Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law
&
Security Review

Cybersecurity in the Internet of Things: Legal aspects

Rolf H. Weber *, *Evelyne Studer*

University of Zurich, Zurich, Switzerland

Keywords:
Cybersecurity
Internet of things
Security challenges
Legal instruments

ABSTRACT

The explosion in the number of smart, connected, and inherently insecure devices is shifting the security paradigm. While the Internet of Things technological shift will require clear legal frameworks, alternative approaches also need to be developed. This article examines the changing legal cybersecurity environment in the Internet of Things context. It discusses selected applicable international regulations as well as alternative approaches to addressing the security issues arising in the Internet of Things.

> "If we know that virtually everything can now be connected to the Internet, we have to recognize its corollary statement: everything that can be connected to the Internet can be hacked"[1],[2]

1. Introduction

Although by now a familiar tale, the ever-growing number of cyber attacks[3] in recent times, with victims ranging from individuals and startups to Fortune 500 companies, law enforcement agencies and governments around the world, continues to cause alarm.[4] The year 2014 was labelled the Year of the Breach[5] and 2015 has been dubbed by some industry commentators as the Year of the Breach 2.0.[6] While these labels may be overly generic, the general (and frightening) picture that this paints is one of more frequent, more sophisticated and more severe cyber attacks. In addition, there has reportedly been a progressive shift to more destructive as well as more personal[7] attacks.[8]

* Corresponding author. University of Zurich, Zurich, Switzerland.
E-mail address: rolf.weber@rwi.uzh.ch (R.H. Weber).

http://dx.doi.org/10.1016/j.clsr.2016.07.002

[1] Sue Poremba, *The Internet of Things Has a Growing Number of Cybersecurity Problems* (January 2015), http://www.forbes.com/sites/sungardas/2015/01/29/the-internet-of-things-has-a-growing-number-of-cyber-security-problems/#1c56d59c4a47.

[2] All websites were last accessed on 25 May 2016.

[3] According to the ITU, a cyber attack occurs when "a threat breaches security controls around a physical or an information asset" (ITU National Cybersecurity Strategy Guide (September 2011), p. 16, http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf).

[4] See Khyati Jain, *These Top 7 Brutal Cyber Attacks Prove No One is Immune to Hacking – Part I* (September 2015), http://thehackernews.com/2015/09/top-cyber-attacks-1.html. See also the real-time cyberattack map of Norse Corp (a California-based cybersecurity firm) at http://map.norsecorp.com/.

[5] See Tara Seals, *2014 So Far: The Year of the Data Breach* (August 2014), http://www.infosecurity-magazine.com/news/2014-the-year-of-the-data-breach/; Ponemon Institute Survey, 2014: A Year of Mega Breaches (January 2015), http://www.ponemon.org/blog/2014-a-year-of-mega-breaches; Chad Hemenway, *A look back at 2014: The year of the data breach* (January 2015), http://www.cyberrisknetwork.com/2015/01/01/look-back-2014-year-of-the-breach/.

[6] See Jay Johnson, *If 2014 Was The Year Of The Data Breach, Brace For More* (January 2015), http://www.forbes.com/sites/danielfisher/2015/01/02/if-2014-was-the-year-of-the-data-breach-brace-for-more/#495d5a6c6ac3; Chris Paoli, *2015 Security Review: Top Hacks, Breaches and Cyber Scams* (December 2015), https://rcpmag.com/articles/2015/12/01/top-security-hacks.aspx.

[7] See Dan Lohrmann, *2015: The Year Data Breaches Became Intimate* (December 2015), http://www.govtech.com/blogs/lohrmann-on-cybersecurity/2015-the-year-data-breaches-became-intimate.html.

[8] To gain a sense of the variety and number of attacks currently being perpetrated, see, e.g., the recent report of the European Union Agency for Network and Information Security "ENISA Threat Landscape 2015" (January 2016), p. 5, https://www.enisa.europa.eu/

A number of forces are responsible for the steep rise in hostile cyber intrusions and unauthorized network breaches. The explosion of new technologies and growth of societal dependency on globally interconnected technology, combined with the automation and commoditization of cyberattack tools,[9] cyber attacker sophistication, and low entry barriers into the cybercrime market[10] are no doubt amongst the key ones.[11]

The emergence of the Internet of Things has also dramatically altered the cyber threat landscape.[12] As discussed in further detail below, the Internet of Things phenomenon entails the ever-expanding integration of (generally) poorly secured devices (*things*) into networks through the connections to the Internet and to each other.[13] The mass-scale deployment of such inherently vulnerable devices creates exponentially more vectors for attack,[14] which, in turn, introduce an exponentially greater order of security risks.[15] Thus, the paradigm shift brought on by the Internet of Things appears to have created the perfect security storm,[16] calling the validity of traditional legal cybersecurity approaches into question on numerous and profound levels.[17]

In answer to this challenge, this article seeks to examine the changing face of cybersecurity in the Internet of Things – as one of the greatest near term security challenges – from a legal perspective.[18]

This article is structured as follows. Section 2 sets the stage by exploring the concepts of cybersecurity and the Internet of Things. Section 3 investigates the security challenge brought on by the increasingly crowded and dynamic Internet of Things ecosystem. Section 4 analyses applicable international regulations that are relevant to cybersecurity. Finally, Section 5 briefly discusses alternative regulatory approaches to addressing the security challenge in the Internet of Things.

2. Basic concepts and terminology

2.1. *Cybersecurity*

2.1.1. *(Absence of a) definition*

The first step to framing the issue of security in cyberspace is to understand concretely the meaning of the term 'cybersecurity'. This appears to be a challenging endeavour since, to date, no standard or universally accepted definition of the term exists.[19] To make things more complex, there is neither a clear consensus on the exact meaning of the term, nor is there even an agreement on its spelling.[20] On that issue, the Internet Society remarked that "as a catchword, cybersecurity is frighteningly inexact and can stand for an almost endless list of different security concerns, technical challenges, and 'solutions' ranging from the technical to the legislative".[21]

activities/risk-management/evolving-threat-environment/enisa-threat-landscape/etl2015https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape/etl2015.

[9] See ENISA, Threat Landscape 2015 (n. 8), p. 6 and p. 54.

[10] See Cassandra Kirsch, *The Grey Hat Hacker: Reconciling Cyberspace Reality and the Law*, Northern Kentucky Law Review (2014), p. 383 ff, p. 385, http://www.academia.edu/4721959/Grey_Hat_Hacking_Reconciling_Law_with_Cyber_Reality; Anthony Wing Kosner, *Target Breach Of 70 Million Customers' Data Used Bargain Basement Malware* (January 2014), http://www.forbes.com/sites/anthonykosner/2014/01/15/blackpos-malware-used-in-target-attack-on-70-million-customers-retails-for-1800/#402f5612530d; see also the blog post on the Infosec Institute blog: *25 Ways to Become the Ultimate Script Kiddie* (August 2015), http://resources.infosecinstitute.com/25-ways-to-become-the-ultimate-script-kiddie/.

[11] See Samantha Bradshaw, *Combatting Cyber Threats: CSIRTs and Fostering International Cooperation on Cybersecurity*, Global Commission on Internet Governance Paper Series (December 2015), p. 6, https://www.cigionline.org/publications/combatting-cyber threats-csirts-and-fostering-international-cooperation-cybersecurity; see also the recent report of McAfee Labs "2016 Threat Predictions" (2015), p. 21, McAfee Labs Report 2016 Threats Predictions.

[12] See Debra Donston-Miller, *The Internet of Things Poses New Security Challenges* (February 2014), http://www.forbes.com/sites/sungardas/2014/02/25/the-internet-of-things-poses-new-security-challenges/#30b9afde2696; Omner Barajas, *How the Internet of Things (IoT) Is Changing the Cybersecurity Landscape* (September 2014), https://securityintelligence.com/how-the-internet-of-things-iot-is-changing-the-cybersecurity-landscape/; Jonathan Camhi, *Vulnerable IoT devices are changing the cybersecurity landscape* (February 2016), http://uk.businessinsider.com/iot-devices-are-changing-cybersecurity?r=US&IR=T.

[13] See the recent study of Hewlett Packard, Hewlett Packard Internet of Things Research Study, 2015 Report (2015), p. 3, http://www8.hp.com/h20195/V2/GetPDF.aspx/4AA5-4759ENW.pdf; see also the report of the Internet Society, Internet Society, The Internet of Things: an Overview (2015), p. 2, https://www.internetsociety.org/sites/default/files/ISOC-IoT-Overview-20151014_0.pdf.

[14] See Christopher J. Rezendes & W. David Stephenson, *Cybersecurity in the Internet of Things* (June 2013), https://hbr.org/2013/06/cyber-security-in-the-internet/.

[15] See Hewlett Packard, Internet of Things Research Study (n. 13), p. 3; Internet Society, The Internet of Things: an Overview (n. 13), p. 2.

[16] See Gary Davis, *Brace Yourselves: The 'Perfect Security Storm' is Coming* (September 2015), https://blogs.mcafee.com/consumer/august-threats-report-2015/.

[17] See Christopher J. Rezendes & David W. Stephenson, *Cybersecurity in the Internet of Things* (June 2013), https://hbr.org/2013/06/cyber-security-in-the-internet; ENISA, Threat Landscape 2015 (n. 8), p. 68; McAfee Labs Report, 2016 Threat Predictions (n. 11), p. 7.

[18] This article will not examine the (crucial) privacy issues that arise in connection with the Internet of Things. For a general overview of such issues, see Rolf H. Weber, *Internet of Things: Privacy Issues Revisited*, Computer Law & Security Review (2015), p. 618–627.

