International Cyber Norms:
Legal, Policy & Industry Perspectives,
Anna-Maria Osula and Henry Rõigas (Eds.),
NATO CCD COE Publications, Tallinn 2016

CHAPTER 10

Technological Integrity and the Role of Industry in Emerging Cyber Norms

Ilias Chantzos and Shireen Alam

1. Introduction

This article explores the development of cyber norms and illustrates how the cyber security industry cooperates with government agencies and institutions to address an array of cyberspace issues. The discussion then focuses on the development of the principle of technological integrity, an issue which has arisen in the wake of arguments against the weakening of encryption through the installation of hidden functionality in software and hardware products. Symantec is committed to the principle of technological integrity as a critical cyber norm. The article explains some of the key benefits to be derived from technological integrity, as well as the risks if it is not observed. It concludes by laying out a number of recommendations, such as the importance of technological integrity as a norm, the need to develop feasible requirements, the need to remain open to alternative policy options, and the need to balance cyber security and national security.

The article also emphasises that governmental institutions benefit from having the perspectives of the private sector, especially since industry as the primary technology innovator and provider has a greater impact on cyber norms development and consequences than perhaps on norms in other fields.[1] In that regard the

1 Matt Thomlinson, 'Advancing the Discussion on Cybersecurity Norms,' *Microsoft Cyber Trust Blog*, October 21, 2013, https://blogs.microsoft.com/cybertrust/2013/10/21/advancing-the-discussion-on-cybersecurity-norms/.

concept of building cyber norms is unique to the creation of other types of norms. In this article, Symantec applies an overarching approach as it views cyber norms as explicit, agreed on principles, rules of behaviour, procedures, or codes of conduct, that are not necessarily legally binding.[2]

Technological integrity is a principle that promotes privacy measures and shuns the prospect of hidden functionality. Law enforcement agencies around the world are battling against widespread encryption and asserting that a lack of backdoors is causing criminal – including terrorist – investigations to 'go dark'.[3] However, it is nearly impossible to have the luxury of strict security together with surveillance, since beyond a certain point the ability to survey erodes security.[4] In turn, this means that there remains no option for governments to have spying capabilities without creating this opportunity to criminals.

Leading cryptographers have deemed hidden functionality to be unworkable, citing factors including security, feasibility, cost, credibility, and economic repercussions as well as legal and ethical entanglements.[5]

2. Cyber Norms

For the purposes of this article, cyber norms are defined as generally accepted principles of cyber behaviour which set a framework for discussion. They are regarded as inclusive as well as flexible in providing greater options, and they progressively change mind-sets and behaviours.[6] Norms are changeable and capable of strengthening or weakening over a period of time.[7] Cyber norms evolve through policies, products and patterns of behaviour in gaining social acceptance and thus become convention. They can be formalised or enforced through more specific legally binding norms or policy agreements both on the domestic and international levels.

In contrast to the historical evolution of international norms, the development of cyber norms should engage the private sector. While it remains true that only

2 Richard A. Clarke, *Securing Cyberspace through International Norms Recommendations for Policymakers and the Private Sector* (Washington D.C.: Good Harbor Security Risk Management, 2013), 7-10, http://www.goodharbor.net/media/pdfs/SecuringCyberspace_web.pdf.

3 Joshua Kopstein, 'The Feds Don't Need Digital Backdoors – They Can Hack You,' *Aljazeera America*, July 17, 2015, http://america.aljazeera.com/opinions/2015/7/the-feds-dont-need-digital-backdoors-they-can-hack-you.html.

4 Bruce Schneier, 'What is the DoD's Position on Backdoors in Security Systems?' *Schneier on Security*, June 24, 2015, https://www.schneier.com/blog/archives/2015/06/what_is_the_dod.html.

5 Harold Abelson, *et al,* The Massachusetts Institute of Technology, *Computer Science and Artificial Intelligence Laboratory, Keys Under Doormats*: *Mandating Insecurity* by *Requiring Government Access* to *all Data* and *Communications: Computer Science and Artificial Intelligence Laboratory Technical Report, MIT-CSAIL-TR-2015-026 (6 July 2015),* https://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf.

6 Royal United Services Institute, *Cyber Norms of Behaviour: Executive Summary* (15 March 2015), https://www.rusi.org/downloads/assets/Cyber_norms_of_behaviour_report_-_Executive_Summary.pdf.

7 Tim Maurer, *Cyber Norm Emergence at the United Nations – An Analysis of the UN's Activities Regarding Cyber-Security? Discussion Paper 2011-11* (Cambridge, Mass.: Belfer Center for Science and International Affairs, Harvard Kennedy School, 2011), http://belfercenter.ksg.harvard.edu/files/maurer-cyber-norm-dp-2011-11-final.pdf.

nation states can create legally binding norms, the role of industry is unique as a significant amount of the infrastructure of the Internet is privately owned.[8] For example, the private sector has helped to develop agreements such as the Financial Action Task Force on Money Laundering[9] and was also indispensable in securing parliamentary support for its ratification.[10] Similarly, in Europe, the private sector has been consistently consulted by policy-makers in charge of developing and furthering the European Union's policies on network and information security, such as through the European Public-Private Partnership for Resilience[11] and the European Network and Information Security Platform.[12]

Some concrete ways in which the cyber security industry plays a role in influencing cyber norms include: 1) developing the latest technologies and their use; 2) monitoring and informing on the evolution of the threat landscape; 3) engaging in Public Private Partnerships (PPP) and capacity-building efforts; 4) assisting law enforcement in fighting cyber crime; and 5) providing technologies and scalable capabilities to enable countries to implement regulations and public policies.

2.1 Developing Technologies and Use

The cyber security industry plays a pivotal role in developing norms through its products and services markets.[13] It will continue to be involved in the development of norms because of its role in ultimately conceiving of and building products, services, and infrastructure that enable the digital world. Groups focusing on advancing Internet technologies and standards offer good examples of the development of informal international norms through their scale and footprint across international product markets.[14]

Technology is implemented in the context of existing cultures, customs and laws and plays a key role because it determines how norms evolve. In a way, the relationship between norms and technology is interdependent and mutually influential. Due to the constant evolution of technology and the emergence of new practices and behaviours which they enable in cyberspace, new norms are needed to address challenges on the international stage between countries.

