traditional forms of crime (theft, for example) that can be perpetrated digitally at a much lower risk than old-fashioned analogues such as robbing banks. Some traditional illegal trading is made possible at scale by the existence of the dark Net component of the Internet (such as Silk Road and similar illegal marketplaces

56 This argument by the UK government was accepted by the court examining claims of unlawful interception. See [2014] UKIPTrib 13_77-H, para 32 et seq.

57 At least that would be an interpretation of the long-standing principle established by the ECtHR in *Bertrand Russell Peace Foundation v. UK* (1978) 14 D&R 117. In the words of the UK Court of Appeal, the ECHR contains no requirement that a signatory state should take up the complaints of any individual within its territory touching the acts of another sovereign state. See www.bailii.org/ew/cases/EWCA/Civ/2006/1279.html.

58 The member states of the European Union have, for example, always withheld competence on matters of national security from the European Commission, seeing these as the prerogative of the nations themselves, meeting in the European Council of Ministers.

59 See www.oecd.org/internet/ieconomy/49258588.pdf.

selling drugs and counterfeit items). The scale of Internet criminal enterprise itself spawns criminal marketplaces for false identities, credit card details and malware exploits that can be used for criminal purposes.

On the dark Net, beyond the indexing of Google, and accessible only with Tor or other anonymization software, jihadist beheading videos are circulated. Guns and weapons of all kinds, counterfeit goods, drugs, sex and slaves are sold. And this is where the cybercriminal can acquire the latest malware for their attacks.

An increasing number of nations are realizing the importance of consumer and business confidence in the Internet and are devoting considerable resources to improving cyber security, including through better education on the risks and counter-measures to be taken. Secure encryption and sound security protocols are needed for everyday communications to protect private communications and financial transactions and defeat global cybercriminals.

Alleged exploits of the NSA to get around hard encryption in pursuit of the external national security mission have raised doubts about whether software used for the everyday purposes of commerce and socializing has been weakened.[60] When flaws are detected in software systems (as they are all the time, given the staggering complexity of modern software and the interactions of applications, operating systems and communications) there is potential tension with (as inferred from some of the Snowden material) the value to intelligence agencies of exploiting such flaws and exploits. Nevertheless, sound military reasoning would argue that a defence being breached is much more serious than losing the hypothetical value of a future tool. It would seem appropriate, therefore, to consider having norms here:

- To encourage the disclosure of software vulnerabilities in the interests of getting them fixed, and when it is a choice of keeping vulnerability for future covert use or disclosing it to bolster cyber defence, and it is a close call, the defence should always win.
- A nation under cyber attack should be able to call for, and expect, international support, and there needs to be the network of CERTS (Computer Emergency Response Teams) to provide it.
- Nations should sign up to the UN Human Rights Council Resolution 20/8 that the rights that apply in the offline world apply in cyberspace, too.
- Specifically, as the North Atlantic Treaty Organization (NATO) Tallinn Manual[61] states, international humanitarian law applies in cyberspace, too. So, the constraints of humanitarian law in warfare, the principle of discrimination to protect civilians, avoid collateral damage and so on, apply to cyber attacks.
- In the long term, it might even be possible to contemplate among the permanent five members of the United Nations Security Council (UNSC) an agreement that it is in each state's interest not to invite potentially fatal crisis instability by trying to plant cyber Trojan malware in key space and nuclear command and control systems.

Everyday Internet use is also the level at which data protection legislation, both national and international (for example, the new draft European Union Data Protection Regulation and Directive), kicks in to protect citizens' personal data from unlawful use. Such data protection is based on identifying and protecting personal data by insisting on the consent of the subject. Under the latest proposals, the subject would be given the "right to be forgotten" and thus the legal power to compel the deletion of personal data. Conflicts are already arising between jurisdictions with different interpretations of safeguarding and disclosing personal data, and erasing it. More international discussion is needed in order to establish agreement that to minimize conflicting and overlapping legal jurisdictions, national data protection legislation should be based on common principles such as sanctioning negligence in the safeguarding of personal data and misusing personal data for unlawful purposes.

The increasing dependence on the Internet for the routines of everyday life — and for the critical national infrastructure, such as power, telecommunications, transport and logistics, on which the normal life of the citizen depends — introduces new vulnerabilities into society. Even where systems are air-gapped from the Internet, such as the control systems for nuclear plants, the potential exists for breaches of security through the access required for visiting contractors or the staff of the facility themselves. The threat is from malicious hackers intent on disruption in support of their own causes or simply to prove a point, from criminals seeking gain through economic blackmail and from potentially hostile states.

60 Tim Berners-Lee has criticized the NSA in those terms and has called for an Internet Magna Carta. Berners-Lee and the World Wide Web Consortium, a global community with a mission to lead the Web to its full potential, have launched a year of action for a campaign called the Web We Want, urging people to push for an Internet "bill of rights" for every country. See www.bdimedia.com/blog/happy-birthday-internet-web-founder-berners-lee-now-calls-magna-carta-protect-internet-users/.