[19] On this issue, see e.g.: Nazli Choucri, Elbait Gihan Daw & Madnick Stuart, *What is Cybersecurity? Explorations in Automated Knowledge Generation* (2012), http://ecir.mit.edu/images/stories/Madnick%20et%20al%20Comparison%20Paper%20for%20ECIR%20workshop%20-%20Fig%201%20also%20FIXED%20v2.pdf; Tim Maurer & Robert Morgus, *'Cybersecurity' and Why Definitions Are Risky* (November 2014), http://isnblog.ethz.ch/intelligence/cybersecurity-and-the-problem-of-definitions; Trey Herr & Allan Friedman, *Redefining Cybersecurity*, The American Foreign Policy Council (January 2015), http://www.afpc.org/publication_listings/viewPolicyPaper/2664.

[20] See Choucri, Gihan Daw & Stuart (n. 19).

[21] Internet Society, Some Perspectives on Cybersecurity: 2012 (2012), p. 1, http://www.internetsociety.org/doc/some-perspectives-cybersecurity-2012.

For the purpose of this article, the definition of the International Telecommunication Union (ITU) will be used.[22] The ITU defines cybersecurity as "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 organisation and user's assets".[23] Organisations' and user's assets include in particular "connected computing devices",[24] such as Internet of Things devices.

According to the ITU, the ultimate goal of cybersecurity is to ensure that the security properties of organizations' and users' assets are attained as well as maintained against relevant security risks in the cyber environment.[25] General security objectives include those of (i) confidentiality, (ii) integrity, and (iii) availability (also known as the CIA triad in the information security industry[26]).[27] Confidentiality means that information is not improperly disclosed to unauthorized individuals, processes, or devices.[28] Integrity refers to information being protected against unauthorized modification or destruction without authorization.[29] Availability refers to timely and reliable access to data and information for authorized users.[30]

2.1.2. *Cyber threat landscape*

2.1.2.1. *Possible categorization*. One way to start a discussion about security is with the identification of the threats[31] that challenge it. This section will briefly lay out the contemporary cyber threat landscape, by using a linear approach that distinguishes threats by (i) threat agents, (ii) threat tools, and (iii) threat types.[32] It should be noted that while such categorization is useful for the purpose of the following discussion, it does not (aim to) paint a comprehensive picture of the very complex nature and characteristics of cyber threats.

2.1.2.2. *Threat agents*. A wide array of external and internal agents threatens cybersecurity. Threat agents can be sophisticated or unsophisticated. They include nation states, profit-driven cyber criminals, criminal organizations, hackers (black, grey or white hats[33]), hacktivists, extremists and insiders. These categories are not mutually exclusive.[34]

The motivations of threat agents vary significantly. Agents act for political reasons (e.g. destroying, damaging, disrupting, or taking control of targets, engaging in cyber espionage or political protest).[35] They may additionally have financial motivations (e.g. stealing valuable personal or financial data, such as the social security numbers and credit card numbers that can be used for identity theft and fraud[36]) as well as sociocultural motivations (e.g. engaging in attacks with philosophical goals or for purposes of publicity, curiosity or ego).[37]

2.1.2.3. *Threat tools*. Threat agents typically make use of similar threat tools. The basic security breach tools encompass malware[38] and its variants (ransomware,[39] viruses, worms, Trojan horses, etc.) and botnets.[40]

Malware is a general category which generally refers to any code or software covertly installed on a device without authorization. It includes malicious code designed for the purposes of damaging, disrupting, or generally inflicting some kind of illegitimate action on data, systems, or networks.[41] A further variation is ransomware, a type of malware that restricts access to the infected device or system in some way.[42] While a ransomware attack leaves the system working with all data present, it renders certain files inaccessible or no longer usable.[43] Cyber attackers then demand a ransom, generally in Bitcoin, to restore the original integrity of the files.[44] Botnets usually consist of command and control (C&C) servers and networks of computers infected by malware that can be managed remotely.[45]

According to the 2015 ENISA Threat Landscape Report, malware represented the number one cyber threat in 2015.[46] Ransomware was and, according to industry experts, will remain

[22] Although the ambiguity of the term cybersecurity and the absence of a standard universal definition bear important consequences, such consequences will not be examined in this article.

[23] ITU Definition of cybersecurity, http://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx.

[24] *Ibid.*

[25] *Ibid.*

[26] See Thomas J. Shaw, Information Security and Privacy: A Practical Guide for Global Executives, Lawyers and Technologists (2011), p. 18 f., Axel M. Arnbak, Securing private communications: Protecting private communications security in EU law: fundamental rights, functional value chains and market incentives, Amsterdam, (2015), p. 30 and 155 f.

[27] ITU Definition of cybersecurity, http://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx.

[28] See Shaw (n. 26), p. 18.

[29] *Ibid.*

[30] *Ibid.*

[31] A threat in this context means any potential for an entity to exploit vulnerability or otherwise cause harm (Shaw (n. 26), p. 161).

[32] See the report of the European Parliament, Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses, Study for the LIBE Committee (2015), p. 26 ff, http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536470/IPOL_STU%282015%29536470_EN.pdf.

[33] See Jay P. Kesan & Carol Mullins Hayes, *Bugs in the Market: Creating a Legitimate, Transparent, and Vendor-focused Market for Software Vulnerabilities*, University of Illinois College of Law Legal Studies Research Paper No. 16–18 (February 2016), p. 13.

[34] *Ibid.*

[35] *Ibid.*

[36] Shaw (n. 26), p. 162.

[37] *Ibid.*

[38] The term malware is short for malicious software.

[39] See Susan W. Brenner, Cybercrime and the Law: Challenges, Issues, and Outcomes (Northeastern University 2012), p. 36 ff; Kesan & Mullins Hayes (n. 33), p. 3.

[40] The term botnet is a combination of the terms robot and network.

[41] See *Defining Malware: FAQ*, https://technet.microsoft.com/en-us/library/dd632948.aspx; Shaw (n. 26), p. 164.

[42] See McAfee Labs Report, 2016 Threat Predictions (n. 11), p. 35.

[43] *Ibid.*

[44] *Ibid*; see also Kim Zetter, *Hacker Lexicon: A Guide to Ransomware, the Scary Hack That's on the Rise* (September 2015), https://www.wired.com/2015/09/hacker-lexicon-guide-ransomware-scary-hack-thats-rise/.

[45] See ENISA, Threat Landscape 2015 (n. 8), p. 25–26; see also the post by Norton, *Bots and Botnets – A Growing Threat*, http://us.norton.com/botnet/.

[46] See ENISA, Threat Landscape 2015 (n. 8), p.19.

a major and rapidly rising threat.[47] Botnets were flagged as one the main elements in cyber crime consumerization (the "botnet-for-hire" business model, in which attacks can reportedly be ordered for as little as USD 38/month, underlining the important disproportion between attack cost and damage potential[48]).[49] Recently, botnets were also reported to feature among the preferred weapons of cyber criminals.[50] With regard to threats specifically to the Internet of Things, both malware and botnets were cited as top emerging threats in the ENISA Report.[51]

2.1.2.4. *Threat types*. Threats to cybersecurity involve threats concerning information modification or misuse, information destruction, unauthorized access, data breaches, data theft and denial-of-service (DoS).[52]

Although all facets of the CIA triad (see above Section 2.1.1) are threatened by cyber attacks, McAfee Labs predicted that the threats to *integrity* of systems and data would constitute one of the most significant new vectors of attack in 2016.[53] This is because, as described by McAfee Labs, "confidentiality and availability attacks are loud, brute, and obvious. They break things and expose data – causing embarrassment, inconvenience, and some losses. Integrity attacks are stealthy, [and] selective, [. . .]. Instead of doing damage or making off with vast amounts of sensitive data, they instead focus on carefully changing particular elements within transactions, communications, or data to gain a significant benefit".[54]

2.2. *Internet of Things*

2.2.1. *Definition and notion*

The term Internet of Things (IoT) was first coined by British technology pioneer Kevin Ashton in 1999 to describe a system in which objects in the physical world could be connected to the Internet through sensors.[55]

Although no standard or universally accepted definition of the IoT exists, unlike with cybersecurity (see above Section 2.1.1), there is a consensus on its concept.[56] As such, the IoT has become "a popular term for describing scenarios in which internet connectivity and computing capability extend to a variety of objects, devices, sensors, and everyday items",[57] including cars, refrigerators, thermostats, health monitors and roads. As such, the IoT adds the dimension of 'any *thing*' to information and communications technologies (ICTs), which already feature 'any *time*' and 'any *place*' aspects of functionality[58] and transforms traditional objects into 'smart' ones.[59]

Various definitions of the IoT are currently floating around. Important differences among definitions emerge depending on the perspective taken to examine the IoT. According to the frequently cited definition of the ITU, the IoT is "a global infrastructure for the information society, enabling advanced services by *interconnecting* (physical and virtual) things based on existing and evolving interoperable information and communication technologies"[60] (emphasis added). As such, the ITU's definition primarily focuses on the interconnectivity attribute of the IoT without any reference to the Internet.[61]

In terms of its significance, there is little arguing with the fact that the IoT technological shift has far-reaching implications and massive disruptive potential. Various kinds of applications are emerging in the IoT context, which are increasingly coming to permeate our everyday existence.[62] As such, the IoT spans industries and domains such as smart health (e.g. patient surveillance), smart transport (e.g. self-driving cars), smart living (e.g. baby monitoring), smart buildings (e.g. intelligent thermostat), smart food (e.g. supply chain management/control), smart energy (e.g. smart grid), smart industry (e.g. temperature sensor controls) and even smart cities (e.g. traffic congestion monitoring).[63]

2.2.2. *(Brief) technical background*

The IoT currently relies on a number of different enabling technologies.[64] These encompass radio frequency identification

[47] See McAfee Labs Report, 2016 Threat Predictions (n. 11), p. 24. In 2015, the US Federal Bureau of Investigation (among many others), issued an alert according to which all types of ransomware are on the rise, https://www.fbi.gov/news/stories/2015/january/ransomware-on-the-rise.