The valuable expertise that the private sector carries bestows upon the sector an added advantage in setting technical as well as performance-based standards. By setting high standards for security products, the private sector can set the criteria for

8 Microsoft Corporation, *Five Principles for Shaping Cybersecurity Norms* (2013), http://download.microsoft.com/download/B/F/0/BF05DA49-7127-4C05-BFE8-0063DAB88F72/Five_Principles_Norms.pdf.

9 FATF is an intergovernmental organization established by the G7 in Paris and its membership consists of 36 nations which makes policies for combating money laundering, terrorist financing and other matters related to the integrity of the international financial system.

10 Clarke, *Securing Cyberspace through International Norms Recommendations for Policymakers and the Private Sector.*

11 European Union Agency for Network and Information Security, 'European Public Private Partnership for Resilience (EP3R),' https://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/european-public-private-partnership-for-resilience-ep3r.

12 European Union Agency for Network and Information Security, 'NIS Platform,' https://resilience.enisa.europa.eu/nis-platform.

13 Royal United Services Institute, *Cyber Norms of Behaviour: Executive Summary.*

14 Ibid.

the level of security we can expect. A prime example of this is the Software Assurance Forum for Excellence in Code (SAFECode) of which Symantec is a founding member. SAFECode develops guides for software assurance within its community, which includes some of the largest software providers in the world. In doing so, it provides industry leadership on software assurance as well as clarity on the applicable best practices and recommendations for assuring security, reliability and confidence in the security of software that is purchased.[15]

2.2 Creating Threat Awareness

According to the annual Symantec Internet Security Threat Report (ISTR), there were 317 million new pieces of malware in 2014, or nearly one million new malware variants per day. Social media was confirmed as the fastest-growing vector for malware proliferation.[16] Due to their worldwide coverage, private sector operators are better positioned than most national governments to develop comprehensive near real-time threat awareness. They are also able to share timely and relevant information with appropriate public agencies across multiple jurisdictions, and this proves to be a crucial asset for many nations and their alliances in developing and maintaining their cyber defence postures.

2.3 Public-Private Partnerships and Capacity-Building

Public-Private Partnerships (PPP)[17] and capacity-building[18] are essential elements in the eventual development of cyber norms.[19] A key minimum requirement in the development of norms is consensus, or at least a common understanding among states about the nature of the problem and the need for it to be resolved in a particular way. Capacity-building creates and increases skills, experience, knowledge, and ultimately helps states and other organisations to understand the technological problem and to recognise the need for effective cyber security. PPPs provide much-needed information and help build the necessary expertise at the local level that makes the application and enforcement of norms possible.

Deeper collaboration between the private and public sectors is a crucial asset in cyber security endeavours. Government agencies at all levels should form meaningful partnerships with the private sector. A single player does not have all the answers, resources, skills, assets or scalable capabilities to counter rapidly growing

15 Shaun Gilmore, et al, *Principles for Software Assurance Assessment. A Framework for Examining the Secure Development Processes of Commercial Technology Providers* (*Software Assurance Forum for Excellence in Code* (SAFECode), 2015), http://www.safecode.org/publication/SAFECode_Principles_for_Software_Assurance_Assessment.pdf.

16 The ISTR is the Symantec annual report that analyses a year of observations captured over the Symantec Global Intelligence Network, a set of over fifty million sensors spread over the Internet in more than 150 Countries. The full report and supplemental data are available at Symantec, *The 2015 Internet Security Threat Report (ISTR20)*, vol. 20 (April 2015), https://www4.symantec.com/mktginfo/whitepaper/ISTR/21347932_GA-internet-security-threat-report-volume-20-2015-social_v2.pdf.

17 PPP is a joint government and private venture as it is funded and run through the government as well as a private sector or multiple private companies.

18 Capacity-building is the strengthening and enhancing of skill sets to enable communities as well as organizations to flourish and help keep up with developments and changing times.

19 'Capacity Building in Cyberspace: Taking Stock' (Event Report, European Union, Institute for Security Studies, A seminar organised in the framework of the EUISS Cyber Task Force, Brussels, 19 November 2013), http://www.iss.europa.eu/uploads/media/EUISS_Cyber_Task_Force_Report.pdf.

and evolving cyber threats. Therefore, it is in the interests of all parties to foster different collaboration models that enable the exchange of information, as well as the dissemination of expertise and capacity-building. PPPs serve a vital function as they can facilitate knowledge and capability transference, alleviate shortages of skilled cyber security professionals through collaborative work, and enable real time exchange of cyber threat information.[20]

Capacity-building is not only limited to developing technical skills, but also requires a broader understanding of the technology, policy and threat environment. Without this knowledge, policy-makers are not well equipped to make fully informed decisions. For example, international organisations like the International Telecommunication Union (ITU)[21] and the Organization of American States (OAS)[22] have entered into partnerships with companies to disseminate information to their members on the current threat landscape with an emphasis on particular regions or issues. The objective is to ensure that knowledge on cyber security matters is shared and to build a common understanding among the member nations' policy-makers.

Thus, the contribution of the cyber security industry in the development of national and regional policies creates a local framework in which norms are established and helps ensure their practical implementation. PPPs support capacity-building and policy development by helping states to be better informed and to debate various types of norms. Despite the different stages of technological maturity and various legal and political cultures, an improved common understanding about the nature of cyber security challenges raises the likelihood of reaching consensus on how cyber norms need to reflect that understanding.

2.3.1 Assistance to Law Enforcement in Fighting Cyber Crime

It has been acknowledged that only a decentralised governing method of the cyber domain will present a successful approach.[23] The areas of cyber crime and law enforcement contain the greatest potential for international collaboration in creating cyber norms. For example, although the Budapest Convention[24] is regarded by many states as the international benchmark for combatting cyber crime, its status as a Council of Europe instrument places limits on the extent of its influence globally. It has been suggested by some that a possible avenue to address and resolve this would be to draft a new instrument, which encompasses international issues for all states based on the Budapest Convention.[25]

20 Frederick Wamala, International Telecommunication Union, *The ITU National Cybersecurity Strategy Guide* (September 2011), http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf.