61 The NATO Tallinn Manual was the outcome of a detailed expert study of international law applicable to cyberspace. See https://ccdcoe.org/tallinn-manual.html.

Law Enforcement Activity on the Internet

Supporting the everyday level, therefore, is a layer of law enforcement activity by police, customs, immigration, child protection, civil contingencies and other authorities attempting to control the worst excesses of criminality, and to uphold the law and ensure the continuity of essential services. As earlier noted, the volume and nature of Internet communications and the claim asserted by some to an individual's right to anonymity in cyberspace[62] pose issues for law enforcement. Areas for norm construction for everyday activity might therefore include the need for an international norm that accepts Internet freedom of expression and personal privacy as fundamental rights as provided for in the UN Declaration (and national constitutions such as the US Constitution), but accepts explicitly that they are not absolute rights — they have to be qualified by other rights of the citizen such as the right to live in peace and to enjoy one's property. So, there is also no *absolute* right to anonymity on the Internet, but it is a part of the right to privacy that has to be respected and interference with it justified. Specifically, agreement that the Internet cannot be allowed to be a safe space for criminal activity by allowing absolute protection for personal communications.

The current work of law enforcement in attempting to police the top level of everyday Internet use has had some successes,[63] but in most states, law enforcement is falling further and further behind. Conventional non-cyber crime is decreasing in many nations as digital crime offers higher rewards at lower risk in terms of probability of detection and length of sentence if caught. The problems this poses for law enforcement include the following:

- As noted earlier, criminals of all types, including terrorists, use the same range of mobile devices and applications as everyone else, including the ability to disguise or strongly encrypt their communications and thus to hide criminal conspiracies.
- Traditional criminal investigation tools such as those derived from telephone billing information and wiretapping are increasingly ineffective as more communications switch to the Internet.
- There are insufficient numbers of suitably qualified cyber-trained officers capable of dealing with the volume of criminal activity on the Internet, including coping with a rising volume of cyber fraud, and of specialist officers capable of pursuing the most complex of cases to successful prosecution.
- The need to follow cyber attacks in near-real time, and the difficulties of attributing attacks that are bounced off servers located in different countries severely tests mechanisms of international law enforcement cooperation based on traditional models. The process for requests under Mutual Legal Assistance Treaties may not be the most appropriate mechanism for international cooperation required in the cyber age.
- It is in the nature of the Internet that victims and offenders are mostly no longer in proximity and a single offender can use the Internet to attack multiple victims across many police areas and national jurisdictions. Some of the most persistent and capable criminal groups are based in jurisdictions that do not or cannot respond fully to requests for assistance or to extradition requests/arrest warrants.
- Cyber criminals can buy exploits in dark markets as well as access to credit card and other personal details of potential victims, and do not need advanced hacker skills themselves.[64]

There needs, therefore, to be active domestic law enforcement activity on the Internet, supporting everyday life, and trying to police the worst abuses of cyberspace. One of the biggest challenges is the absence of global agreement on dual criminality across a wide rage of cyber-related offences (including the nature of hate speech). The nature of the Internet is that for every nation there will be communications and websites that offend against domestic law (for example, by exhibiting images of child abuse, glorifying terrorism or expressing racial or other hate crime), following a set of norms that are widely recognized internationally:

- As is the practice within the European Union, there needs to be the widest possible international mutual legal recognition of certain clear classes of criminal offence that are cyber enabled, including child abuse (the double or dual criminality test that an act is, in law, a crime in all the jurisdictions involved), and cyber dependent, such as ransom-ware.
- The basic principles of necessity and proportionality, to be found in international and national human rights law, should be applied throughout law enforcement activity.

62 A right to anonymity was never conceded by states in the world of three dimensions to apply to those committing crimes or harming society.

63 Examples include the international cooperation led by the FBI that resulted in the taking down of the dark Web criminal sites Silk Road 1 and Silk Road 2, and the arrest of a number of suspects.

64 In September 2014, a report from Europol's European Cybercrime Centre, *Internet Organised Crime Threat Assessment*, revealed the diffusion of the business model in underground communities and highlighted that barriers to entry in cybercrime rings are being lowered even if criminal gangs have no specific technical skills. Criminals can rent a botnet of machines for their illegal activities, to infect thousands of machines worldwide. These malicious infrastructures are built with a few requirements that make them suitable for the criminals, including user-friendly command-and-control infrastructure and sophisticated evasion techniques.

- The Internet companies responsible for maintaining global networks cannot be expected to take on the role of policing the Internet, but they can and should take steps to enable those who do have that legal responsibility to exercise it properly, provided that such steps are legally authorized. Steps should include retention of communications metadata, under appropriate safeguards and retention periods, and, if necessary, financed by national government.

- The close cooperation of Internet companies with law enforcement is essential both in their own interests to help manage cybercriminal attacks and in supporting criminal investigations that affect their customer confidence and profitability, and in the interests of corporate social responsibility, for example by removing illegal content.

- Cooperation with law enforcement should include prompt response to proper legal warrants for requests for information about subscribers and their use of the Internet and about threats to public safety and security.

