PAPER
2017

CYBER-SECURITY, CYBERCRIME AND THE ROLE OF CRIMINAL LAW: A SHORT AND SWEET CONSIDERATION

ALESSIA SCHIAVON

UNIVERSITÀ DEGLI STUDI FIRENZE

Center for Cyber Security and International Relations Studies

CENTER FOR CYBER SECURITY AND INTERNATIONAL RELATIONS STUDIES (CCSIRS)

Centro Interdipartimentale di Studi Strategici,
Internazionali e Imprenditoriali (CCSSII)
Università degli Studi di Firenze
Via delle Pandette 2, 50127, Firenze

https://www.cssii.unifi.it/ls-6-cyber-security.html

Le dichiarazioni e le opinioni espresse nella presente relazione sono unicamente quelle dell'autore e non implicano l'approvazione da parte dell'Università di Firenze, del Centro Interdipartimentale di Studi Strategici, Internazionali e Imprenditoriali o del Center for Cyber Security and International Relations Studies.

Center for Cyber Security and International Relations Studies

CYBER-SECURITY, CYBERCRIME AND THE ROLE OF CRIMINAL LAW: A SHORT AND SWEET CONSIDERATION

Alessia Schiavon

UNIVERSITÀ DEGLI STUDI FIRENZE

Paper

2017

CYBER-SECURITY, CYBERCRIME AND THE ROLE OF CRIMINAL LAW: A SHORT AND SWEET CONSIDERATION

1.Introduction

The convergence of telecommunications and computer technologies brought humanity into a new era known as the information age.
The ubiquitous ICTs revolutionised and integrated almost every facet of modern society, promoting the tendency towards "connecting everything/everyone to everything/everyone". It is now easy to produce and share contents, ideas, information even across geographical divides. As a result people, things and system live hyper-connected in a physical-cyber shared environment called cyberspace.

The term, firstly appeared in sci-fi novel *Neuromancer*, wrote by William Gibson in 1984, evokes a navigable, digital space of networked computers accessible from computer consoles. Subsequently used in a variety of ways, all referred to a new environment created by emerging computer-mediated communication and virtual reality technologies (Dodge & Kitchin, 2001), it now represents a *locus* of interaction and benefits for individuals, government and enterprises. Reaching unprecedented levels of information and individual prosperity as creating enormous opportunities for innovation, it enlights a paradigmatic shift in the way people engage in global economic activity and manage critical infrastructure (Loader, 2003).

At the same time, cyberspace is a medium that has opened a deep store of endless risks associated with cyber-related services. Clearly, this global and dynamic domain made up of information and communication structure represents a new area of conflicts and threats, also considered as the fifth dimension of battlefield, after the traditional domain land, sea, air and space (Schmitt, 2017). Malicious conducts against information systems such as computer systems and networks now have the potential of affecting individuals, countries and the global economy in ways never before unimagined. This expose the weakness

of digital systems and makes also the physical world more vulnerable to new threats.

Consequently, protection of data and networks has rapidly become a high priority (Lucas, 2015) along with the cybercrime deterrence (Westby, 2004).

With the fast continuing evolution of information and communication technologies, growing at a speed unprecedented by any other commodity, nowadays cybersecurity represents a part of a much broader transformation across society and a great challenge that will increase in importance.

2. Cybersecurity and cybercrime: a taxonomy

Cybersecurity is a brand-new and broadly used term. It made its first appearance in the late 1970s in the United States' post Cold War scenario influenced by the technology innovations and the changed geopolitical conditions.

However, it emerged out in the other countries only in the 1990s, firstly used by computer scientist to indicate computer vulnerabilities. Rapidly, in the first decade of the 21th century the debate has shifted from the technical discourse to the threats posed by the digital technologies to society, economic system and national security. (Hansen & Nissenbaum, 2009).

Described "*as meaningful as meaningless*" (Klavans, 2015), it is a useful term that tends to defy precise definition. In fact, even if it has been the subject of academic and popular literature as at the top of global agenda, the lack of a comprehensive definition leads to semantic confusion and a considerable misperception.

Created by the juxtaposition of *cyber* and *security*, it embraces two relevant domains, both notoriously hard to define. Cyber is a prefix derived from "cybernetic", which comes from the Greek adjective *κυβερνητικός* meaning skilled in steering or governing, and evokes the context of cyberspace, a "*the complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical forms*" (ENISA, 2016). It can refer to both the electronic and

physical infrastructure of cyberspace and the line of alphanumeric data—the code—that tells a computer how to act (Deibert, 2013) .On the other hand, security is related to being free from danger or threat as both a process and a result of taking measures (Pricop & Stamatescu, 2018).