21 International Telecommunication Union, 'Global Partnerships with Industry Players,' http://www.itu.int/en/ITU-D/Cybersecurity/Pages/symantec_and_trend_micro.aspx.

22 Organization of American States, Press Department, *OAS and Symantec to Present Cyber Security Report on June 2nd*. AVI-100/14, 28 May 2014, http://www.oas.org/en/media_center/press_release.asp?sCodigo=AVI-100/14.

23 James Jay Carafano and Eric Sayers, *Building Cyber Security Leadership for the 21st Century*, No. 2218 (Washington D.C.: The Heritage Foundation, 2008), http://www.heritage.org/research/reports/2008/12/building-cyber-security-leadership-for-the-21st-century.

24 *Convention on Cybercrime*, Budapest, 23 November 2001, *Council of Europe Treaty Series*, No. 185, http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf.

25 Royal United Services Institute, *Cyber Norms of Behaviour: Executive Summary.*

Using the common understanding of what constitutes cyber crime that the Budapest Convention provides allows industry to collaborate extensively across different jurisdictions with law enforcements agencies. These operations are often newsworthy and focus against organised cyber crime in infrastructure takedown. For instance, Symantec has formal partnerships with law enforcement organisations around the world including Europol, and participates with several other companies in sharing information on infrastructure used by cyber criminals. It then participates in the process of taking down that infrastructure, thus assisting law enforcement and protecting its customers and the broader community.[26]

2.3.2 Development and Implementation of Public Policies

The cyber security industry has been actively involved in the development of public policies through a number of mechanisms including public consultations. Industry experts are regularly invited to provide policy recommendations as well as functional and technical expertise. In particular, the cyber security industry is often asked to assess policy recommendations, and to provide input on the technical feasibility and practical impact of future policies.

Some recent examples where the cyber security industry has been invited to provide expertise, business perspectives and best practices to policy-makers include the European Union General Data Protection Regulation (GDPR),[27] the Network and Information Security (NIS) Directive,[28] the European cyber security strategy,[29] the European Regulation on Electronic Identities and Trust Services (eIDAS),[30] and the Directive on Attacks Against Information Systems.[31]

Cyber security experts participate in advisory roles for international agencies and organisations which are active in cyber security matters. For instance, the statutes of the European Network and Information Security Agency (ENISA) of the European Union[32] created the Permanent Stakeholder Group (PSG) appointed

26 'Ramnit Cybercrime Group Hit by Major Law Enforcement Operation,' *Symantec Connect*, February 25, 2015, http://www.symantec.com/connect/blogs/ramnit-cybercrime-group-hit-major-law-enforcement-operation; EUROPOL, *Botnet Taken Down through International Law Enforcement Cooperation*, 25 February 2015, https://www.europol.europa.eu/content/botnet-taken-down-through-international-law-enforcement-cooperation.

27 European Commission, *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)*, COM(2012) 11 final (25 January 2012), http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.

28 European Commission, *Proposal for a Directive of the European Parliament and of the Council Concerning Measures to Ensure a High Common Level of Network and Information Security Across the Union*, COM(2013) 48 final (7 February 2013), http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013PC0048&from=EN.

29 European Commission, *Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Cyber security Strategy of the European Union: An Open, Safe and Secure Cyberspace*, JOIN(2013) 1 final (7 February 2013), ec.europa.eu/newsroom/dae/document.cfm?doc_id=1667.

30 European Parliament and Council of the European Union, *Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market and Repealing Directive 1999/93/EC*, 910/2014 (23 July 2014), http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910&from=EN.

31 European Parliament and Council of the European Union, *Directive 2013/40/EU on Attacks against Information Systems and Replacing Council Framework Decision 2005/222/JHA*, 2013/40/EU (12 August 2014), http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=URISERV:l33193&from=EN.

32 European Parliament and Council of the European Union, *Regulation (EC) No 460/2004 Establishing the European Network and Information Security Agency*, 460/2004, (10 March 2004), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:EN:HTML.

every 2½ years to serve in an advisory capacity to the Executive Director with the aim of providing feedback on ENISA's work programme. ENISA's objective consists of improving the cyber security posture across the European single market. ENISA's model of engaging stakeholders from the onset in the decision-making process through preparation of the work programme has proven to be successful.

In addition, the European Cyber Crime Centre (EC3), that sits within the European Police Agency (EUROPOL), has adopted a similar model. The EC3 has different advisory groups which provide advice and support on the exercise of the Agency's mandate. The Internet Security Advisory Group is focused on advising on and facilitating law enforcement action against cyber crime. The EC3 has announced a number of successful operations in collaboration with the cyber security industry that have eliminated criminal infrastructure, such as major botnet takedowns.[33]

The North Atlantic Treaty Organization (NATO) established the Cooperative Cyber Defence Centre of Excellence (CCD COE) in May 2008 and the Centre obtained the status of International Military Organisation in October 2008. The Centre has recognised the compelling need to address emerging challenges on cyber which affect the ability of NATO to achieve its mission and impact the defensive capabilities of NATO nations. Its mission is to enhance cyber defence awareness and security through capability, cooperation and information sharing among NATO member nations and partners.[34] In achieving its mission the NATO CCD COE is partnering with the private sector in activities such as cyber defence exercises.[35]

NATO is also in the process of developing its own cyber security partnership. It initially indicated its readiness to engage with the cyber security industry during the Wales Summit of 2014.[36] The Alliance recognised the importance of working with the private sector in order to better protect NATO and allied infrastructure and to support its ability to conduct operations. A number of activities are already underway focusing on information sharing, capacity-building and promoting technological innovation to address emerging challenges. Within the framework of the NATO cyber security partnership initiatives, Symantec recently signed an agreement with the NATO Communications and Information Agency.[37] The aim of the agreement is to share information on cyber security threats in an effort to develop a collective approach in building trust and defending global networks and critical infrastructure.