Intelligence Activity in Cyberspace

To help overcome the problems of policing cyberspace, law enforcement in many nations is increasingly looking to national intelligence agencies for support. Some nations have specifically legislated to allow their national intelligence community to provide support for law enforcement[65] and the priority given to domestic counterterrorism has accentuated this trend. There are of course differences. Modern law enforcement has an intelligence function (for example, mapping crime hot spots to allow targeted policing). But most of the time, law enforcement is seeking evidence after the crime has been committed that can be deployed as part of an open judicial process and whose legitimate derivation and meaning can be proved beyond reasonable doubt. Intelligence work is often described as probabilistic, as a jigsaw puzzle and as incomplete, fragmentary and sometimes wrong.[66] Digital intelligence can often generate leads for follow-up by conventional law enforcement methods designed to gather specific evidence, such as visual surveillance or the search of a premises.

The opportunity offered by mobile phone geo-location is an example of a digital technique that has been quickly taken up by police services, for example, to test alibis, eliminate suspects from an inquiry and help track down the perpetrators of multiple serious crimes. The power of keeping track, over a period of time, of the location of a mobile device (and what other mobile phones or devices might have been in the close vicinity of that device) is clearly of interest to the police, but is potentially very intrusive, as has been recognized by parliamentarians and civil liberties organizations. Nevertheless, for some jurisdictions, there are still constitutional concerns over the sharing of intelligence with conventional domestic police services and, in some cases, historical tensions due to past disputes over competence and territory. There is also a tension between the inevitably top-down federal nature of state intelligence activity and the local nature of policing in which "the police are the public and the public are the police," where the ability of the police to perform their duties is dependent upon public approval of police existence, actions, behaviour and the ability of the police to secure and maintain public respect.[67] One of the consequences of the Snowden affair is such questions are being increasingly posed in relation to national digital intelligence activity.

In general, national intelligence agencies have been ahead of police services in exploiting the more advanced digital information sources. For many, including the United States, the United Kingdom, Canada, Australia and New Zealand (the Five Eyes partnership that emerged from World War II) and the NATO nations, their SIGINT capabilities naturally developed into capability and cooperation in digital realms, and the same has been true for many other nations, including China, Russia, India, Japan, South Korea, Taiwan, Israel, Sweden and Finland. The Snowden material provides glimpses not only into US, Five Eyes and NATO digital intelligence but also into the capabilities that can be assumed of other nations.[68] In some cases, the claims of advanced techniques can be assumed to be spurring on others to follow suit.

An inevitable consequence of the purpose of secret intelligence being to obtain information that others are trying to hide is the essential part played by secrecy. The effectiveness of secret intelligence rests on sources and methods that must remain hidden, otherwise the targets know how to avoid detection. Oversight of intelligence activity cannot, therefore, be fully transparent and has

65 The EctHR has recognized the prevention and detection of serious crime as a legitimate purpose for intrusive intelligence activity along with national security and economic well-being.

66 "To supplement their knowledge in areas of concern where information is, for one reason or another, inadequate, governments turn to secret sources. Information acquired against the wishes and (generally) without the knowledge of its originators or possessors is processed by collation with other material, validation, analysis and assessment and finally disseminated as 'intelligence'" (Butler 2004).

67 The second of the 1829 principles of law enforcement (upon the founding of Scotland Yard). See www.durham.police.uk/About-Us/Documents/Peels_Principles_Of_Law_Enforcement.pdf.

68 In his speech at the Department of Justice on January 17, 2014, President Obama said, "We know that the intelligence services of other countries — including some who feign surprise over the Snowden disclosures — are constantly probing our government and private sector networks, and accelerating programs to listen to our conversations, and intercept our emails, and compromise our systems. We know that" (Obama 2014).

to be by proxy: by senior judges and a limited number of parliamentarians who can, on society's behalf, be trusted to enter the "ring of secrecy" and give confidence that legal and ethical standards are being maintained.

Whatever view is taken of the legitimacy of Edward Snowden as a genuine whistleblower and of the proportionality of his actions,[69] his allegations have, in many respects, breached the necessary minimum secrecy that should surround details of intelligence sources and methods. It is important to recognize that the resulting damage to intelligence collection applies globally, not just to the agencies exposed by Snowden, from:[70]

- the scale of publicity sensitizing terrorists and criminal groups to the whole issue of digital intelligence, warning suspects of the need to be more secure and, for example, criminal networks to change their operating methods and equipment;
- highlighting/compromising specific types and methods of intelligence collection, and exposing gaps in coverage that provide signposts for criminal and hostile actors on how to reduce the probability of detection;
- accelerating the commercial information and communication technology sector's move to hard encryption on devices and software that cannot be overcome even with legal warrants (the response of the intelligence agencies is likely to be to try to get much closer to their targets, with consequential greater moral hazard of collateral intrusion);
- reduction in Internet company cooperation with law enforcement and government agencies as they seek to protect their commercial reputations for being able to secure their customers' data (and thus also prevent competitors deriving value from the content they are carrying); and
- the risk of overregulation due to fears of mass surveillance.