[48] See Noreen Seebacher, *You Can Bring Down a Website for $38* (June 2015), http://www.cmswire.com/information-management/you-can-bring-down-a-website-for-38/.

[49] See ENISA, Threat Landscape 2015 (n. 8), p. 26.

[50] See Dave McMillen, *Why Botnets Remain the Go-To Weapon for Cybercriminals* (March 2016), https://securityintelligence.com/why-botnets-remain-the-go-to-weapon-for-cybercriminals/.

[51] See ENISA, Threat Landscape 2015 (n. 8), p. 75.

[52] See Jay P. Kesan & Carol Mullins Hayes (n. 33), p. 3.

[53] See McAfee Labs Report, 2016 Threat Predictions (n. 11), p. 34.

[54] *Ibid.*

[55] See Kevin Ashton, *That 'Internet of Things' Thing*, RFID Journal (June 2009), http://www.itrco.jp/libraries/RFIDjournal-That%20Internet%20of%20Things%20Thing.pdf.

[56] See Internet Society, The Internet of Things: an Overview (n. 13), p. 11.

[57] *Ibid.*, p. 7.

[58] ITU–T Recommendation Y.2060, Overview of the Internet of Things (06/2012), p. 2, http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=11559.

[59] See Ala Al-Fuqaha, Mohsen Guizani, Mehdi Mohammadi, Mohammed Aledhari & Moussa Ayyash, *Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications*, 17 IEEE Communication Surveys & Tutorials No. 4, (2015), p. 2347, http://www.comsoc.org/files/Publications/Tech%20Focus/2016/iot/3.pdf.

[60] Rec. ITU-T Y.2060 (06/2012) (n. 58), p. 1.

[61] See Internet Society, The Internet of Things: an Overview (n. 13), p. 11.

[62] See Ovidiu Vermesan et al, *Internet of Things Strategic Research and Innovation Agenda*, in: Internet of Things – From Research and Innovation to Market Deployment, O. Vermesan & P. Friess (eds), River Publishers Series in Communication, p. 30 ff, http://www.internet-of-things-research.eu/pdf/IERC_Cluster_Book_2014_Ch.3_SRIA_WEB.pdf; Stan Schneider, *Understanding The Protocols Behind The Internet Of Things* (October 2013), http://electronicdesign.com/iot/understanding-protocols-behind-internet-things.

[63] See Scott Shackelford, Anjanette Raymond, Rakshana Balakrishnan, Prakhar Dixit,Julianna Gjonaj & Rachith Kavi, *When Toasters Attack: A Polycentric Approach to Enhancing the Security of Things*, Kelley School of Business Research Paper No. 16-6 (January 2016), p. 9; Ovidiu Vermesan et al (n. 62), p. 30 f.

[64] See Benjamin Khoo, *RFID as an Enabler of the Internet of Things: Issues of Security and Privacy*, 2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing (2011), p. 709, http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6142169; Zahraddeen Gwarzo, *Security*

(RFID) systems, as well as wireless sensor networks (WSNs), machine-to-machine (M2M) systems, big data, cloud services and smart applications.[65]

RFID technology is one of the key building blocks for the IoT.[66] It is a technology used to uniquely, accurately and automatically identify, track and locate assets through wireless radio waves (as opposed to optical barcodes).[67] RFID systems are composed of two components: (i) a transponder (RFID tag), which is attached to a "thing" (which can be practically anything, from a computing device to a grocery product, even an animal or a human being[68]) and serves as a data carrier, and (ii) a reader or registration device, which reads the data of the transponder.[69] From a security perspective, RFID is a highly vulnerable component, as no higher level of intelligence can be enabled on it.[70]

A popular industry proposal for the infrastructure of the IoT is based on an Electronic Product Code (EPC). [71] In such an infrastructure, 'things' are objects that carry RFID tags with a unique EPC. [72] The infrastructure can offer and query EPC Information Services (EPCIS), both locally and remotely to and from subscribers. [73] Instead of saving the information on a RFID tag, distributed servers on the Internet can supply the information through linking and cross-linking with the help of an Object Naming Service (ONS).[74]

3. Security implications of the Internet of Things

3.1. *Challenges occasioned by the Internet of Things*

The continued development and deployment of IoT systems largely rest on one critical factor: security.[75]

While the issue of security in the context of information technology is of course not new, the IoT introduces new and unique challenges.[76] As summarized by an industry expert[77] in the following syllogism: "Anything connected to the Internet can be hacked. *Everything* is being connected to the Internet. [Thus,] everything is becoming vulnerable [. . .]".[78] Hence, it would seem that any device in this emerging *Internet of Everything*[79] will inevitably be compromised at some point. From this perspective, the question is not so much *whether* but *when* a thing will be hacked.

A key security challenge in the IoT context is the increase of the overall attack surface[80] for malicious attacks,[81] as compared to isolated (i.e. non-connected) systems. This may be attributed in particular to the following factors:

First, due to the ease and (relatively low) cost of developing IoT devices as well as to the high adoption rate of smart connected things, the IoT ecosystem will continue to steadily grow in volume and variety in the coming years.[82] Various companies and organizations have made projections regarding the number of things that will be connected to the Internet in the coming years. A conservative prediction by Gartner, for example, is that the number of networked devices in use worldwide will reach 20.8 billion by 2020.[83] Cisco's estimates are around 50 billion IoT connections by 2020.[84] Huawei projects that such connections will hit the 100 billion figure by 2025.[85] While the differences in these predictions make any specific figure questionable, the overall picture is clearly one of significant growth.[86] The direct result is that there will soon be a massive amount

and Privacy Issues in Internet of Things, in: Jusletter IT (2016), p. 1.

[65] See De-Li Yang, Feng Liu & Yi-Duo Liang, *A survey of the Internet of Things*, Proc. 1st ICEBI (2010), p. 358; Gwarzo (n. 64), p. 1.

[66] See Matthew Trotter, *RFID Makes Internet of Things Come to Life, machine design* (May 2014), http://machinedesign.com/iot/rfid-makes-internet-things-come-life.

[67] For further details see Rolf H. Weber & Romana Weber, Internet of Things, Legal Perspectives (2010), p. 2 f.; Gwarzo (n. 64), p. 3.

[68] See Gwarzo (n. 64), p. 3.

[69] *Ibid.*

[70] Alessio Botta, Walter de Donato, Valerio Persico & Antonio Pescapé, *On the Integration of Cloud Computing and Internet of Things*, 2014 International Conference on Future Internet of Things and Cloud (2014), p. 29.

[71] See Rolf H. Weber, *Internet of Things – Need for a new legal environment?*, Computer and Law & Security Review (2009), p. 522 f.

[72] *Ibid.*

[73] *Ibid.*

[74] *Ibid.*

[75] See the report of Capgemini Consulting "Securing the Internet of Things Opportunity: Putting Cybersecurity at the Heart of the IoT" (2015), p. 3, https://www.capgemini-consulting.com/resource-file-access/resource/pdf/securing_the_internet_of_things.pdf.

[76] See the report of Cisco "Securing the Internet of Things: A Proposed Framework", http://www.cisco.com/c/en/us/about/security-center/secure-iot-proposed-framework.html.

[77] Rod Beckstrom, Cybersecurity Expert and former President and Chief Executive Officer of Internet Corporation for Assigned Names and Numbers (ICANN).

[78] Speech by Rod Beckstrom at the London Conference on Cyberspace (November 2011), https://www.icann.org/en/system/files/files/beckstrom-speech-cybersecurity-london-02nov11-en.pdf.

[79] Regarding the (increasingly used) term Internet of Everything, see e.g. Tim Bajarin *The Next Big Thing for Tech: The Internet of Everything* (January 2014), http://time.com/539/the-next-big-thing-for-tech-the-internet-of-everything/.

[80] A system's attack surface can be defined as the subset of its resources that an attacker can use to attack the system (Pratyusa K. Manadhata & Jeannette M. Wing, *An Attack Surface Metric*, in: IEEE Transactions on Software Engineering (2010), p. 4.)

[81] See Bradshaw (n. 11), p. 8; see also the EY report on "Cybersecurity and the Internet of Things" (2015), p. 8 ff, http://www.ey.com/Publication/vwLUAssets/EY-cybersecurity-and-the-internet-of-things/$FILE/EY-cybersecurity-and-the-internet-of-things.pdf; Internet Society, The Internet of Things: an Overview (n. 13), p. 21.

[82] See McAfee Labs Report, 2016 Threat Predictions (n. 11), p. 13.

[83] See the Gartner Press release "*Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent From 2015*" (November 2015), http://www.gartner.com/newsroom/id/3165317.

[84] See the Cisco white paper "IoT System Security: Mitigate Risk, Simplify Compliance, and Build Trust" (2015), p. 1, http://www.cisco.com/c/dam/en/us/products/collateral/se/internet-of-things/iot-system-security-wp.pdf.