The cyber security industry also works with governments to develop standards which meet private and public sector needs. Such collaboration in the United States produced the National Institute of Standards and Technology (NIST) Cybersecurity

33 EUROPOL, *Botnet Taken Down through International Law Enforcement Cooperation*.

34 NATO Cooperative Cyber Defence Centre of Excellence, https://ccdcoe.org/.

35 North Atlantic Treaty Organization, Allied Command Transformation, *Lock Your Shields and Brace for Impact*, 29 October 2013, https://www.act.nato.int/article-2013-2-3.

36 North Atlantic Treaty Organization, *Wales Summit Declaration. Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Wales* (5 September 2014), http://www.nato.int/cps/en/natohq/official_texts_112964.htm.

37 North Atlantic Treaty Organization, *NATO Builds Cyber Alliances*, 11 December 2015, https://www.ncia.nato.int/NewsRoom/Pages/151211_NATO-builds-cyber-alliances.aspx.

Framework, which stems from a Presidential Executive Order released in February 2013 titled, 'Improving Critical Infrastructure Security'.[38] The NIST Cybersecurity Framework consists of guidelines and references to global standards and best practices that help organisations to identify, detect, protect, respond and recover from cyber attacks. The NIST Cybersecurity Framework also creates a common language to ease internal and external communications for cyber security.[39]

3. Emergence of Cyber Norms

Private sector organisations also have been key in supporting human rights norms around Internet freedom. Internet freedom states that existing international human rights standards pertain to the Internet in guaranteeing the right to freedom of expression.[40] An example of this is the Global Network Initiative (GNI), a non-profit organisation composed of various groups including private technology firms, investors, universities, and civil society groups. The GNI has created rules and implementation guidelines for Information and Communication Technologies (ICT) companies to ensure they are supporting the principles of Internet freedom.[41]

A number of non-governmental organisations (NGOs) also engage in the cyber norms discussion. The International Committee of the Red Cross is regarded as an influential non-state promoter of norms on international humanitarian law. The Red Cross has consistently maintained that the law of armed conflict (LOAC) must guide offensive cyber operations.[42] The law of armed conflict prevents unnecessary suffering, and requires proportionality while taking into account military necessity and not impeding on the effective waging of war. The Tallinn Manual (a non-binding document produced by legal and military experts), considered to be an authority on international cyber law, recognises that standalone cyber attacks may constitute armed conflicts depending on the circumstances.[43] If the circumstances fit the criteria then LOAC applies and in a similar manner to a traditional battlefield environment.[44]

38 The White House, Office of the Press Secretary, *Executive Order -- Improving Critical Infrastructure Cybersecurity*, 12 February 2013, https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

39 PricewaterhouseCoopers LLP, *Why You Should Adopt the NIST Cybersecurity Framework* (May 2014), https://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/adopt-the-nist.pdf.

40 United Nations, General Assembly, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue*, A/HRC/17/27 (16 May 2011), http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf.

41 Clarke, *Securing Cyberspace through International Norms Recommendations for Policymakers and the Private Sector.*

42 Information Technology Industry Council, *The IT Industry's Cybersecurity Principles for Industry and Government* (Washington D.C., Information Technology Industry Council, 2011), http://www.itic.org/dotAsset/191e377f-b458-4e3d-aced-e856a9b3aebe.pdf.

43 Michael N. Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge: Cambridge University Press, 2013).

44 Ibid.

An aspect of the current debate focuses on whether the application of LOAC is needed when cyber attacks like the example below cause significant collateral damage. As the LOAC principles continue to develop, there has been talk of establishing norms for reimbursing harmed private sector corporations that are damaged or disrupted by state activities. The main argument of those supporting the application of LOAC is that states must take responsibility for these costs as currently the private sector bears the costs.

The UN Group of Governmental Experts (UN GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security is comprised of 20 nations that are equitably distributed based on geography, and includes nation states regarded as leaders in the field of cyber. The UN GGE released a consensus report which proposes norms of responsible behaviour and includes commentary on applicable principles of international law.[45] These norms require that a state should not conduct or knowingly support ICT activity that intentionally damages or otherwise impairs the use and operation of critical infrastructure. States should also take appropriate measures to protect their critical infrastructure from ICT threats. States should not harm the information systems of the authorised emergency response teams of another state or use those teams to engage in malicious international activity. States should encourage the responsible reporting of ICT vulnerabilities and take reasonable steps to ensure the integrity of the supply chain and prevent the proliferation of malicious ICT tools, techniques or harmful hidden functions.[46] However, attacks on cyber infrastructure by state or non-state actors are illegal under the principles of international law and the UN GGE stated that the UN Charter, including the principles on non-intervention and use of force, are applicable to cyberspace.[47]

The recent consensus achieved at UN GGE has received support from the private sector and is seen as a positive step forward in the norms debate. It should be noted that with regard to the other side of the spectrum (requiring action by countries in defending against cyber damage), nations have been progressively using bilateral, regional or multilateral methods for cyber security towards critical infrastructure. Other countries use the principles of international law directly. It has also been suggested that 'the goal is to consider what norms should apply below the level of armed conflict in cyberspace'.[48]

45 Henry Rõigas and Tomáš Minárik, *2015 UN GGE Report: Major Players Recommending Norms of Behaviour, Highlighting Aspects of International Law,* Incyder News, NATO Cooperative Cyber Defence Centre of Excellence, https://ccdcoe.org/2015-un-gge-report-major-players-recommending-norms-behaviour-highlighting-aspects-international-l-0.html.

46 United Nations, General Assembly, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: note by the Secretary-General*, A/70/174 (22 July 2015), 3, http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174.

47 David Didler, 'Cyber Norm Development and the Protection of Critical Infrastructure,' *Council on Foreign Relations*, July 23, 2015, http://blogs.cfr.org/cyber/2015/07/23/cyber-norm-development-and-the-protection-of-critical-infrastructure/.