The main justification for all intelligence activity, including digital, remains national security, including support for the armed forces and for defensive alliances such as NATO and cooperative organizations such as the African Union. Where powerful digital intelligence tools exist, it is natural for law enforcement to seek support (or in some cases, such as social media, monitoring to acquire their own capability).

It is a proper use of national intelligence resources to support law enforcement, provided that the use of intrusive methods is legally regulated, as they would be if used by law enforcement itself.

As earlier noted, more often than not nowadays a common feature of the demands placed on an intelligence community by the armed forces and law enforcement alike are for actionable intelligence about people — the terrorists, insurgents, cyber- and narco-criminal gangs, people traffickers and pedophile networks, cyber-vandals and hackers. For such targets, what is likely to be sought as of most value are their identities (a non-trivial issue given digital anonymity), associations, location, movements, financing and intentions. Often, large issues of public policy rest on the outcome of intelligence on dictators committing or threatening to carry out war crimes. For example, trying to establish whether there are Russian paramilitaries in Eastern Ukraine, on which UNSC and European Council sanctions decisions may rest. Or whether Islamic State of Iraq and the Levant jihadists in Iraq and Syria, responsible for the appalling executions of hostages, will bring their campaign to domestic streets in Europe, America and the Middle East. Of course, there are still demands from governments for intelligence on the activities of some traditional states, including friendly states where their intentions in specific areas engage vital national security interests[71] — but even in such cases the communications of interest are likely to be carried on virtual private networks on the Internet.

Not all intelligence requirements are, however, of equal importance or urgency. The limited budgets for intelligence activity at a time of general austerity in public expenditure (at least in most democratic nations) should force prioritization. Most of the top priorities will be obvious — in supporting the armed forces on operations and in providing leads for counterterrorist operations to protect the public, or where there are important diplomatic decisions to be taken, as with the negotiations with Iran over its nuclear enrichment program and over sanctions on Russia in relation to its actions in Ukraine. Intelligence agencies also have the task of providing strategic warning of new threats not yet on policy makers' radar, and leeway

69 Snowden has said his greatest concern was with what he saw as the unconstitutional nature of the NSA's bulk collection and storage program of the metadata of communications of US citizens, authorized under s.215 of the USA PATRIOT Act 2001. President Obama acknowledged the sensitivity of this program in his speech. The large volume of classified material (circa 170,000 documents) Snowden stole and passed to investigative journalists to expose went much wider than domestic surveillance, including US and NATO support to military operations. In addition, he passed on 58,000 top-secret documents taken from the British partner agency GCHQ. See www.headoflegal.com/2013/08/30/r-miranda-v-home-secretary-witness-statement-of-oliver-robbins/.

70 See www.telegraph.co.uk/news/uknews/law-and-order/11300936/GCHQ-warns-serious-criminals-have-been-lost-in-wake-of-Edward-Snowden-leaks.html.

71 Relevant here is President Obama's 2014 statement directing the US intelligence community not to monitor the communications of heads of state and government of close friends and allies, unless there is a compelling national security purpose. See The White House (2014).

has to be allowed in authorizing intelligence collection operations accordingly, and in allowing intelligence relationships to be developed with other states.

Nations should make timely arrangements for sharing securely intelligence warnings on threats to the public, and, in relation to terrorism, should establish appropriate points of contact between national counterterrorism analysis centres or authorities.[72]

Most security and intelligence authorities see themselves as having a duty to seek and use information, including digital intelligence, to help manage threats to public and national security. Secret intelligence, because it involves overcoming the determined efforts of others, such as terrorists, to prevent it being acquired, inevitably involves running moral hazard such as collateral intrusion upon privacy of those such as family members who may be entirely innocent. Like law enforcement at the start of an investigation, it is also often necessary to examine a number of witnesses to a crime or associates of suspects in order to eliminate them from enquiries. The examination of those later shown to be innocent of wrongdoing is an inevitable consequence of investigative law enforcement. It should also be recognized that the powerful tools of digital intelligence are already being used in some repressive non-democratic countries for censorship and control of dissidents.

There are already, from the work of the EctHR and from academic legal scholarship, suggestions for internationally acceptable norms on how such activity is organized in order to reduce the risk of intelligence activity being abused. Taken together, and underpinned by domestic law, these form a new social contract in which, through democratic process, the public accepts the need for some infringement of privacy (within limits) in return for the government's commitment to keep the public secure:

- Intelligence agencies should be placed on a national legal footing with the organizations concerned having legal personalities.
- The purposes of secret intelligence should be restricted by law — for example, excluding its use for domestic political purposes and for commercial advantage.
- Investigative activity should be regulated by black letter law — there should not be secret law unavailable to the citizen.
- Highly intrusive methods should be authorized under a warranting system laid down by law.
- There should be independent oversight of intelligence activity, with sufficient access through some combination of judicial and parliamentary means, to ensure that the law is being applied and that the policies being followed are in accordance with democratic wishes. It would be best practice for governments to publish statistics on the scale of use of warranted digital intrusive methods.
- There should be the means for an independent court to assess claims of abuse of these powers, able to provide redress if proven, together with the authority to set matters right after mistakes have been made, for example, by having an individual removed from a watch-list or no-fly list.