In addition, a plethora of terms may be used as synonymous of cybersecurity as information security, ICT security, network security, Internet security (Klimburg, 2012). Whilst they are meaningful to the populace, these terms have nuanced differences.

It well know that cybersecurity becomes increasingly popular as states adopt and revise specific cybersecurity strategies that lead to actions with numerous consequences for a broad range of actors. Security of information network is a very complex and multifaceted sphere of activity, which has different dimensions and various implications, concerning different actors as governments, militaries, industries and individuals. As it refers to the protection of networks and information system against human mistakes, natural disasters, technical failure or malicious attacks, it is also closely connected to fundamental rights and values: security, protection of data privacy, freedom of expression, protection from crime, defence and international peace. According to the perspective of the Copenhagen School's theory of securitization, it has to be considered "*the product of an historical, cultural, and deeply political legacy*" (Buzan et al., 1998).

Referring to a set of issues as varied as distinct, it lacks of a defining clarity. In fact, multiple national and international organizations, bodies and fora as well as researchers have built definitions according to their perspectives and aims.
Inter alia, there are three international definitions.

According to International Communication Unit (ITU) "*cybersecurity refers to the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant*

security risks in the cyber environment. The general security objectives comprise the following: availability; integrity, which may include authenticity and non-repudiation; and confidentiality". (2010)

In addition, "'Cybersecurity', or 'cyberspace security' has been defined as the 'preservation of confidentiality, integrity and availability of information in the Cyberspace'. However, it has also been noted that other properties such as authenticity, accountability, non-repudiation and reliability can be involved in cybersecurity." (Klimburg, 2012)

Then EU Strategy (2013) states "*cyber security commonly refers to the safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure. Cybersecurity strives to preserve the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein*."

It is evident from these sample definitions that cybersecurity works as an all-inclusive term that refers on information security properties, confidentiality, availability and integrity. Specifically, it indicates a proactive and reactive processes working toward the ideal of being free from threats to the confidentiality, integrity or availability of the computers, networks, and information that form part of, and together constitute, cyberspace (Adams et al., 2015).

Added to its broader scope, it carries a sense of ambiguity. There are many terms used to describe crimes or incidents in which IT is the target or where IT plays a major role in the realization of the offense. In fact, cyber security is more commonly surfacing in general discussions along with cybercrime, cyber threats and cyber risk and often these terms are mistakenly considered interchangeable (Boster & Currie, 2014).

Especially cybercrime and cybersecurity are often used interchangeably. Although these concepts have not yet received straightforward definitions, they are to some extent overlapping. Both *à la page* topics in security circles, they are worlds apart. Virtually every security violations involving cyber technology is criminal, but not every crime in cyberspace necessarily involves a breach or violations of cybersecurity.

On one hand, cyber-security can be seen as an umbrella term for numerous, differentiated and fragmented security risks, all of which share one common factor: the use of cyberspace and the Internet. It

usually relates to four major societal threats- crime, cyber war, cyber terrorism and espionage.

On the other hand, cybercrime it is a broad term that refers to offences committed using electronic devices, system or networks. According to Wall, there is much confusion about the risks posed by cybercrime and the consensus that it exists (Wall, 2007). Conceptually, cybercrime may be defined both narrowly, to include offences against computer data and systems but also more broadly, to include offences committed with the help of computer data and systems (Clough, 2010).

Differently, cyber risks concern the IT-dependent risks all cyberspace actors in the various cyber sub-domains are exposed to when performing cyber activities. The misinterpretation of these terms clearly enlight the absence of a fine line between these quite fragmented fields, expression of the new needs of the information society. There is a specific relation between the taxonomy of cybercrime and cyber security and the regulation of cyber risk.

Specifically, cybercrime can be considered as a subset of general concept of cybersecurity (Appazov, 2014). They are involved in a cause-effect relationship which is not limited to cyber security coming from new threats but embraces a continuous interaction that defines inexperienced scenarios. Therefore, the definitional separation of cybercrime from cyber-security in rule-making is widely criticised as apparent in many legal orders and systems (Brenner & Koops, 2006).

3. Regulating the cyber threats: the role of criminal law

Considering the multiple dimensions and complexity of the matter, the debate surrounding cyber threats has been placed within a larger framework, scattered over different areas of law.

In this context the issue of cybercrime has been addressed in numerous legislations and strategy documents as one of the first central pillar of prioritised action. However, it was not easy to bring more computer-specific offences, such as those targeted at the confidentiality, integrity, or availability of computer systems, under traditional provisions. To this end, cyber security policy has firstly been driven by a logic of

criminalisation to protect cyberspace against cyber criminals that attack critical information infrastructures.