48 Ibid.

4. Technological Integrity Principle

There are norms that have achieved a certain degree of consensus, such as those proposed by the UN GGE, as well as other norms emerging in the debate.[49] As technology and public policy challenges continue to develop, it is a normal evolution that norms will need further refinement to address new situations and complexity. The 'technological integrity principle' is an emerging cyber norm to prevent unauthorised modification of information. Integrity also covers trust in the accuracy, completeness and reliability of information.[50]

In this discussion, the focus is on the security aspect of a particular implementation of this principle. The technological integrity principle supports the need for strong security in technology products. It also argues against the creation of hidden functionality or back-door channels in products that would weaken basic security technologies such as encryption, which are also relevant to practices such as whitelisting[51] of cyber threats in cyber protection tools.[52]

In cryptography, the concept of hidden functionality is particularly worrisome as the primary purpose of encryption is to protect the confidentiality and integrity of data. Encryption is the most effective way to achieve data security. In order to read an encrypted file, you must have access to a key or password that enables decryption. Encryption converts electronic data into another form known as cipher text which can then only be deciphered by key holders.[53]

Most organisations today use encryption widely to protect valuable data and communications. Governments rely heavily on encryption to secure strategic communications and protect vital information such as military and diplomatic decision-making. Financial institutions use encryption to ensure the confidentiality and integrity of customer and transaction data.[54] Preserving these technologies is vital. If regulatory measures were created to weaken encryption for legitimate vendors, one must remain mindful that it would do nothing to curb the parallel, 'underground' cryptographic tools developed by malicious users. In essence, the measures would instil a strong sense of insecurity within the legitimate market by sacrificing viable technologies without achieving a meaningful solution for the security issue.[55]

49 For detailed information on the developments in the UN GGE, see chapters 6 and 7.

50 Wamala, International Telecommunication Union, *The ITU National Cybersecurity Strategy*, 13.

51 Whitelisting is the practice by which information, such as credentials, applications and network addresses are added to a list considered trustworthy.

52 Fran Howarth, *Taking Back Control in Today's Complex Threat Landscape …using Application and Change Control to Thwart Attackers: White Paper* (London: Bloor Research, 2011), http://www.mcafee.com/us/resources/white-papers/wp-bloor-application-change-control.pdf.

53 Ahmad Kamal, *The Law of Cyber-Space: An Invitation to the Table of Negotiations* (Geneva: United Nations Institute of Training and Research, 2005), https://www.un.int/kamal/sites/www.un.int/files/The%20Ambassador's%20Club%20at%20the%20United%20Nations/publications/the_law_of_cyber-space.pdf.

54 Mark Hickman, 'Why Financial Institutions Need Data Encryption Education,' *CreditUnionTimes*, October 26, 2014, http://www.cutimes.com/2014/10/26/why-financial-institutions-need-data-encryption-ed.

55 Sara Sorcher, 'Influencers: Stronger Encryption on Consumer Devices Won't Hurt National Security (+Video),' *The Christian Science Monitor*, March 11, 2015, http://m.csmonitor.com/World/Passcode/Passcode-Influencers/2015/0311/Influencers-Stronger-encryption-on-consumer-devices-won-t-hurt-national-security-video.

The weakening of encryption may also mean that some malicious actors would be more likely to exploit the mandated weakness by gaining possession of the master encryption key. Cracking strong encryption is an arduous and resource intensive process. It is therefore not an ideal method for a criminal who wishes to remain swift and undetected, unless it is known that the technology has a built-in vulnerability which streamlines the procedure.[56]

Renowned security expert and cryptographer Bruce Schneier warned that various governments' proposals to ban strong encryption threaten to 'destroy the Internet'.[57] Due to encryption, online banking, e-commerce transactions and exchange of communications can be conducted with security and ease, and there are also less obvious ways in which encryption assists on a daily basis. Schneier observed that, in many nations, it helps dissidents, journalists and human rights workers stay alive, and in an era where widespread computer security is still in its infancy, it is a safeguard measure that works well.[58]

With regard to the installation of backdoors, US FBI Director James Comey has stated:

> '... it makes more sense to address any security risks by developing intercept solutions during the design phase, rather than resorting to a patchwork solution when law enforcement comes knocking after the fact. And with sophisticated encryption, there might be no solution, leaving the government at a dead end – all in the name of privacy and network security.'[59]

Contrasting views were expressed by Vice Chairman of the US Joint Chiefs of Staff Admiral James A. Winnefeld who stated that we would all be better off if our networks were secure. An emphasis was placed on having the peace of mind that secure networks bring, which although posing a harder problem for intelligence, remains a far better option than maintaining vulnerable networks which provide an easy route for any potential security agency investigation.[60]

Backdoors can be introduced into software in a number of ways. A well-crafted stealthy backdoor in one module of the software, such as its cryptographic component, could suffice to compromise many other functionalities. Depending on the intended use of the software, backdoors might materialise at different stages. The negative impact of hidden backdoors cannot be overstated from the perspective of the provider of the technology. Not only does it put at risk the economic activity and create legal liabilities, it also threatens corporate image and brand reputation.

56 Abelson, *et al, Keys Under Doormats.*
57 Rob Price, 'Bruce Schneier: David Cameron's Proposed Encryption Ban Would "Destroy the Internet"', *Business Insider*, July 6, 2015, http://www.businessinsider.com/bruce-schneier-david-cameron-proposed-encryption-ban-destroy-the-internet-2015-7.
58 Ibid.
59 Abelson, *et al, Keys Under Doormats.*
60 Ibid.

5. State Surveillance

Disturbingly, this trend of backdoor channels can lead to civil liberties infringements as some states may identify the mere use of encryption as illicit behaviour. In certain nations, charges against online communities have been laid implying that merely training in communication security was evidence of criminal wrongdoing.[61] States also undermine freedom of expression and privacy when they penalise innocent actors who use and produce tools to facilitate Internet access for citizens. For example, a report by the UN Human Rights Council stated that the rights to 'privacy and freedom of expression are interlinked' and found that encryption and anonymity are protected because of the critical role they can play in securing those rights.[62] Mandated backdoors would needlessly weaken and disrupt technology, undermine both its credibility and its innovation capacities, and provide an ideal environment for malicious actors.