There are also important principles of proportionality and necessity that should apply to legislation governing the intelligence agencies, so those authorizing intelligence activity, the regulators and overseers, and those inside the agencies all recognize the legal duty they have to satisfy themselves that the degree of intrusion or moral hazard likely to be occurred is in proportion to the harm to national security or public safety that is to be prevented or the benefit to be gained. Additionally, the operation must be necessary to help achieve the approved purpose, and must be one whose purpose could not reasonably be achieved in another way that did not have to involve secret intelligence. Not everything that technically can be done, should be done. Edward Snowden's allegations about the interception of the mobile telephone of Angela Merkel, the German chancellor, prompted President Obama to issue his own norm[73] on the interception of the communications of the leaders of friendly states: intelligence agencies should not, unless there is a compelling national security purpose, monitor the communications of heads of state and government of close friends and allies.

The analogy between the ethics that might responsibly apply to the activities of secret intelligence and those of the "just war" tradition underlying humanitarian law was referred to earlier. In brief, as applied to digital intelligence, appropriate norms might cover the following ground:

- **There must be sufficient sustainable cause.** There needs to be a check on any tendency for the secret world to expand into areas unjustified by the scale of potential harm to national interests, including

72 This suggested area for norm development follows the thrust of the UNSC Resolution 1373 adopted unanimously after the attacks of September 11, 2001.

73 See Obama (2014).

public safety, so the purposes of intelligence should be limited by statute.[74]

- **All concerned must behave with integrity.** Integrity is needed throughout the whole system, from the reasons behind requirements, and the actions taken in the collection, through to the analysis, assessment and use of the resulting intelligence.
- **The methods to be used must be proportionate.** The likely impact and intrusion into privacy of the proposed intelligence collection operation, taking account of the methods to be used, must be in proportion to the harm that it is sought to prevent and the mechanisms for determining proportionality need to be tested through independent oversight.
- **There must be right authority.** There must be a sufficiently senior authorization of intrusive operations and accountability up a recognized chain of command to permit effective oversight. Right authority too has to be lawful and respectful of internationally accepted human rights.
- **There must be reasonable prospect of success.** Even if the purpose is valid and the methods to be used are proportionate to the issue, there needs to be discrimination and selectivity (no large-scale "fishing expeditions"[75]) with a hard-headed assessment of how to manage the risk of collateral intrusion on others.
- **Necessity.** Recourse to the specific method of secret intelligence collection should be necessary for achieving the authorized mission and should certainly not be used if there are open sources that can provide the information being sought.

CONCLUSION

As a result of pressure from civil rights organizations following Snowden, governments are rightly re-examining processes and legal frameworks for intelligence activity and seeking to improve oversight mechanisms. No doubt the outcome of such inquiries will help the development of norms based on well-understood and tested principles that can help democratic societies regulate necessary digital intelligence activity in ways that respect the right to privacy and that help ensure that confidence is retained in the Internet.

The domestic legal framework of regulation and oversight within which intelligence activity has to be conducted will — and should — inevitably constrain the free interplay of demand for and potential supply of intelligence, not least derived from digital sources. That constraint also inevitably involves the public avowal of intelligence activity, and the according of legal status to the agencies that collect and analyze secret intelligence, as well as the provision of at least enough information outside the secret circles of agency activity to enable confidence in their activity to be justified publicly. It is not enough for the insiders to be confident that there are very effective safeguards. It is also essential for the democracies that digital intelligence is seen to be regulated effectively by applying safeguards that are recognized to give assurance of ethical behaviour, in accordance with modern views of human rights, including respect for personal privacy.

If — and it is a risk — nations are overzealous in response to Edward Snowden in constraining digital intelligence-gathering capability and data sharing, then the interests of national publics will be failed, since governments will not be able to manage the risks from terrorism, cybercrime and other criminality, nor will they have the intelligence on which sound policy decisions can be made. If, on the other hand, nations fail to exercise sufficient restraint on the use of the powerful digital tools in the hands of their intelligence agencies, and fail to be believed in doing so, then the resulting unease on the part of a vocal section of national publics and in such bodies as the European Parliament will destabilize the very intelligence communities whose work is essential in the collective interest to manage twenty-first-century risks.

Manifesting norms that law enforcement and security and intelligence agencies clearly abide by will go a long way to meet the challenge that intelligence agencies in the democracies must also be seen to behave consistently in ways that the public considers ethically sound.

74 An example is the UK's Intelligence Services Act, which only permits the national intelligence agencies to act "(a) in the interests of national security, with particular reference to the defence and foreign policies of Her Majesty's Government in the United Kingdom; or (b) in the interests of the economic well-being of the United Kingdom in relation to the actions or intentions of persons outside the British Islands; or (c) in support of the prevention or detection of serious crime" (Government of the United Kingdom 1994).

75 Law enforcement is used to having to show "probable cause" in relation to intrusive investigation of suspects. Such a criterion cannot simply be transferred over to secret intelligence, which is often seeking discovery of threats yet to crystalize and new threat actors yet to be identified. Nevertheless, "general warrants" remain unlawful both in the United States and the United Kingdom.