[85] See the Huawei white paper "Connectivity Index 2016" (2016), p.43, http://www.huawei.com/minisite/gci/pdfs/Global_Connectivity_Index_2016_whitepaper.pdf .

[86] See Internet Society, The Internet of Things: an Overview (n. 13), p.4.

of Internet-enabled devices operating dynamically that will require proper protection.

Second, owing to the fast development of the IoT that occurred without appropriate consideration for security issues, smart devices are generally inherently insecure.[87] A 2015 study by Hewlett Packard showed that 70 percent of IoT devices contain serious vulnerabilities.[88] These vulnerabilities stem in particular from the following:[89]

- **Lack of transport encryption**: Many IoT devices are simple "unit-taskers" and all devices have cost, size, and processing constraints (additional processing power adds cost).[90] This means that most devices will not support the processing power required for strong security measures and secure communication, such as encryption (e.g. an 8-bit microcontroller, the function of which is merely to switch lights on and off, cannot support the industry standard SSL to encrypt communications[91]) and may transmit data in clear text.[92] This is, of course, particularly problematic in the IoT context, given the massive amounts of data that are being transmitted between smart devices, the cloud and mobile applications.[93]
- **Insufficient authentication and authorization**: Authentication/authorization can be insufficient due to poor password requirements, careless use of passwords (lowest hanging fruit for hackers), lack of periodic password resets and failure to require re-authentication for sensitive data.[94] Weak authentication and authorization compromise the entire IoT system.[95]
- **Insecure Web interface**: Security issues with the web interface include persistent cross-site scripting, poor session management and weak or plain default credentials (which can be exploited by enumerating accounts until access is granted).[96]
- **Insecure software and firmware**: due to resource constraints, most IoT devices are designed without the ability to accommodate software or firmware updates (which would add cost). As a result, vulnerability patching is difficult (if not impossible).[97] This is, of course, problematic since it is "virtually impossible"[98] to design vulnerability-free software.[99] In addition, where updates are available, many devices do not appear to use encryption for software updates downloads.[100]

Hence, the explosion in the number of connected devices, coupled with the IoT's numerous security deficiencies is shifting the security paradigm from hardware to the networks that process the devices. In terms of security, each thing is a potential entry point for an attack, which creates a great imbalance in what appears to be a cybersecurity arms race: While defenders must secure every single part of the ecosystem, all that is needed for an attacker is a single entry way into the network. As such, "anything networked becomes a link in the long chain which is only as strong as its weakest link".[101]

3.2. *Vulnerability and risk elements*

Risks relating to IoT devices are numerous and diverse. As such, the IoT creates the risk that information will be misused, that unauthorized access to devices will be gained, that devices will be controlled or damaged and that attacks on other systems will be facilitated.[102] While these risks exist with traditional computers and computer networks (see above Section 2.1.2), they raise unique concerns in the IoT context.[103,104]

Digital attacks on connected devices not only pose risks in the digital world, they also create physical risks to the devices themselves (property damage) as well as, even more critically, safety risks for the IoT users (namely the risk of physical harm and even death).[105] This is perhaps best understood if one considers that there will be an estimated 10 million self-driving cars on the road within a few years.[106] If vulnerabilities

[87] See Gwarzo (n. 64), p. 3; Hewlett Packard, Internet of Things Research Study (n. 13).

[88] See Hewlett Packard, Internet of Things Research Study (n. 13).

[89] *Ibid.*; see also the Symantec White Paper "Insecurity in the Internet of Things" (March 2015), https://www.symantec.com/content/dam/symantec/docs/white-papers/insecurity-in-the-internet-of-things.pdf.

[90] See the Verizon report "2015 Data Investigations Report" (2015), p. 63, http://www.verizonenterprise.com/DBIR/2015/.

[91] *Ibid.*

[92] See Shackelford, Raymond, Balakrishnan, Dixit, Gjonaj & Kavi (n. 63), p. 14; Gwarzo (n. 64), p. 2; Hewlett Packard, Internet of Things Research Study (n. 13); Internet Society, The Internet of Things: an Overview (n. 13), p. 25.

[93] See Gwarzo (n. 64), p. 3.

[94] See the list by The Open Web Application Security Project (OWASP) of the Top 10 Insufficient Authentication/Authorization, https://www.owasp.org/index.php/Top_10_2014-I2_Insufficient_Authentication/Authorization.

[95] See Gwarzo (n. 64), p. 3.

[96] See Brad Russell, *Data Security Threats to the Internet of Things* (November 2015), https://www.parksassociates.com/blog/article/data-security-threats-to-the-internet-of-things; Gwarzo (n. 64), p. 3.

[97] See Hewlett Packard, Internet of Things Research Study (n. 13); Internet Society, The Internet of Things: an Overview (n. 13), p. 23.

[98] See Jay Pil Choi, Chaim Fershtman & Neil Gandal, *Network Security: Vulnerabilities and Disclosure Policy*, 58 Journal Of Industrial Economy (2010), p. 869.

[99] See Choi, Fershtman & Gandal (n. 98), p. 869.

[100] See Gwarzo (n. 64), p. 3.

[101] See Shackelford, Raymond, Balakrishnan, Dixit, Gjonaj & Kavi (n. 63), p. 14.

[102] See Gwarzo, (n. 64), p. 1.

[103] See Jon Oltsik, *The Internet of Things: A CISO and Network Security Perspective* (2014), p. 4 f., http://www.cisco.com/c/dam/en_us/solutions/industries/docs/energy/network-security-perspective.pdf; see also the FTC Staff Report "Internet of Things: Privacy and Security in a Connected World" (January 2015), p. 10, https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

[104] A mere glimpse at the Shodan website for instance (https://www.shodan.io/) (also known as the "dark Google" or the "scariest search engine on the Internet"), which navigates Internet's back channels to enable users to find Internet-connected devices and systems, gives a pretty clear idea of the potential damage that could be done if the search results were to fall in the wrong hands.

[105] See Shackelford, Raymond, Balakrishnan, Dixit, Gjonaj & Kavi (n. 63), p 13 f.

[106] See John Greenough, *10 million self-driving cars will be on the road by 2020* (July 2015), http://www.businessinsider.com/report-10-million-self-driving-cars-will-be-on-the-road-by-2020-2015-5-6?IR=T.

in such devices are found and exploited by cybercriminals, not only will road safety be impacted, the lives of persons will be gravely threatened.[107] Pacemakers are another good example of the serious physical threats that are created by insecure connected devices (see below).[108]

The risk not only lies in the possibility of attackers taking control of devices but also in relation to the massive and rapidly growing store of data that is being generated by smart objects. Indeed, devices with extensive data gathering capabilities are increasingly being introduced into spaces commonly considered private, even intimate (i.e., organizations, homes, cars, and, through wearable and ingestible technologies, even bodies).[109] The result is that colossal amounts of data, including potentially intimate or business-critical data, is being generated, collected, and stored.[110] Inevitably, due in particular to the great value of data,[111] this creates a great potential for misuse.[112]

A spate of recent (publicized) hacks and breaches shed light on the very real concerns relating to the rise of Internet-connected devices. As such, for instance, in the field of smart health (which is “perhaps the most susceptible to the security implications of [the] IoT”[113]), a security researcher discovered a flaw in hospital pumps that could have allowed hackers to deliver potentially fatal drug doses to patients over the Internet.[114] Another highly-publicised incident concerned critical vulnerabilities in a large number of connected baby monitors. These vulnerabilities were exploited by hackers to carry out a number of malicious activities (including shouting at toddlers and their parents, disabling the monitors or, on the contrary, changing the camera settings to turn the monitors into spy cams).[115] In one instance, an attacker published live feeds from a thousand baby monitors onto a website called “Big Brother is Watching You”.[116] As mentioned, connected cars are also vulnerable to hacking. In July 2015, Fiat Chrysler Automobiles announced the recall of 1.4 million Jeep vehicles after it identified that Internet-connected internal systems (dashboard functions, steering, transmission and braking systems) could be hacked from a remote laptop to carry out any number of nefarious activities, including unlocking the doors or even shutting down the car in motion.[117] Further, children are also at risk in the IoT world since (connected) toys are being hacked as well. The electronic toy-maker VTech admitted to a breach by an “ethical hacker” that affected 6.3 million children.[118] The hacker stole the children’s names, home addresses, pictures and chat logs and warned the toy-maker to rapidly fix the security flaws.[119]

In light of the above, enhancing and ensuring robust security in the IoT networks and systems is a matter of urgency.

4. Legal framework

4.1. *Preliminary remarks*

In the face of this perfect security storm, the cyber legal and regulatory landscape is constantly and rapidly evolving in an attempt to address such concerns as the exposure to threats becomes known.

Cybersecurity is now routinely cited by policy-makers and consistently finds itself at the top of political agendas. Governments from around the world have (at least, officially) endeavoured to secure cyberspace and its systems.[120] They have devised and adopted countless cybersecurity strategies.[121] In addition, they have made concerted efforts to implement new or enhanced cyber-oriented laws and regulations, in an effort to adapt to the shifting environment and address the need for coordinated action in light of the inherently transnational nature of the issue and the resulting need to achieve cybersecurity on a global level.[122]

Despite the flurry of activity and initiatives relating to cybersecurity, there is, as of this writing, no truly universal, comprehensive instrument in this field. Rather, the global picture is one of fragmented participation in agreements at the international and regional level and of a patchwork quilt of sectoral laws at the national level. Amidst this patchwork of protection, there appears to be some confusion as to what legislation to allude to. Nonetheless, widely adopted legal instruments that address the challenges of cybercrime and security in cyberspace do exist.