Revelations over state surveillance practices have brought the issue of hidden functionality to the fore. As a result, encryption has become a main topic in the debate over privacy rights.[63] The typical justification behind calls for weakening of Internet technologies is for governments and law enforcement agencies to exercise greater control in tackling cyber crime and terrorism.[64] Both law enforcement and governments have called for access to information,[65] including end-to-end encrypted data, because the mounting use of encryption undermines investigative capabilities. Some proposals have called for communication systems and data storage to be designed to allow for exceptional access. However, this recommendation is unworkable in practice, raises ethical and legal issues, and represents a step backwards in terms of cyber security at a crucial period of time when Internet vulnerabilities are being so thoroughly exploited by criminals.[66]

Granting such exceptional access provisions to governments requires a significant amount of trust that governments will not use the data for untoward purposes and will be able to protect the security of the data itself. Confidential information such as banking and other sensitive proprietary data could be placed at higher risk. There have also been a large number of government data breaches which does not instil confidence that networks and systems are properly protected. Exceptional access provisions in democratic societies would also spur nation states with poor human rights records to do the same.[67]

---

61 United Nations, Human Rights Council, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye*, A/HRC/29/32 (22 May 2015), http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Documents/A.HRC.29.32_AEV.doc.

62 Ibid.

63 Nicole Perlroth, 'Security Experts Oppose Government Access to Encrypted Communication,' *New York Times*, July 7, 2015, http://www.nytimes.com/2015/07/08/technology/code-specialists-oppose-us-and-british-government-access-to-encrypted-communication.html.

64 United Nations, Office on Drugs and Crime, *The Use of the Internet for Terrorist Purposes* (September 2012), https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf.

65 Abelson*, et al, Keys Under Doormats.*

66 Ibid.

67 Perlroth, 'Security Experts Oppose Government Access to Encrypted Communication.'

From a public policy perspective, the natural answer would be to provide law enforcement personnel with the best possible tools in order to investigate crime, subject to due process. However, on scientific analysis, there is a distinguishing feature present between what may be desirable versus what is technically possible.[68]

Concerns about mass surveillance continue to grow due to the increased investments in offensive cyber capabilities by states that view cyberspace as a new domain of warfare. Revelations continue to emerge that many nations engage in large-scale cyber espionage, leveraging technology tools at their disposal or exerting pressure over technology providers in their jurisdiction. Press reports abound on how government intelligence agencies covertly exploit commercial technologies for cyber espionage, much in the same way as cyber criminals and other malicious players would.[69] Such revelations are often met with either officially issued statements, or claims that the purposes were not malicious or fraudulent, but rather served legitimate public policy objectives such as national security and counterterrorism. Regardless, these scenarios highlight the importance of commercially available technologies such as encryption being secure, uncompromised, and free from backdoors. Robust encryption is still regarded as highly effective for protecting electronic data, including from some surveillance and intelligence agencies who have reportedly tried and failed to circumvent them[70] and should be regarded as one of our most important defences.[71]

Aside from mass surveillance, backdoors may also create an environment of conflict which, if attributed to another state, generates political tension and may lead to retaliatory measures. If political tensions between countries already exist, such actions could lead to escalation. In addition, the erosion of public trust in the underlying technology infrastructure reduces its economic value as a driver of innovation, growth and source of social welfare.

68 Abelson*, et al, Keys Under Doormats.*

69 Jacob Appelbaum, Judith Horchert and Christian Stöcker, 'Shopping for Spy Gear: Catalog Advertises NSA Toolbox,' *Spiegel Online International*, December 29, 2013, www.spiegel.de/international/world/catalog-reveals-nsa-has-back-doors-for-numerous-devices-a-940994.html; 'Inside TAO: Documents Reveal Top NSA Hacking Unit,' *Spiegel Online International*, December 29, 2013, http://www.spiegel.de/international/world/the-nsa-uses-powerful-toolbox-in-effort-to-spy-on-global-networks-a-940969.html.

70 Gary McGath, 'Why We Need Encryption Even the NSA Can't Decipher,' *Newsweek*, July 10, 2015, http://www.newsweek.com/why-we-need-encryption-even-nsa-cant-decipher-352073; 'Digital Disease Control. Basic Security Hygiene Goes a Long Way,' *The Economist*, July 12, 2014, http://www.economist.com/news/special-report/21606417-basic-security-hygiene-goes-long-way-digital-disease-control.

71 Rob Price, 'Bruce Schneier: David Cameron's Proposed Encryption Ban Would "Destroy the Internet"'; Alex Comninos and Gareth Seneque, *Cyber Security, Civil Society and Vulnerability in an Age of Communications Surveillance* (Global Information Society Watch, 2014), https://giswatch.org/en/communications-surveillance/cyber-security-civil-society-and-vulnerability-age-communications-sur.

6. Erosion of Trust in Technology: Economic and Societal Impact

Proponents of technological integrity have stated that introducing hidden functionality into technologies must be opposed as it undermines the entire premise of information and communications technologies. Users of technology need an assurance that products serve the purpose and only the purpose for which they were purchased.[72] Having knowledge (or merely suspicion) that a tool could have backdoors would automatically disqualify the product and its vendors to both the consumer and community at large. This would result in devastating economic consequences for the technology sector and users would also lose the benefit of access to the latest and most innovative technologies.

The economic impact would be twofold. First, the cost of devising and implementing a key escrow[73] system on the scale which would be required by the growing Internet would be exorbitant. Second, it has been calculated that revenues would be lost due to global consumers losing confidence in the security of technology products and services.[74] In the absence of encryption, as well as other protective and security technologies, secure transfer protocols (SSL and TLS) would not exist, leaving countless consumers' personal, health and financial information vulnerable to espionage and theft.[75] It also would further compound the already substantial economic impact of the mass surveillance revelations of recent years.[76]

Trust in technology – or at the very minimum an assurance of trust in technology – is paramount as illustrated by recent occurrences. As has been reported in the media, the existence of a complex environment of many entities (suppliers, system integrators, external service providers, etc.) may have provided an opportunity for supply chain circumvention by intelligence agencies who then reinserted the products back into the market place.[77] Mere speculation of involvement was enough for reputable multinational ICT vendors to be forced to issue broad statements, risking significant erosion of their brand reputation and the business consequences that may attach.[78]

Weakening encryption would undeniably have a profound effect on the economy. In the US alone e-commerce has grown from $100 million total annual sales in 1994

72 Appelbaum, Horchert and Stöcker, 'Shopping for Spy Gear: Catalog Advertises NSA Toolbox.'

73 Key escrow system is a data security measure in which keys required to decrypt data are held in escrow, so that in necessary circumstances an authorized third party may be able to gain access.