WORKS CITED

Aid, Matthew M. 2013. "Greenwald's Interpretation of BOUNDLESSINFORMANT NSA Documents Is Oftentimes Wrong." November 24.

Ball, James. 2013. "NSA Stores Metadata of Millions of Web Users for up to a Year, Secret Files Show." *The Guardian*, September 30. www.theguardian.com/world/2013/sep/30/nsa-americans-metadata-year-documents.

Barlow, John Perry. 1996. "A Declaration of the Independence of Cyberspace." http://w2.eff.org/Censorship/Internet_censorship_bills/barlow_0296.declaration.

Brewster, Thomas. 2014. "Russians Suspected in 'Uroburos' Digital Espionage Attacks." TechWeek Europe, March 3. www.techweekeurope.co.uk/workspace/russian-intelligence-uroburos-malware-140494.

Butler, R. 2004. *Review of Intelligence on Weapons of Mass Destruction*. UK House of Commons, HC 898, July 14.

Chapple, Irene. 2013. "Why Minerals Dispute Threatens Electronics Industry." CNN, March 14.

Corera, G. 2006. *Shopping for Bombs*. New York: Oxford University Press.

Europol. 2014. *The Internet Organised Crime Threat Assessment*. Europol. September. www.europol.europa.eu/content/internet-organised-crime-threat-assesment-iocta.

Follorou, Jacques. 2013. "Surveillance : la DGSE a transmis des données à la NSA américaine." *Le Monde*, October 30. www.lemonde.fr/international/article/2013/10/30/surveillance-la-dgse-a-transmis-des-donnees-a-la-nsa-americaine_3505266_3210.html.

———. 2014. "Espionnage : comment Orange et les services secrets coopèrent." *Le Monde*, March 20. www.lemonde.fr/international/article/2014/03/20/dgse-orange-des-liaisons-incestueuses_4386264_3210.html.

Gallagher, Ryan. 2014. "The Surveillance Engine: How the NSA Built Its Own Secret Google." *The Intercept*, August 25. https://firstlook.org/theintercept/2014/08/25/icreach-nsa-cia-secret-google-crisscross-proton/.

Government of the United Kingdom. 1994. Intelligence Services Act. www.legislation.gov.uk/ukpga/1994/13/pdfs/ukpga_19940013_en.pdf.

Intelligence and Security Committee. 2013. *Foreign Involvement in the Critical National Infrastructure: The Implications for National Security*. June. www.gov.uk/government/uploads/system/uploads/attachment_data/file/205680/ISC-Report-Foreign-Investment-in-the-Critical-National-Infrastructure.pdf.

———. 2014. *Report on the Intelligence Relating to the Murder of Fusilier Lee Rigby*. HC 795, November 25.

Mandiant. n.d. "APT1: Exposing One of China's Cyber Espionage Units." http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

Manningham-Buller, Eliza. 2003. "Transcript of the James Smart Lecture by the Director General of the Security Service, Eliza Manningham-Buller, City of London Policy Headquarters, 16 October 2003."

National Commission on Terrorist Attacks. n.d. *Law Enforcement, Counterterrorism and Intelligence Collection in the United States Prior to 9/11*. Staff Statement No. 9.

Obama, Barack. 2014. "Remarks by the President on Review of Signals Intelligence." Department of Justice, Washington, DC, January 17. www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence.

Omand, David. 2006. "Ethical Guidelines in Using Secret Intelligence for Public Security." *Cambridge Review of International Affairs* 19 (4): 613–28.

———. 2010. *Securing the State*. London: Hurst, and New York: Oxford University Press.

Omand, D., J. Barlett, and C. Miller. 2012. "Introducing Social Media Intelligence." *Intelligence and National Security* 27 (6): 803–23.

Parker, Andrew. 2015. "Address by the Director General of the Security Service, Andrew Parker, to the Royal United Services Institute (RUSI) at Thames House, 8 January 2015." MI5 Security Service.

Schneier, Bruce. 2013. "Metadata Equals Surveillance." *Schneier on Security*, September 23. www.schneier.com/blog/archives/2013/09/metadata_equals.html.

Tene, O. and J. Polonetsky. 2002. "Privacy in the Age of Big Data." *Stanford Law Review* 64. www.stanfordlawreview.org/online/privacy-paradox/big-data.

The White House. 2014. "Presidential Policy Directive — Signals Intelligence Activities." Office of the Press Secretary. January 17. www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities.

Troianovski, Anton and Danny Yadron. 2014. "German Government Ends Verizon Contract." *The Wall Street Journal*, June 26. www.wsj.com/articles/german-government-ends-verizon-contract-1403802226.

Vodafone. 2014. "Law Enforcement Disclosure Report." In *Sustainability Report*. www.vodafone.com/content/sustainabilityreport/2014/index/operating_responsibly/privacy_and_security/law_enforcement.html.