[107] See McAfee Labs Report, 2016 Threat Predictions (n. 11), p. 33.

[108] See FTC Staff Report 2015 (n. 103), p. viii.

[109] *Ibid.*, p. 55.

[110] See McAfee Labs Report, 2016 Threat Predictions (n. 11), p. 7. By one estimate, the digital universe will grow to approx. 5200 gigabytes of data for every human on the planet by 2020, http://www.emc.com/leadership/digital-universe/2012iview/executive-summary-a-universe-of.htm.

[111] As is frequently mentioned, data is as the “oil of the 21st century”; see in particular the World Economic Forum report “Personal Data: The Emergence of a New Asset Class” (January 2011), p. 5, http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf.

[112] See the blog post by Bruce Schneier, *Data Is a Toxic Asset* (March 2016), https://www.schneier.com/blog/archives/2016/03/data_is_a_toxic.html.

[113] See Shackelford, Raymond, Balakrishnan, Dixit, Gjonaj & Kavi (n. 63), p. 21.

[114] See Fergal Gallagher, *Hackers Could Remotely Send Fatal Doses to Patients Via Flawed Hospital Pumps* (June 2015), http://www.techtimes.com/articles/59180/20150609/hackers-remotely-send-fatal-doses-patients-via-flawed-hospital-pumps.htm.

[115] See Conor Gaffey, *Web of Insecurity: Hacked Baby Monitors Highlight Perils of Internet of Things* (September 2015), http://europe.newsweek.com/web-insecurity-hacked-baby-monitors-highlight-perils-internet-things-332464.

[116] See Kashmir Hill, *Watch out, new parents – Internet-connected baby monitors are easy to hack* (September 2015), http://fusion.net/story/192189/internet-connected-baby-monitors-trivial-to-hack/.

[117] See Mike Spector & Danny Yadron, *Regulators Investigating Fiat Chrysler Cybersecurity Recall* (July 2015), http://www.wsj.com/articles/fiat-chrysler-recalls-1-4-million-vehicles-amid-hacking-concerns-1437751526.

[118] See Andrea Stroppa, *Are web-enabled toys safe?* (December 2015), http://www.weforum.org/agenda/2015/12/are-web-enabled-toys-safe.

[119] *Ibid.*

[120] See Bradshaw (n. 11), p. 6.

[121] As at 25 May 2016, 72 out of 193 ITU Member States had a publicly available National Cybersecurity Strategy, see http://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies-Repository.aspx.

[122] See ENISA, Threat Landscape 2015 (n. 8), p. 5.

The following sections analyse two such legal instruments, i.e. the Council of Europe Convention on Cybercrime (Budapest Convention), as the first binding international legislative treaty to regulate cybercrime (Section 4.1), and the recently adopted Network and Information Security Directive (NIS Directive), as the first binding EU-wide legislative tool to regulate the broader field of "network and information security" (Section 4.3).

4.2. *Budapest convention*

4.2.1. *Background*

The Budapest Convention[123] was adopted in 2001 and entered into force in 2004.[124] It is considered to be the oldest binding and widest adopted legal instrument in the field of cybercrime.[125]

The Budapest Convention is open to worldwide membership. To date, 48 states have become parties to the Convention, including several non-EU members, amongst whom are Australia, Canada, Japan and the US.[126] Additionally, six states are signatories and 12 have been invited to accede.[127] Despite such wide adoption, the Convention is not yet truly global. Significantly, it excludes in large part developing countries,[128] which means that a noteworthy segment of Internet users do not fall within its scope.[129]

4.2.2. *Objectives and content*

As set forth in the preamble, the main objective of the Budapest Convention is to pursue a "common criminal policy" against cybercrime by "adopting appropriate legislation and fostering international co-operation".[130] The aim of the Convention is to "deter action directed against the confidentiality, integrity and availability of computer systems, networks and computer data as well as the misuse of such systems, networks and data" by criminalizing such conduct and by facilitating detection, investigation, and prosecution at the domestic and international level.

Pursuant to the explanatory memorandum of the Budapest Convention, the rationale for a common criminal policy is that, while the "most effective means" to prevent unauthorised access is "effective security measures", a comprehensive response must also include deterrence, i.e. "the threat and use of criminal law measures".[131]

The Budapest Convention provides for four categories of substantive offences, including offences against (i) the confidentiality, integrity and availability of computer data and systems (Art. 2–6) and (ii) computer-related offences (Art. 7–8). The explanatory report specifies that the criminal offences defined under Articles 2–6, which include hacking and computer trespass (under the general concept of "unauthorised intrusion"),[132] are intended to protect the confidentiality, integrity and availability of computer systems.[133] As such, the importance of (protecting) the CIA triad is clearly reflected in the Budapest Convention.[134] The term "computer systems" is defined in the Budapest Convention as "any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data" (Art. 1). Such a broad definition captures nearly all digital devices,[135] including IoT devices in particular.

In terms of scope, the categories of offences of the Budapest Convention do not encompass the full range of cybercrimes (that are defined as offences in the national criminal codes of member states).[136] This may be attributable to the fact that certain offences were likely not anticipated (which is not surprising since the Convention was drafted over a decade ago) but may also indicate that international consensus could not be reached with respect to certain offences.[137] Even so, the Budapest Convention provides for the possibility of supplementing or amending the Convention (Art. 46). Furthermore, other bodies or organization can address the substantive offences of the Budapest Convention, provided that such activity does not conflict with the Convention.[138] In practice, this provides the means for member states to update their cybercrime legislation, despite the fact that the Budapest Convention has remained static.[139]

As regards the broader issue of cross-border cooperation, the Budapest Convention requires parties to cooperate with each other "to the widest extent possible" for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of electronic evidence (Art. 23). The goal of effective cross-border cooperation is to "minimise impediments to the smooth and rapid flow of information and evidence"[140] on an international level. This general obligation to cooperate is further reaffirmed in subsequent provisions, which lay down the principles of extradition (Art. 24), mutual assistance (Art. 25) and "spontaneous information" (Art. 26), which entitles parties to receive relevant data without a prior request.

[123] Cybercrime Convention – Council of Europe Convention on Cybercrime, CETS 185, Budapest November 2001, http://www.coe.int/fr/web/conventions/full-list/-/conventions/rms/0900001680081561.

[124] For a detailed discussion of the Budapest Convention, see the Explanatory Report, Convention on Cybercrime, opened for signature 23 November 2011, ETS No 185, https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800cce5b (cited Explanatory Report).

[125] http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185; for further details on the Budapest Convention see Jonathan Clough, *A World of Difference: The Budapest Convention on Cybercrime and the Challenges of Harmonization*, Monash University Law Review (2014), p. 698.

[126] http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=jnOd8Vj5.

[127] *Ibid*.

[128] *Ibid*.

[129] See Jianhong Liu, Bill Hebenton, Susyan Jou, Handbook of Asian Criminology (2012), p. 58.

[130] http://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561.

[131] See Explanatory Report (n. 124), p. 9; see also Arnbak (n. 26), p. 61.

[132] See Explanatory Report (n. 124), p. 9.

[133] *Ibid*, p. 8.

[134] The preamble of the Budapest Convention also expressly refers to the CIA-triad.

[135] See Arnbak (n. 26), p. 62.

[136] See Clough (n. 125), p. 702.

[137] See Explanatory Report (n. 124), p. 7; Clough (n. 125), p. 703.

[138] See Explanatory Report (n. 124), p. 57.

[139] See Clough (n. 125), p. 703.

[140] See Explanatory Report (n. 124), p. 42.

4.2.3. *Critical evaluation*

The Budapest Convention was the first (ambitious) attempt to harmonize legal frameworks to combat cybercrime.[141]

Despite its role in providing an internationally recognized framework for international harmonization and its influence on a great deal of the current EU cybercrime legislation,[142] over a decade after its coming into force, the Budapest Convention has been described by its critics as largely outdated and in great need of reform. Various reasons have been cited for this claim of obsolescence, including the fact that the Convention is based on types of offenses which originated at the time of its drafting (i.e. the late 1990s) and therefore (naturally) does not take into account new attack tools (such as botnets and ransomware).[143] Furthermore, the Convention does not specifically mention virtual economic crime.[144] As a result, there have been calls for a general revision of the Budapest Convention or even the adoption of a new (and truly) universal treaty on cybercrime, for instance at the UN level.[145]

4.3. *NIS directive*

4.3.1. *Preliminary remarks*

The EU has set out to combat cybercrime and bolster cybersecurity through various actions. In this context, the EU has adopted and devised the following recent instruments and strategy: (i) the NIS Directive, (ii) the General Data Protection Regulation (GDPR) and (iii) the EU Digital Single Market strategy (DSM) (which synthesizes initiatives on security and data protection in particular).[146] Additionally, in view of the importance of private sector involvement in the cybersecurity arms race (which results from the fact that the majority of network and information systems are privately operated),[147] the EU plans to launch a public–private partnership on cybersecurity in 2016, as announced in the DSM in 2015.[148] The following sections will focus on the NIS Directive.