Often considered as a remedy for all of society's ill, criminal law has been always considered the primary response of national state to address particularly pressing social problems that other regulatory instruments cannot sufficiently address themselves.

Thus, criminal laws related to computers and the Internet have developed differently in various countries. In fact, at the very beginning, the criminal approach evolved in a piecemeal form, amongst a plethora of legal instruments and conceived apart from cybersecurity.

Whilst an approach existed, key dimensions were missing and it was certainly not coordinated as required for the construction of an effective security ecosystem for cyberspace.

More than any other area of the law, criminal law is tied up both with the cultural values of a nation and with the sovereign exercise of power over citizens on a territory. However, with the growing of information era cyberspace does not respect national boundaries anymore, creating an obvious tension between the global character of the Internet and the nation-based exercise of criminal law. Although many offences are transnational in nature- for instance trafficking in humans, weapons and drugs, money laundering and terrorism-cybercrime presents unique challenges for cross-border criminal investigation and jurisdiction.

As a consequence, criminal laws have proven insufficient and inefficient to face the new challenges posed by the new technologies and to better secure the information society. The practical solution regulators have found to deal with this tension was the harmonisation of legal rules and greater law enforcement cooperation.

The first round of a proper cyber criminalisation was stimulated by the adoption of Budapest Convention on Cybercrime, adopted in 2001, that firstly considered at international level those actions directed against the confidentiality, integrity and availability of computer data and system, comprising illegal access and interception, data and system interference, misuse of devices, along with computer-related offences, content-related and offences related to infringement of copyright and related rights. It is still represents the only binding multilateral treaty instrument aimed at combating cybercrime, although initiatives have

been pursued at various levels, including the United Nations and the European Union.

To date the global picture is one of a certain degree of fragmentation in membership of international and regional instruments related to cybercrime. Notwithstanding, this trend has left still much room for national divergence, emphasizing the difficulty of achieving consensus in criminal legal matters outside of the traditional sphere of political democracy in the nation state (Summers, 2015).

Furthermore, cybercrime grapples with technology. It means new concepts and objects, not traditionally addressed by law. It does not take into account the particularities of information and information technology that are associated with cybercrime and crimes generating electronic evidence. And as matter of fact, technology evolves faster than the law. These reasons have led to a widespread disagreement about the resort to criminal law as an effective component of cyber security policy, calling for a favoured multilateral approach based also on the participation of other "non-governmental" stakeholders in the global fight against cyber threats, given their increasing role in influencing policy outcomes.

Nevertheless only criminal rules are able to create that social climate in which citizens assume responsibility for preventing cybercrime without violating implicit social expectations as to the proper use and scope of criminal liability (Brenner, 2004). Despite its recognised weak points, criminal law still must be considered as an essential instrument of deterrence. If it's true that a basic summary of the historical scene revolving around cyber criminal phenomena shows that the increase of both cyber crime and deterrence remain unbalanced (Xingan Li, 2017), it is only the result of the need to re-think criminal law outside the traditional constraints.

This all focuses attention back to the aims and the extent of cyber-criminalisation. An ongoing updating of the legal framework is necessary as there are little doubt that a more harmonised approach to criminal law regulation might enable broader consensus and wider global reach. These must be at the forefront of cybersecurity strategy.

4. Conclusion

Since the peace of Westphalia the governing authority at the nation-state level was considered to have a monopoly over the so-called public interest, but in modern societies the traditional hierarchy has shifted to a network structure involving new types of actors. In other words it has been recognised that cyberspace is fluid and that a multiplicity of both state and non-state actors can exert cyber power in order to face the risks created by cyberspace.

Therefore, a multi-stakeholder approach is considered to be crucial for managing the challenges of cyberspace and governments are just one the actors involved in this polycentric governance based on a private-public partnership.

In this context criminal law finds itself between the weakness of national sovereignty and the need for an effective response to cyber criminality. However, even if it may not be considered the principal instrument anymore, certainly it represents one of the weapons part of a wide range of regulatory arsenal. The threats posed by the information age still need to be dealt with in the framework of global challenge posed to criminal law by the development and the widespread use of technologies.

Ensuring the participation in the global fight against cybercrime of stakeholder may help. However, harmonizing and updating substantive criminal law still represent a major step in the direction of combating cyberthreats.

Bibliography

Adams, S., Brokx, M., Dalla Corte, L., Galic, M., Kala, K., Koops, B. J., Leenes, R., Schellekens, M., E Silva, K., & Skorvánek, I. (2015), *The governance of cybersecurity: A comparative quick scan of approaches in Canada, Estonia, Germany, the Netherlands and the UK*.,. Available from: https://www.wodc.nl/binaries/2484-volledige-tekst_tcm28-73672.pdf

Appazov A. (2014), *Legal Aspects of Cyber-security*. Available from: http://justitsministeriet.dk/sites/default/files/media/Arbejdsomraader/Forskning/Forskningspu ljen/Legal_Aspects_of_Cybersecurity.pdf

Boister, N., Currie, R.J. (2014) *Routledge Handbook of Transnational Criminal Law*, New York, Routledge.