Whitehead, Tom. 2014. "Internet Is Becoming a 'Dark and Ungoverned Space,' Says Met Chief." *The Telegraph*, November 6. http://www.telegraph.co.uk/news/uknews/law-and-order/11214596/Internet-is-becoming-a-dark-and-ungoverned-space-says-Met-chief.html.

Yoo, J. and G. Sulmasy. 2007. UC Berkeley Public Law Research Paper No. 1030763. *Michigan Journal of International Law* 28.

CIGI PUBLICATIONS
ADVANCING POLICY IDEAS AND DEBATE

The Regime Complex for Managing Global Cyber Activities

GCIG Paper No. 1
Joseph S. Nye, Jr.

When trying to understand cyber governance, it is important to remember how new cyberspace is. Advances in technology have, so far, outstripped the ability of institutions of governance to respond. This paper concludes that predicting the future of the normative structures that will govern cyberspace is difficult.

Tipping the Scale: An Analysis of Global Swing States in the Internet Governance Debate

GCIG Paper No. 2
Tim Maurer and Robert Morgus

This paper offers an analysis of the global swing states in the Internet governance debate and provides a road map for future in-depth studies.

Legal Mechanisms for Governing the Transition of Key Domain Name Functions to the Global Multi-stakeholder Community

GCIG Paper No. 3
Aaron Shull, Paul Twomey and Christopher S. Yoo

Under the existing contractual arrangement, the Internet Corporation for Assigned Names and Numbers (ICANN) has been accountable to the US government for the performance of these functions. However, if the US government is no longer party to this agreement, then to whom should ICANN be accountable?

Legal Interoperability as a Tool for Combatting Fragmentation

GCIG Paper No. 4
Rolf H. Weber

The recently developed term "legal interoperability" addresses the process of making legal rules cooperate across jurisdictions. It can facilitate global communication, reduce costs in cross-border business and drive innovation, thereby creating a level playing field for the next generation of technologies and cultural exchange.

Innovations in Global Governance: Toward a Distributed Internet Governance Ecosystem

GCIG Paper No. 5
Stefaan G. Verhulst, Beth S. Noveck, Jillian Raines and Antony Declercq

The growth and globalization of the Internet over the past 40 years has been nothing short of remarkable. Figuring out how to evolve the Internet's governance in ways that are effective and legitimate is essential to ensure its continued potential.

The Impact of the Dark Web on Internet Governance and Cyber Security

GCIG Paper No. 6
Michael Chertoff and Tobby Simon

The deep Web has the potential to host an increasingly high number of malicious services and activities. The global multi-stakeholder community needs to consider its impact while discussing the future of Internet governance.

On the Nature of the Internet

GCIG Paper No. 7
Leslie Daigle

This paper examines three aspects of the nature of the Internet: the Internet's technology, general properties that make the Internet successful and current pressures for change.

Finding Common Ground: Challenges and Opportunities in Internet Governance and Internet-related Policy

Briefing Book
CIGI Experts

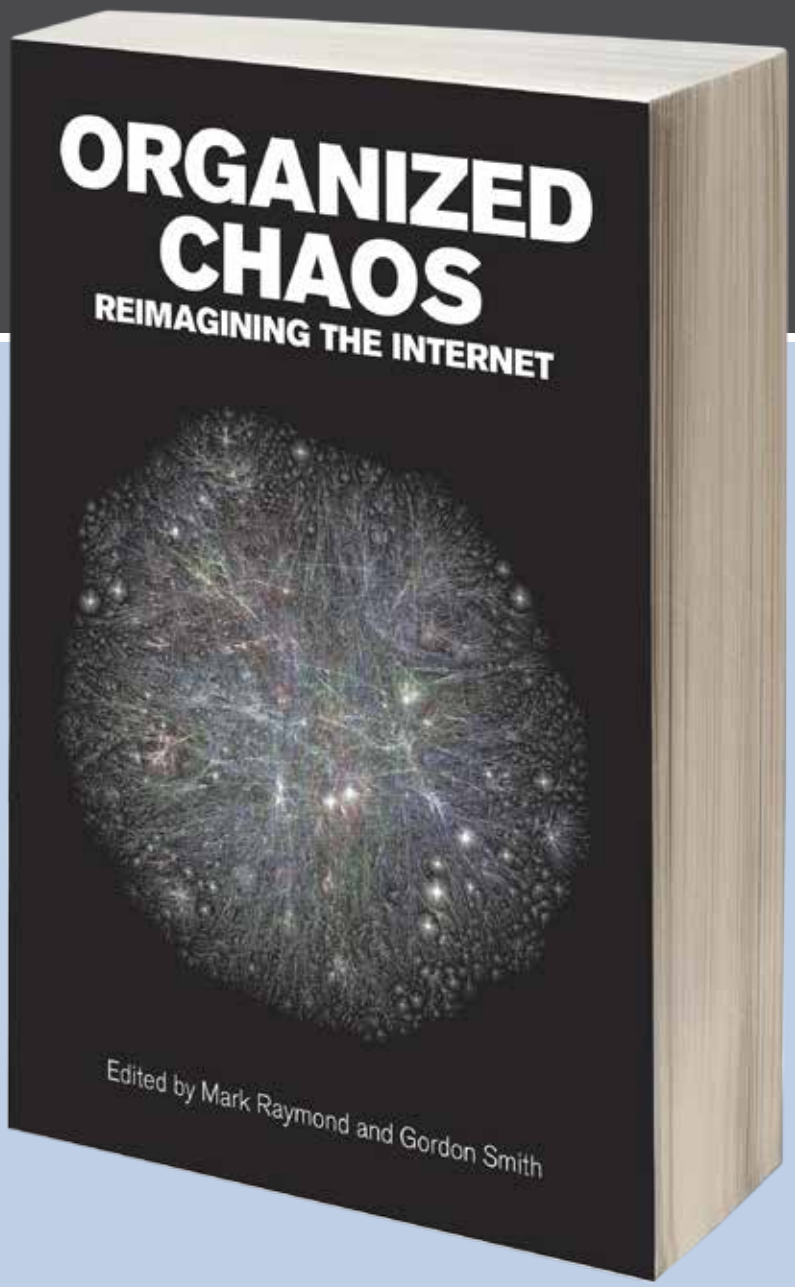
This briefing book contextualizes the current debate on the many challenges involved in Internet governance. These include managing systemic risk — norms of state conduct, cybercrime and surveillance, as well as infrastructure protection and risk management; interconnection and economic development; and ensuring rights online — such as technological neutrality for human rights, privacy, the right to be forgotten and the right to Internet access.