74 Ryan Hagemann and Josh Hampson, *Encryption, Trust, and the Online Economy. An Assessment of the Economic Benefits Associated with Encryption* (Niskanen Center, 2015), https://niskanencenter.org/wp-content/uploads/2015/11/RESEARCH-PAPER_EncryptionEconomicBenefits.pdf.

75 Hagemann and Hampson, *Encryption, Trust, and the Online Economy. An Assessment of the Economic Benefits Associated with Encryption.*

76 Danielle Kehl, 'OTI Policy Director Kevin Bankston Offers Ten Reasons Why Backdoor Mandates Are a Bad Idea: In Testimony before the House Oversight and Government Reform Committee, Bankston Argues against Legislative "Fixes" for Strong Encryption,' *New America*, April 28, 2015, https://www.newamerica.org/new-america/oti-policy-director-kevin-bankston-offers-ten-reasons-why-backdoor-mandates-are-a-bad-idea/.

77 Robert S. Metzger, 'Cybersecurity and Acquisition Practices: New Initiatives to Protect Federal Information of Civilian Agencies,' *Bloomberg Law*, May 20, 2015, http://www.bna.com/cybersecurity-acquisition-practices-n17179926734/.

78 Appelbaum, Horchert and Stöcker, 'Shopping for Spy Gear: Catalog Advertises NSA Toolbox.'

to over $220 billion in 2014.[79] In Europe, e-commerce figures are even higher in the 28 EU member states with total annual sales of €368.8 billion in 2014.[80] Although it is not possible to attribute a precise figure for this growth to the widespread use of secure encryption, it is improbable that such tremendous growth would have taken place without the underpinning trust engendered by security technologies such as encryption and online secure data transfer protocols.[81]

Beyond the strict impact on businesses and the economy, at the societal level, knowledge that governments and other organisations are able to exploit hidden technological capabilities to monitor citizens would consecrate what can only be described as a structural violation of civil liberties, at least in open societies where public oversight over democratically elected governments is the norm. This is of particular concern as public trust in the government's effective use of technology is indispensable.[82]

Furthermore, such measures could lead to criminals and terrorists gaining access to hidden functionality.[83] If the potential targets of surveillance became users of the hidden functionality, the security, stability and welfare of the public could be placed in grave danger. In that sense, the measures proposed to deter terrorism could come at a potentially higher cost to national and economic security, and this crucial point must not be overlooked. The solution cannot be to structurally weaken the protective technology itself.

7. Recommendations

7.1 Developing Specifications for Feasible Requirements

Government and law enforcement demands for exceptional access provisions entail the serious risk that malicious actors (whether individual criminals, terrorists, or nation states) will gain backdoor access to technologies to attack the very population that agencies have a duty to protect. If exceptional access provisions are placed on industry through a transparent process such as legislation, these measures will force industry to make a difficult choice regarding whether or not to comply. For compliance to be possible, authorities will also need to provide evidence of the indispensable need for such drastic measures, outline their requirements, and produce feasible particulars of the specifications for exceptional access mechanisms that

79 Matt Byrom, 'Data Driven Ecommerce – Infographic,' *Business 2 Community*, June 3, 2014, http://www.business2community.com/infographics/data-driven-ecommerce-infographic-0902379#DZoMLO0USQWDOO5G.97.

80 Ecommerce Europe, 'Infographics,' http://www.ecommerce-europe.eu/facts-figures/infographics.

81 Hagemann and Hampson, *Encryption, Trust, and the Online Economy. An Assessment of the Economic Benefits Associated with Encryption*.

82 Gregory T. Nojeim, 'Cybersecurity and Freedom on the Internet,' *Journal of National Security Law & Policy* 4 (2010), http://jnslp.com/wp-content/uploads/2010/08/09_Nojeim.pdf.

83 Comninos and Seneque, *Cyber Security, Civil Society and Vulnerability in an Age of Communications Surveillance*.

would meet their expectations.[84] In addition, a due process mechanism to secure that access would be required.

Faced with such requirements, industry would need to consider if it is prepared to take the risk of compromising its technology, its brand image, and its duty to its customers with the potential consequence of either departing from a product line or making it unavailable in a particular market. There would be long term consequences other than the loss of economic activity. Experience shows that the prospect of an alternative technological solution that would circumvent local government requirements is very likely.[85]

If a point is reached where technology is effectively compromised, it will not only impact the industry from a business point of view, but it will also mark the end of cyber security as we know it. The result will be that data of governments, businesses and individuals will be in the open and they will be unable to protect themselves using legitimate means. In such a situation, only malicious actors would stand to win, and terrorists, criminals and cyber criminals in particular will find and develop other clandestine and confidential ways to communicate. Or, to put it very simply and quoting the creator of PGP encryption: 'if privacy is outlawed, only outlaws will have privacy'.[86]

7.2 Remaining Open to Alternative Policy Options

Given such compelling arguments against undermining the integrity of security technologies, it may also be worth considering altogether different policies that could achieve the targeting of illegal actors and facilitate the targeted interception of criminal and malevolent communications without compromising the foundations of cyber security and trust in the Internet. Carefully drafted, balanced policy measures could seek to maintain digital traces on the Internet without indulging in mass surveillance, or undermining the integrity of the technology. Advanced and novel investigative tools to collect digital evidence may then be leveraged in a well targeted and narrowly focused manner.[87]

This approach would both increase the legitimacy of the targeted surveillance operations that are necessary in the interest of public security, and create meaningful safeguards against undue, unnecessary or disproportionate practices such as generalised mass surveillance. Discussions in that direction are ongoing in several countries, notably to explore the option of retaining[88] electronic communications data for the purpose of combatting crime and terrorism. Other countries are considering steps associated with the removal of some anonymity associated with some

84 Abelson, *et al, Keys Under Doormats.*

85 'Mass Surveillance Isn't the Answer to Fighting Terrorism,' *New York Times*, November 17, 2015, http://www.nytimes.com/2015/11/18/opinion/mass-surveillance-isnt-the-answer-to-fighting-terrorism.html.