Buzan, B., Waever O & de Wilde J, (1998) *Security: A new framework for analysis*, Lonodn, Lynne Riener Publishers.

Brenner S. W., (2004) Toward a Criminal Law for Cyberspace: distributed security, *Boston University Journal of Science and Technology Law*, 10, 1-109.

Brenner, S. W., (2012) *Cybercrime and the Law: challenges, issues and outcomes*, Boston, Northeastern University Press.

Brenner, S., Koops B.J. (2006) *Cybercrime and Jurisdiction: A Global Survey*, The Hague, Asser Press.

Calderoni, F., (2010) The European Legal Framework on Cybercrime: Striving for an Effective Implementation, *Crime, Law and Social Change*, 54, 339-357

Clough, J., (2010) *Principles of Cybercrime*, Cambridge, Cambridge University Press.

Contreras, J.L., De Nardis, L., Teplinsky, M., (2013) Mapping Today's Ceybersecurity Landscape, *American University Law Review*, 62, 1113-1130.

Deibert, R. J. (2013) *Black Code: Surveillance, Privacy, and the Dark Side of the Internet*, Toronto, McClelland & Stewart.

Dodge, M., Kitchin, R. (2001) *Mapping Cyberspace*. London, Routledge.

ENISA, (2016) *Definition of Cybersecurity Gaps and overlaps in standardisation*.
Available from: https://www.enisa.europa.eu/publications/definition-of-cybersecurity

European Commission, (2013) *Cybersecurity Strategy of the European Union: An open, safe and secure cyberspace*, Available from: http://eeas.europa.eu/policies/eu-cybersecurity/cybsec_comm_en.pdf.

Hansen, L., Nissenbaum, H., (2009) Digital disaster, Cybersecurity and the Copenhagen School, *International Studies Quarterly*, 53, 1155-1175.

Klavans, J.L. (2015), *Cybersecurity-What's language got do with it?.* White Paper. Available from: https://drum.lib.umd.edu/handle/1903/17165

Koops, B.J. 'Technology and the Crime Society: Rethinking Legal Protection' (2009) 1 Law, Innovation and Technology 93.

Klimburg, A. (2012), *National cyber security framework manual*. Available from: https://www.ccdcoe.org/

ITU (International Telecommunications Union) (2014), Measuring the Information Society Report 2014, Geneva: ITU. Available from: https://www.itu.int/en/ITUD/Statistics/Pages/publications/mis2014.aspx

Loader, B. (2003) *The Governance of Cyberspace: Politics, Technology and Global Restructuring*, London, Routledge.

Lucas, E., (2015) *Cyberphobia: identity, trust, security and the Internet*, London Bloomsbury

Pricop, E., Stamatescu, G., (2016), *Recent Advances in Systems Safety and Security*, Springer International Publishing.

Rowe, D.C., Lunt, B., (2012) *Mapping the cyber security terrain in a research context*. Proceedings of the First Annual Conference on Research in Information Technology Conference, 7-12

Schmitt, M.n., (2017) *Tallinn manual 2.0 on the international law applicable to cyber operations*, Cambridge, Cambridge University Press.

Summers, S., (2015), Eu Criminal Law and the Regulation of Information and Communication Technology, *Bergen Journal of Criminal Law and Criminal Justice*, 3, 48-60

Xinagn L. J. (2017), Cyber Crime and Legal Countermeasures: A Historical Analysis, nternational Journal of Criminal Justice Sciences (IJCJS), 196-207

Wall, D., (2007) *Cybercrime: The transformation of Crime in the Information Age*, Cambridge, Polity.

Wall, D., (2009) *Crime and Deviance in Cyberspace*, London, Routledge.

Williams, M.C., (2007) *Culture and Security: Symbolic Power and the Politics of International Security*, London, Routledge.

Wetsby, J. R., (2004) *International Guide to Cyber Security*, Chicago, American Bar Association.

CENTER FOR CYBER SECURITY AND INTERNATIONAL RELATIONS STUDIES (CCSIRS)

Centro Interdipartimentale di Studi Strategici,
Internazionali e Imprenditoriali (CCSSII)
Università degli Studi di Firenze
Via delle Pandette 2, 50127, Firenze

https://www.cssii.unifi.it/ls-6-cyber-security.html

Center for Cyber Security and
International Relations Studies