Available as free downloads at www.cigionline.org

ORGANIZED CHAOS
REIMAGINING THE INTERNET

EDITED BY

MARK RAYMOND AND
GORDON SMITH



Leading experts address a range of pressing challenges, including cyber security issues and civil society hacktivism by groups such as Anonymous, and consider the international political implications of some of the most likely Internet governance scenarios in the 2015–2020 time frame. Together, the chapters in this volume provide a clear sense of the critical problems facing efforts to update and redefine Internet governance, the appropriate modalities for doing so, and the costs and benefits associated with the most plausible outcomes. This foundation provides the basis for the development of the research-based, high-level strategic vision required to successfully navigate a complex, shifting and uncertain governance environment.

Price: CDN$25.00
200 Pages, Trade Paperback
ISBN 978-1-928096-04-7

CIGI

Centre for International Governance Innovation

Single copy orders: cigionline.org/bookstore
Available in paperback and ebook form.

ABOUT CIGI

The Centre for International Governance Innovation is an independent, non-partisan think tank on international governance. Led by experienced practitioners and distinguished academics, CIGI supports research, forms networks, advances policy debate and generates ideas for multilateral governance improvements. Conducting an active agenda of research, events and publications, CIGI's interdisciplinary work includes collaboration with policy, business and academic communities around the world.

CIGI's current research programs focus on three themes: the global economy; global security & politics; and international law.

CIGI was founded in 2001 by Jim Balsillie, then co-CEO of Research In Motion (BlackBerry), and collaborates with and gratefully acknowledges support from a number of strategic partners, in particular the Government of Canada and the Government of Ontario.

Le CIGI a été fondé en 2001 par Jim Balsillie, qui était alors co-chef de la direction de Research In Motion (BlackBerry). Il collabore avec de nombreux partenaires stratégiques et exprime sa reconnaissance du soutien reçu de ceux-ci, notamment de l'appui reçu du gouvernement du Canada et de celui du gouvernement de l'Ontario.

For more information, please visit www.cigionline.org.

ABOUT CHATHAM HOUSE

Chatham House, the Royal Institute of International Affairs, is based in London. Chatham House's mission is to be a world-leading source of independent analysis, informed debate and influential ideas on how to build a prosperous and secure world for all. The institute: engages governments, the private sector, civil society and its members in open debates and confidential discussions about significant developments in international affairs; produces independent and rigorous analysis of critical global, regional and country-specific challenges and opportunities; and offers new ideas to decision-makers and -shapers on how these could best be tackled from the near- to the long-term. For more information, please visit: www.chathamhouse.org.

CIGI MASTHEAD

Managing Editor, Publications	Carol Bonnett
Publications Editor	Jennifer Goyder
Publications Editor	Vivian Moser
Publications Editor	Patricia Holmes
Publications Editor	Nicole Langlois
Graphic Designer	Melodie Wakefield
Graphic Designer	Sara Moore

EXECUTIVE

President	Rohinton Medhora
Vice President of Programs	David Dewitt
Vice President of Public Affairs	Fred Kuntz
Vice President of Finance	Mark Menard

COMMUNICATIONS

Communications Manager	Tammy Bender	tbender@cigionline.org (1 519 885 2444 x 7356)

CIGI

67 Erb Street West
Waterloo, Ontario N2L 6C2
tel +1 519 885 2444 fax +1 519 885 5450
www.cigionline.org

CHATHAM HOUSE
The Royal Institute of International Affairs

10 St James's Square
London, England SW1Y 4LE, United Kingdom
tel +44 (0)20 7957 5700 fax +44 (0)20 7957 5710
www.chathamhouse.org