4.3.2. *Policy context*

Already in 2001, the European Commission had highlighted the increasing importance of network and information security (NIS) in its *Communication Network and Information Security: Proposal for a European Policy Approach*.[149]

In 2004, the European Network and Information Security Agency (ENISA) was established with the objective to promote “a culture of network and information security for the benefit of citizens, consumers, business and public sector organisations in the European Union”.[150] ENISA was mainly tasked with tracking information security risks, facilitating cooperation and information-sharing between public and private sector entities, and assisting member states in their development of industry-specific cybersecurity strategies.[151]

Two years later, in 2006, the European Commission adopted a *Strategy for a Secure Information Society*, with the goal of developing a culture of NIS in Europe.[152] The main elements of the 2006 strategy, including the security and resilience of ICT infrastructures, were endorsed in a European Council Resolution.[153]

In line with the 2006 strategy, in 2009, the European Commission adopted a *Communication on Critical Information Infrastructure Protection*, which focused on the protection of Europe from cyber disruptions by enhancing security and resilience.[154]

In 2012, the European Commission held an online public consultation on *Improving NIS in the EU*.[155] The key outcome of the consultation was the showing of wide support among stakeholders for improving NIS across the EU.[156] The (published) results of the consultation were used to help inform the proposal for the 2013 *Proposal for a Network and Information Security Directive* (as discussed further below).[157]

In 2013, the European Commission published the *Cybersecurity Strategy of the European Union: An open, safe and secure cyberspace*[158] (Strategy). The Strategy sets forth the EU’s approach for best preventing and responding to cyber disruptions and attacks. It does not centralize supervision, but rather encourages member states to organize and respond to cyber

[141] See Clough (n. 125), p. 701.
[142] *Ibid.*, p. 732 and p. 736; Arnbak (n. 26), p. 62.
[143] See Liu, Hebenton & Jou (n. 129), p. 60.
[144] See Clare Chambers-Jones, Virtual Economies and Financial Crime: Money Laundering in Cyberspace (2012), p. 202.
[145] See Liu, Hebenton & Jou (n. 129), p. 58; Martin Gill, The Handbook of Security (2014), p. 334.
[146] See the European Commission Press release (May 2015), http://europa.eu/rapid/press-release_IP-15-4919_en.htm.
[147] Draft Directive on Network and Information Security (Examination of the final compromise text in view to agreement), Amended recital 15, http://www.consilium.europa.eu/en/press/press-releases/2015/12/pdf/st15229-re02_en15_pdf/.
[148] See European Commission, Press release (n. 146).
[149] Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions, Network and Information Security: Proposal for A European Policy Approach (2001), http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52001DC0298.
[150] Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency (2004), http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:EN:HTML.
[151] *Ibid.*
[152] Communication Network and Information Security: Proposal for a European Policy Approach (n. 149).
[153] Council Resolution 2007/068/01.
[154] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection (2009), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF.
[155] Consultation on Network and Information Security – Publication of individual responses (June 2013), https://ec.europa.eu/digital-single-market/news/consultation-network-and-information-security-publication-individual-responses.
[156] 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 (2013), http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52013PC0048.
[157] Consultation on Network and Information Security (n. 155).
[158] Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (2013), http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=1667.

threats at the national level.[159] The Strategy sets forth a series of actions aimed at enhancing cyber resilience and reducing cybercrime among other things.[160] It also grants ENISA the power to cooperate with the public and private sectors in order to advance the adoption of NIS standards and support with the development of guidelines that reflect industry best practices.[161]

In conjunction with the release of the Strategy, the European Parliament and the European Council proposed a *Network and Information Security Directive* to "ensure a high common level of network and information security standards among member states" (NIS Directive Proposal).[162] The proposed directive aims at improving the security of the Internet and private networks and information systems on which the digital society relies. Prior to the introduction of the NIS Directive Proposal, the European Commission had noted the absence of any effective mechanism at EU level for promoting effective cooperation and collaboration and for facilitating trusted information sharing on NIS incidents and risks among member states. This, the European Commission had warned, created the risk of uncoordinated regulatory interventions, incoherent strategies and divergent standards, resulting in insufficient protection across the EU.[163]

Two years later, on 7 December 2015, the European Parliament and the European Council reached a political agreement on the European Commission's proposed measures to increase online security in the EU.[164]

On 18 December 2015, the final compromise draft of the NIS Directive was released (Draft NIS Directive).[165] On 17 May 2016 the European Council formally adopted the NIS Directive.[166] Upon publication of the adopted text in the Official Journal of the European Union and its entry into force (which is expected to occur in August 2016), member states will have 21 months to transpose the NIS Directive into national legislation (Art. 21 Draft NIS Directive).[167] Following this period, they will have another six months to identify and establish a list of providers of essential services in their territory that are within the Directive's scope (Art. 3a Draft NIS Directive) (see below Section 4.3.3).[168]

4.3.3. *Objectives and content*

As mentioned, the NIS Directive is the first EU-wide legislation on cybersecurity.[169] Its core objectives are to achieve minimum regional (EU) harmonization and to make the online environment more trustworthy,[170] which ultimately supports the establishment of the DSM.[171]

The NIS Directive explicitly refers to the CIA triad in its definition of NIS security, which provides that "the ability of networks and information systems to resist, at a given level of confidence, any action that compromises the *availability*, authenticity, *integrity* or *confidentiality* of stored or transmitted or processed data or the related services offered by or accessible via that network and information systems" (Art. 3 Draft NIS Directive) (emphasis added).

The Directive sets forth the following main objectives and measures to bring about the desired high common level of NIS in Europe (Art. 1 Draft NIS Directive).[172]

i. **Improved National Cybersecurity Capabilities**: Member states are required to adopt a national cybersecurity strategy (Art. 5 Draft NIS Directive) (NIS Strategy). This includes creating a policy and a regulatory environment for information security. The NIS directive further requires member states to establish institutional capacities. As such, member states must designate national competent authorities for the implementation and enforcement of the NIS Directive (Art. 6 Draft NIS Directive) as well as a national Computer Security Incident Response Teams (CSIRT)[173] responsible for handling incidents and risks (Art. 7 Draft NIS Directive).

ii. **Improved EU-level Cooperation**: The NIS Directive creates a Cooperation Group with the objective of supporting and facilitating strategic cooperation and the exchange of information between member states (Art. 8a Draft NIS Directive).

iii. **Security and Incident Notification Requirements**: In order to "promote a culture of risk management and ensure that the most serious incidents are reported" (Recital Draft NIS Directive), the NIS Directive imposes security and incident notification requirements on two groups of entities, i.e. (A) operators of essential services, and (B) digital

[159] See Scott J. Shackelford, Scott Russell & Jeffrey Haut, *Bottoms Up: a Comparison of Voluntary Cybersecurity Frameworks*, UC Davis Business Law Journal (2016), p. 20.

[160] http://www.consilium.europa.eu/en/policies/cyber-security/.

[161] See Shackelford, Russell & Haut (n. 159), p. 20.

[162] NIS Directive Proposal (n. 156).

[163] *Ibid*.

[164] See the European Commission post, *Network and Information Security Directive: co-legislators agree on the first EU-wide legislation on cybersecurity* (December 2015), https://ec.europa.eu/digital-single-market/news/network-and-information-security-directive-co-legislators-agree-first-eu-wide-legislation.

[165] See the European Council press release, *EU steps up cybersecurity: member states approve agreement* (December 2015), http://www.consilium.europa.eu/fr/press/press-releases/2015/12/18-cybersecurity-agreement/.

[166] See the European Council press release, EU-wide cybersecurity rules adopted by the Council (May 2016), http://www.consilium.europa.eu/en/press/press-releases/2016/05/17-wide-cybersecurity-rule-adopted/.

[167] See the European Commission post (n. 164).

[168] See the European Council press release (n. 165); see also the European Commission press release, *Commission welcomes agreement to make EU online environment more secure* (December 2015), http://europa.eu/rapid/press-release_IP-15-6270_en.htm.

[169] See the European Commission post (n. 164).

[170] Trust in online services is a pre-condition for the EU Digital Single Market; absent a robust cybersecurity strategy (among other things), there can be no trust (see http://www.consilium.europa.eu/en/policies/digital-single-market-strategy/). If trust is undermined, the technology industry suffers setbacks and technologies cannot reach their full potential (see Shackelford, Raymond, Balakrishnan, Dixit, Gjonaj & Kavi (n. 63), p. 25).

[171] See the European Commission post (n. 164).

[172] See the European Commission press release (n.168) as well as the European Commission's post on cybersecurity (April 2016), https://ec.europa.eu/digital-single-market/en/cybersecurity.

[173] CSIRTs are often seen as the "firefighters" of cyberspace (see Bradshaw (n. 11), p. 6, citing Atif Ahmad, Justin Hadgkiss and A.B. Ruighaver, *Incident response teams – Challenges in supporting the organisational security function*, Computer & Security Law Review (2012), p. 643, http://www.sciencedirect.com/science/article/pii/S0167404812000624).

service providers. A recital explains that this distinction and the resulting differentiated treatment is due to the differences between operators of essential services (which have a direct link with physical infrastructure) and digital service providers (which have a cross-border nature) (Amended Recital linked to Chapter IVa).

An operator of essential services is a public or private entity that provides a service that cumulatively: (a) is essential for the maintenance of critical societal and/or economic activities; (b) depends on network and information systems; and (c) is such that an incident to its network and information systems would have significant disruptive effects on the provision of such service (Art. 3a Draft NIS Directive). The NIS Directive includes an annex that sets forth the type of entities that it would treat as operators of essential services (Annex II Draft NIS Directive). Not surprisingly, the annex includes industries such as energy suppliers, transport service providers, large financial institutions, utilities, healthcare providers and digital infrastructure providers.[174]

Annex III of the NIS Directive identifies three categories of digital service providers, i.e. online marketplace providers, online search engines and cloud computing services. Contrary to the requirement to identify operators of essential services (see above), member states will not be required to establish and publish lists of entities that are considered to be digital services providers. Companies will thus have to determine for themselves whether or not they fall within the scope of the NIS Directive and are subject to its requirements. It should be noted that, though it seems the three categories will be interpreted rather widely, the NIS Directive explicitly exempts small or micro enterprises from its requirements, to "avoid imposing a disproportionate financial and administrative burden".[175] Therefore, the Directive will not apply to digital service providers with fewer than 50 employees and an annual balance sheet total of less than 10 million Euros.[176] Furthermore, pursuant to a recital, hardware manufacturers and software developers are not considered digital service providers (nor operators of essential services).[177] Importantly, digital service providers based outside the EU, which offer services within the EU, will fall under the scope of the Directive.