86 Philip R. Zimmermann, *Why I Wrote PGP* (Colorado: Boulder, 1991), https://www.philzimmermann.com/EN/essays/WhyIWrotePGP.html.

87 'German Parliament Votes for New Data Retention Law,' *Deutsche Welle*, October 16, 2015, http://www.dw.com/en/german-parliament-votes-for-new-data-retention-law/a-18786345.

88 Electronic Frontier Foundation, 'Mandatory Data Retention,' https://www.eff.org/issues/mandatory-data-retention.

online and communications transactions. For example, Belgium has proposed the requirement for identification documents in order to purchase a SIM card.[89]

7.3 Careful Balancing of Cyber Security and National Security

Despite the fact that nations feel more vulnerable every day as their reliance on cyber infrastructure increases, governments should avoid falling prey to fear mongering and giving in to the introduction of backdoors.[90] A fine line should be drawn between cyber security and national security issues, as a national security slant may lead to greater civil liberty infringements and subsequent loss of technological integrity.[91]

7.4 Increased Public Awareness and Education

At the broadest level of economy and society, emphasis should be placed on public awareness and education campaigns focusing on cyber security measures beginning at home and highlighting the importance of updating software regularly and the use of up-to-date security and privacy enhancing technologies.[92]

7.5 Maintaining Integrity in Technology

For this to work in practice, trust in the integrity of technology will be indispensable. Symantec firmly calls for the recognition of the principle of technological integrity as a critical cyber norm. More than a public policy consideration and recommendation, this is also the value proposition and core principle on which Symantec's business is built. Therefore, as a company, Symantec not only professes technology integrity, but also abides by it. Our corporate principles are clearly spelled out by Executive Vice-President and General Counsel Scott Taylor that Symantec:

- Does not introduce hidden functionality (back doors) in its technologies;
- Does not whitelist malware in its security solutions;
- Does not keep copies of encryption keys that its corporate customers use, and consequently does not have the ability to comply with requests to produce such keys; and
- Uses the highest known standards for encryption and believes that its encryption technology is secure and has not been undermined.[93]

The purpose and role for introducing the principle of technological integrity as a cyber norm is to make a compelling case for a technology provider's right to make

89 'The Economist Explains: How to Improve International Cyber-Security,' *The Economist*, November 29, 2015, http://www.economist.com/blogs/economist-explains/2015/11/economist-explains-20.

90 Kopstein, 'The Feds Don't Need Digital Backdoors – They Can Hack You.'

91 Ron Deibert has made this argument in Ron Deibert, *Distributed Security as a Cyber Strategy: Outlining a Comprehensive Approach for Canada in Cyberspace* (Calgary: Canadian Defence & Foreign Affairs Institute, 2012), https://citizenlab.org/wp-content/uploads/2012/08/CDFAI-Distributed-Security-as-Cyber-Strategy_-outlining-a-comprehensive-approach-for-Canada-in-Cyber.pdf.

92 Comninos and Seneque, *Cyber Security, Civil Society and Vulnerability in an Age of Communications Surveillance*.

93 Scott Taylor, 'Reaffirming Symantec's Commitment to Security and Privacy for the Online World,' *Symantec Connect*, December 19, 2014, http://www.symantec.com/connect/blogs/reaffirming-symantec-s-commitment-security-and-privacy-online-world.

these claims and abide by them. In addition, the aim is to provide industry operators with an internationally recognised legal basis to oppose government requests and injunctions that would be incompatible with these principles, as well as with due process.

8. Conclusion

The private sector has an important role to play in the development of cyber norms. Despite the fact that cyber norms are, in principle, the result of government-to-government deliberations, the private sector is affected by and influences the development of cyber norms through cooperation and partnership mechanisms. Technological integrity is an emerging cyber norm of growing significance because of the direct link it has with trust in the Internet, technology, market forces, and human rights. The debate on technology integrity is affected by the growing concerns states have about public safety and national security.

The lack of a cyber norm on technological integrity creates an environment in which fundamental rights to privacy are breached, security measures are compromised, and economic growth diminishes. However, as law enforcement and governments become aware of terrorist or criminal plots which are increasingly difficult to detect due to the use of unsuspecting forms of encrypted technology, debates regarding encryption will continue.[94]

Therefore, it is more critical than ever to ensure that policy-makers support the establishment of a cyber norm on technological integrity and achieve consensus around it. They need to be made aware of the inefficiencies and unintended consequences of weakening security technologies such as encryption, and to pursue alternative policies that will enable them to fight crime while protecting human rights, trust and economic growth. Achieving an appropriate balance between cyber security and national security while respecting technological integrity should remain a key public policy objective.

94 Kate Day, 'Why Terrorists Love PlayStation4,' *Politico*, November 25, 2015, http://www.politico.eu/article/why-terrorists-love-playstation-4/; Katrin Bennhold and Michael S. Schmidt, 'Paris Attackers Communicated with ISIS, Officials Say,' *New York Times*, November 15, 2015, https://web.archive.org/web/20151115191248/http:/www.nytimes.com/2015/11/16/world/europe/paris-attackers-communicated-with-isis-officials-say.html; Ellen Nakashima and Greg Miller, 'Why It's Hard to Draw a Line between Snowden and the Paris Attacks. The Debrief: An Occasional Series Offering Reporters' Insights,' *The Washington Post*, November 19, 2015, https://www.washingtonpost.com/world/national-security/why-its-hard-to-draw-a-line-between-snowden-and-the-paris-attacks/2015/11/18/34793ad4-8e28-11e5-baf4-bdf37355da0c_story.html.