A) **Operators of essential services** will be subject to (1) security requirements and (2) mandatory breach notification requirements. Technical and organizational security measures will have to comply with state of the art measures that are appropriate to ensure a level of security of networks and information systems appropriate to the risk presented (Art. 14 Draft NIS Directive). As regards the requirement to provide notice, member states will have to ensure that essential service operators notify national authorities of security breaches that reach a certain threshold of harm, i.e. breaches that have "a significant impact on the continuity of the essential services they provide" (Art. 14 Draft NIS Directive).

To ascertain the significance of an incident, operators will have to consider at a minimum the following parameters (Art. 14 Draft NIS Directive): (a) the number of users relying on the services provided by the entity; (b) the dependency of other sectors on the service provided by the entity; (c) the impact that incidents could have, in terms of degree and duration, on economic and societal activities or public safety; (d) the market share of the entity; (e) the geographic spread with regard to the area that could be affected by an incident; and (f) the importance of the entity for maintaining a sufficient level of the service, taking into account the availability of alternatives for the provision of that service.

B) **Digital service providers** will also be subject to security and mandatory breach notification requirements, albeit far less stringent ones than those faced by essential services operators. Member states will have to ensure that digital service providers be required to report security incidents that have "a substantial impact on the provision of a service . . . they offer within the Union" (Art. 15a Draft NIS Directive).

To determine whether the threshold of harm is met, digital services providers will be required to consider in particular the following factors (Art. 15a Draft NIS Directive): (i) the number of users affected by the incident (in particular users relying on the service for the provision of their own services); (ii) the duration of the incident; (iii) the geographical spread with regard to the area affected by the incident; (iv) the extent to which the disruption seriously impairs the functioning of the service; (v) a high number of users are affected by the disruption of the service, in particular users relying on the service for the provision of their own services; and (vi) the extent of the impact on economic and societal activities.

As regards personal data in the context of cyber breaches, the NIS Directive provides that, since personal data are in many cases compromised as a result of incidents, cooperation between competent authorities and data protection authorities with a view to addressing the personal data breaches resulting from incidents is encouraged (Amended recital 31 Draft NIS Directive).[178]

Failure to comply with national provisions adopted pursuant to the NIS Directive, in particular failure to provide notification of a breach, will have potentially harsh consequences.

[174] Draft NIS Directive, Annex II.

[175] Draft NIS Directive, Amended Recital 27.

[176] See the recommendation of the Commission of the European Communities concerning the definition of micro, small and medium-sized enterprises (May 2003), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2003:124:0036:0041:en:PDF.

[177] Draft NIS Directive, Amended Recital 24(a).

[178] Although this article will not discuss the General Data Protection Directive (GDPR), due in 2018, it should be noted that there is some overlap between the GDPR and the NIS Directive. Both instruments require operators/providers to implement security measures and both foresee notification requirements in the event of an incident. However, the interests that the Directives aim to protect are different (personal data vs. network security) and the types of incidents that will fall under their scope may differ (see Gabe Maldoff, *NIS + GDPR = A New Breach Regime in the EU* (December 2015), https://iapp.org/news/a/nis-gdpr-a-new-breach-regime-in-the-eu/). In addition, there is some tension between the GDPR and the NIS Directive if one considers them under the security vs. privacy paradigm. There is to date no guidance on such overlap/tension.

Although the exact calculation is still unclear, the NIS Directive clearly indicates that penalties will have to be "effective, proportionate and dissuasive" (Art. 17 Draft NIS Directive).

4.3.4. *Critical evaluation*

There is no question that the entry into force of the NIS Directive will change the EU regulatory landscape and affect a wide range of industries and players, including global operators.[179] However, it remains to be seen whether or not the Directive will be the promised game-changer in the EU cybersecurity arena.[180]

Critics of the NIS Directive have claimed that there is still much room for improvement.[181] First, the NIS Directive aims to achieve "minimum" harmonization (Art. 2 Draft NIS Directive). It thus notably allows member states to adopt or maintain laws that may impose requirements on operators in their jurisdiction that are stricter than those set forth in the Directive. This, however, coupled with varying degrees of cybersecurity maturity among the member states, bears the risk of legal fragmentation, which is precisely what the Directive seeks to overcome/minimize. Therefore, market operators operating in multiple jurisdictions would potentially have higher compliance costs across the board with the regulation in place than might otherwise be the case. However, in some cases, it might be best for such companies to have a uniform level of compliance across all jurisdictions, i.e. for all divisions adhere to the highest existing standard. It would then be irrelevant if there were jurisdictions that essentially impose no standard. In the same vein, the notification requirement under the NIS Directive potentially overlaps with other existing breach reporting requirements under other EU legislation, which also contributes to fragmentation.[182]

Second, a number of requirements, such as, for instance, the obligation imposed on operators of essential services to take "appropriate and proportionate technical and organisational measures", are subject to interpretation. A diversity of interpretation among member states could lead to an unlevel playing field among businesses and constitute a barrier to operating simultaneously in different member states.[183]

In addition, concerns have been voiced with respect to the exemption of small and medium enterprises from the scope of the Directive as well as the (surprising) exemption of hardware manufacturers and software developers (who are deemed not to constitute digital service providers, see above Section 4.3.3). The exemption of such companies from compliance with minimum security measures or reporting obligations under the Directive may well lead to their becoming the weakest link in the security chain and easy targets for cybercrime.[184] This is problematic if one considers that small and medium businesses form the largest percentage of companies that use the NIS infrastructure.[185]

With regard to the thorny issue of mandatory breach reporting specifically, it remains to be seen how well this requirement, which caused significant controversy, will be implemented and complied with. Indeed, not all stakeholders welcomed its adoption. The industry in particular feared that, combined with the ability of the notified competent authority or CSIRT to inform the public about individual incidents (where public awareness is necessary), the requirement to report significant breaches carried the risk of potential reputational damage and resulting loss of consumer confidence.[186] A further challenge that arises in this context and which promises to be demanding in its actual implementation is that of setting a disclosure level that is high enough to persuade users to install patches but low enough to avoid revealing information that would enable hackers to reverse engineer an exploit based on the public disclosure.[187]

5. Sector-specific regulation and alternative approaches

5.1. *General remarks*

The digital world, in which the IoT is set, is not controlled nor operated by a single person or body.[188] Thousands of entities, including companies, intergovernmental organizations and governments have some control over, or stake in, the Internet and cyberspace.[189] In addition, the digital world is complex and highly dynamic. From this perspective, regulation that purports to deal with cyber must be crafted in ways that make it flexible and future-oriented enough[190] to stay ahead of the evolving cyber threat curve, assuredly a difficult (if not impossible) task.

Section 5.2 investigates whether a targeted IoT regulation may be required at this stage of development of the IoT. Section 5.3 examines a possible alternative to traditional regulatory approaches based on the theory of polycentric regulation.

[179] See https://ec.europa.eu/digital-single-market/en/news/presentation-ncsc-one-conference-2016.

[180] See Marco Gercke, *Der Entwurf für eine EU-Richtlinie über Netz- und Informationssicherheit (NIS)*, Computer und Recht (January 2016), p. 30.

[181] See e.g. the position of Euractiv in its press release, *Response to EU Cybersecurity Strategy and proposed Directive on Network and Information Security (NIS)* (February 2013), http://pr.euractiv.com/pr/response-eu-cybersecurity-strategy-and-proposed-directive-network-and-information-security-nis.

[182] See James A. Harvey & Jan Dhont, *Privacy & Data Security Advisory: Even More EU Data Regulation: The Network Information Security Directive* (March 2016), http://www.alstonprivacy.com/alston-bird-issues-cyber-alert-network-information-security-directive/.

[183] See the Digital Economy Outlook report of BBVA, "The Network and Information Security (NIS) Directive: Part 2 of 2" (May 2016), p. 9 https://www.bbvaresearch.com/wp-content/uploads/2016/05/DEO_May16_Cap3.pdf.

[184] See BBVA, "The Network and Information Security (NIS) Directive: Part 2 of 2" (n. 183), p. 9.

[185] *Ibid.*

[186] See e.g. the report of the Industry and Parliament Trust "Cybersecurity 2.0", p. 11, http://www.ipt.org.uk/Portals/0/Cyber%20Security%20Commission2%20%282%29%20for%20website.pdf.

[187] See Kesan & Mullins Hayes (n. 33), p. 39.

[188] See Scott J. Shackelford, *Toward Cyberpeace: Managing Cyberattacks through Polycentric Governance*, 62 American University Law Review 5 (2013) p. 1303, http://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?article=1888&context=aulr.

[189] See Shackelford (n. 188), p. 1285.

[190] For a general overview, see Rolf. H. Weber, Realizing a New Cyberspace Framework, Normative Foundations and Guiding Principles (2014), p. 158–159.

5.2. *Viability of an IoT-specific legislation?*

While regulatory activities such as the NIS Directive (see above Section 4.3) will impact the security emphasis in connected devices and systems,[191] a question that is subject to considerable debate is whether IoT-specific legislation is necessary and appropriate at this time.

A 2012 European Commission public consultation exercise, which drew much attention,[192] received divergent views on this matter.[193] With respect to security and personal safety in the IoT, several industry players claimed that additional regulation is not necessary and should in any event be specific to the problem at stake rather than generic.[194] In particular, these respondents cautioned against over-regulation and the creation of unnecessary regulatory burdens in a fast evolving environment.[195] In contrast, a vast majority of respondents put forward the need for guidelines and standards, with several of them underlining the necessity for international cooperation in a "globally operating internet".[196] The majority of the respondents further agreed that guidelines and standards should be created to protect the CIA triad in the IoT context.[197]

In addition, many respondents opined that guidelines and standards should be developed "within a multi-stakeholder framework, with the participation of consumer organisations, civil society and regulatory authorities in addition to public authorities and private stakeholders".[198] The consultation also explored the organization and possible enforcement approaches of a possible IoT governance body/framework. The respondent's views were divided on these topics. Most respondents were in favour of no governance or, at a minimum, a soft approach combined with self-regulation.[199] As a general matter, a significant constituency among industry and academics questioned the legitimacy of state intervention in a field which is still in its infancy.[200]

Meanwhile, in a 2015 Staff report[201] on this issue, the US Federal Trade Commission staff declared that IoT-specific legislation at this time would be "premature" and instead encouraged the development of self-regulatory programs for industry sectors, to improve security (and privacy) practices.[202]

In March 2015, the European Commission initiated the creation of the Alliance for Internet of Things Innovation (AIOTI), the purpose of which is to craft a European IoT roadmap until 2020.[203] In October 2015, the AIOTI published 12 reports,[204] which set forth the "Recommendations for future collaborative work in the context of the Internet of Things Focus Area in Horizon 2020" and cover the main focus areas of the IoT Work Programme 2016–2017, including the "Policy Issues" working group Report[205] (AIOTI WG04: Report on Policy Issues). On the question of whether the emergence of IoT necessitates new regulation, the AIOTI WG04 concluded in the negative, arguing that "[a]ny regulatory proposal targeting the IoT should address only well-defined market failures that cannot be addressed through existing law and self-regulatory measures".[206] The AIOTI also pointed to the elevated risk of regulatory error in a complex and fast-moving environment, such as the IoT.[207]

5.3. *Polycentric regulation as a possible model?*

As is apparent from the above, a number of stakeholders, including the EU,[208] have advocated for a bottom-up, multi-stakeholder approach involving both the public and private sector, to address the global and collective problem of cybersecurity,[209] namely in the IoT context.

A possible approach to tackle the ongoing security challenges in the IoT could consist in one that draws lessons from the polycentric regulation model.[210]

Polycentric regulation can be defined as "the enterprise of subjecting human conduct to the governance of external controls, whether state or non-state, intended or unintended".[211] The theory of polycentric regulation is distinct from other regulatory theories.[212] In particular, it contrasts with state-centric approaches to Internet governance and cybersecurity that have been pursued by a number of nations.[213] Indeed, polycentric regulation focuses on multi-stakeholder governance and embraces self-regulation.[214]

[191] See the report of the AIOTI WG04 "Report on Policy Issues" (October 2015), p. 16, https://ec.europa.eu/digital-single-market/en/news/aioti-recommendations-future-collaborative-work-context-internet-things-focus-area-horizon-2020.

[192] Over 600 respondents, including civil society organizations, academics and industry players participated in the consultation.

[193] See the European Commission report on the Public Consultation on IoT Governance (2013), p. 3, https://ec.europa.eu/digital-single-market/en/news/conclusions-internet-things-public-consultation.

[194] *Ibid.*, p. 5.

[195] *Ibid.*

[196] *Ibid.*

[197] *Ibid.*, p. 5–6.

[198] *Ibid.*, p. 6.

[199] *Ibid.*, p. 13.

[200] *Ibid.*, p. 15; see also Rolf. H. Weber, *Internet of Things – Governance quo vadis?,* Computer Law & Security Review (2013), p. 314 f.

[201] The report summarizes the workshop titled "The Internet of Things: Privacy and Security in a Connected World" (held in November 2013) and sets forth the staff's recommendations in this area.

[202] See FTC Staff Report 2015 (n. 103), p. vii.

[203] https://ec.europa.eu/digital-single-market/alliance-internet-things-innovation-aioti.

[204] https://ec.europa.eu/digital-single-market/en/news/aioti-recommendations-future-collaborative-work-context-internet-things-focus-area-horizon-2020.

[205] http://ec.europa.eu/newsroom/dae/document.cfm?action=display&doc_id=11815.

[206] See AIOTI WG04: Report on Policy Issues (n. 191), p. 4.

[207] See AIOTI WG04: Report on Policy Issues (n. 191), p. 4.

[208] See the Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (n. 158).

[209] See Shackelford, Russell & Haut (n. 159), p.1.

[210] See Shackelford (n. 188), p. 1360. For further details, see Weber (n. 190), p. 90–91.

[211] See Weber (n. 190), p. 91 (citing Andrew D. Murray, The Regulation of Cyberspace: Control in the Online Environment, Milton Park (2007), p. 47 and p. 234–235).

[212] See Shackelford (n. 188), p. 1348.

[213] *Ibid.*, p. 1333.

[214] *Ibid.*, p. 1350. However, though an important aspect of polycentric governance, self-regulation merely constitutes one component of the polycentric theory (Shackelford, Raymond, Balakrishnan, Dixit,

A system of polycentric (cyber) governance would enable stakeholders most familiar with the issue to devise appropriate rules which could then be codified.[215] Some of the most well-positioned stakeholders in this area are in the private sector, which is both the lead technology developer and the stakeholder which owns and controls (significant parts of) cyberspace.[216] Effective polycentric governance aimed at enhancing cybersecurity would combine "laws and norms; market-based incentives; code; self-regulation; public–private partnerships; and bilateral, regional, and multilateral collaboration".[217]

Polycentric regulation helps to design rule-making activities in a way that does not require coverage of the entire range of possible legal issues arising in cyberspace. Moreover, a functional differentiation according to the given needs is possible.[218] Such an approach applies the variable geometry model that regulates according to the given circumstantial requirements.

However, while the polycentric model has unique benefits, no system is perfect, and the polycentric one is no exception. The drawbacks of the polycentric approach include in particular the fact that it does not consider issues related to discretionary rule-making pluralism and legal fragmentation (and can thus potentially lead to an uncoordinated set of rules).[219] In addition, this approach raises issues relating to legitimacy and democratic deficit,[220] as well as issues stemming from the absence of a defined hierarchy, which make concerted action difficult.[221]

Notwithstanding these weaknesses, the involvement of all interested stakeholders in the rule-making procedures that relate to the IoT can help establish increased credibility with regard to the actions that are taken. In addition, it seems clear that private sector involvement is an important factor to adequately address the problems and difficulties faced in the emerging IoT ecosystem.

6. Outlook

The one constant (in cybersecurity) is change: The cyber landscape is constantly changing and evolving due to the breakneck speed of technological change, the sophistication of attackers, the value of potential targets, and the resulting impacts of attacks, among other things.[222]

Due to its characteristics, the IoT presents unique security challenges and requires new approaches to secure data and functionality.[223] Each device that connects to the Internet faces "the full force of today's threats",[224] which, in a world where attack is easier than defence, are infinite and potentially severe. Given the near term explosion in the use of vulnerable Internet-connected objects, enhancing security in the IoT is an issue that is critical, urgent and, as with all things cyber, global.

The IoT technological shift will require clear legal frameworks.[225] The difficulty will rest on the ability to craft frameworks that are flexible and innovative enough to keep up with the rapidly evolving threat environment inherent to the technology.[226] While some progress has been made in this arena, namely within the EU (at least on paper), it remains to be seen how the recently adopted legal instruments will play out in practice.

Boosting cybersecurity in general and in the IoT context in particular should, however, not be limited to legal or regulatory approaches. Rather, regulation in this context should integrate different components (as is already being done), including bottom-up governance and dynamic, multi-stakeholder regulation, potentially through a polycentric approach.[227]

Gjonaj & Kavi (n. 63), p. 23–24).

[215] See Shackelford (n. 188), p. 1353; Rolf. H. Weber, *Governance in the Internet of Things – From Infancy to First Attempts of Implementation?*, Laws (forthcoming).

[216] See Shackelford (n. 188), p. 1285 and p. 1362; see also the BSA EU Cybersecurity Dashboard (2015), p. 6, http://cybersecurity.bsa.org/assets/PDFs/study_eucybersecurity_en.pdf.

[217] See Shackelford (n. 188), p. 1285.

[218] See Weber (n. 190), p. 92.

[219] *Ibid.*, p. 91.

[220] *Ibid.*, p. 91.

[221] See Shackelford, Raymond, Balakrishnan, Dixit, Gjonaj & Kavi (n. 63), p. 5 and p. 36.

[222] See McAfee Labs Report, 2016 Threat Predictions (n. 11), p. 34.

[223] See ENISA, Threat Landscape 2015 (n. 8), p. 68.

[224] See McAfee Labs Report, 2016 Threat Predictions (n. 11), p. 21.

[225] See BSA EU Cybersecurity Dashboard (n. 216).

[226] *Ibid.*

[227] See Shackelford (n. 188), p. 1360.