Governing Critical ICT: Elements that Require Attention

*Eric Luiijf and Marieke Klaver**

With respect to critical information and communication technologies (ICT), nations most often declare their national critical infrastructure to include telecommunication services and in some cases critical services offered by key Internet Service Providers (ISP). This paper debates whether nations, their policy-makers, legislation and regulation largely overlook and fail to properly govern the full set of ICT elements and services critical to the functioning of their nation. The related societal and economical risk, however, needs to be closely mitigated, managed and governed. Legal and regulatory obligations to increase the ICT resilience may sometimes encourage this process.

I. Introduction: National Critical Infrastructure

The European Union defines a critical infrastructure as "an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions." [1] The USA Patriot Act[2] defines a critical infrastructure as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." A number of nations, such as Australia, Canada, Sweden, Switzerland, the Netherlands and United Kingdom use similar definitions. The governance and resilience of these critical infrastructures and their critical services require prevention, preparation, incident management and fast recovery measures. For that reason governments identify what they regard to be critical infrastructure sectors, and the related critical products, services and assets. The early Green Paper by the European Commission on critical infrastructures contains an example list of critical sectors, products and services.[3] For the critical Information and Communication Technologies (ICT) sector, seven products and services are listed: Information system and network protection, Instrumentation automation and control systems (SCADA etc.), Internet, Provision of fixed telecommunications, Provision of mobile telecommunications, Radio communication and navigation, Satellite communication, and Broadcasting.

Nations such as The Netherlands, who have detailed their critical telecommunications or information and communication technology (ICT) sector in critical services and products, recognise fixed telecommunication services, mobile telecommunication services, internet access, satellite communication, and media/broadcasting as critical infrastructure services for their nations.[4] Other nations only define their set of critical sectors or define the services and products at a high level. Switzerland, for instance, recognises the following three ICT subsectors: information technologies (IT), media, and telecommunication.[5]

* Eric Luiijf and Marieke Klaver are both Consultants for Cyber Operations and Critical (Information) Infrastructure Protection at the Netherlands Organisation for Applied Scientific Research TNO, The Hague.

1 Council Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, OJ 2008 L 345/77, Article 2.a.

2 The United States - *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001,* U.S. H.R. 3162, Public Law 107-56, § 1016(e).

3 Commission Green Paper on a European Programme for Critical Infrastructure Protection, COM(2005) 576 final, at Annex 2 pp. 42.

4 Netherlands Ministry of Security and Justice, "Protecting critical infrastructure" , available on the Internet at <http://www.government.nl/issues/crisis-national-security-and-terrorism/protecting-critical-infrastructure> (last accessed on 7 May 2015).

5 Swiss Federal Office for Civil Protection (FOCP), "The Swiss Programme on Critical Infrastructure Protection - Factsheet", November 2010, available on the Internet at <http://www.bevoelkerungsschutz.admin.ch/internet/bs/en/home/themen/ski.parsysrelated1.82246.downloadList.18074.DownloadFile.tmp/factsheete.pdf> (last accessed on 7 May 2015).

The USA recognises eighteen critical infrastructure sectors including the Communication sector and the IT sector.[6] The critical Communication sector comprises wireline, wireless, satellite, cable and broadcasting infrastructures[7]; the critical IT sector comprises the provision of IT products and services, incident management capabilities, domain name resolution services, identity management and associated trust support services, Internet-based content, information and communication services, and Internet routing, access and connection services. [8]

The examples provided above and those found on CIPedia©[9] show that the EU and its Member States as well as other nations do not have an aligned approach to the Communication and IT sectors or the ICT sector with respect to what is critical to their societies. With the ever increasing dependency of society on ICT one would expect a similar approach and understanding in the highly technologically developed nations of what comprises the critical ICT sector. However, from these critical sector lists on e.g. CIPedia© one can conclude that the governance of communications and IT in nations currently focusses on the traditional telecommunication services. Sometimes internet access services and/or key Internet Service Providers (ISPs) are included as well. In the EU Member States, legislation and regulation for the ICT sector mainly stem from EU's Telecoms Package[10] including the Data Security[11] aspects.

The USA uses a slightly different pathway: their sector-specific coordinated approach to critical infrastructure protection (CIP) acknowledges the criticality of underlying ICT services to their society and their critical infrastructures.[12]

Despite their current efforts, this paper will show that nations, their critical infrastructure policy-makers, legislators and regulators largely underestimate the continuous move to a deep and critical penetration of ICT into all aspects of society as well as in all critical sectors. Current ICT has the property to hide itself in what society and organisations consider "user-friendly functionality". For example, modern building and access control systems control the air conditioning system, the building access control through doors and gates, the fire control system, security cameras and the evacuation system. The functionality pleases the responsible facility managers who do not recognise the embedded ICT and the related cyber security risk.[13] [14]

In a similar way, embedded ICT is massively brought via backdoors into organisations, including organisations responsible for critical societal services. Since the governance focus of most nations is aimed at the traditional telecommunication and internet services, new vulnerabilities to nations and their societies are introduced. Below, we will show that policy-makers, legislation and regulators fail to recognise the need for the governance coverage of critical ICT in order to ensure the necessary resilience required to maintain the "societal functions, health, safety, security, economic or social well-being of people".[15]

II. Outlining Critical ICT

This section discusses that the critical ICT sector actually divides into six different critical infrastructure elements as is depicted in Figure 1.

1. "Top" ICT manufacturers

The same software and hardware[16] produced by a relatively small set of extremely large, globally oper-

6 The White House, *Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection (HSPD7)*, Washington DC, December 17, 2003.

7 USA DHS, Communications Sector-Specific Plan, An Annex to the National Infrastructure Protection Plan, 2010, Appendix D: Sector Profile, pp. 91-98.

8 USA DHS, Information Technology Sector-Specific Plan, An Annex to the National Infrastructure Protection Plan, 2010, pp. 8.

9 CIPedia©, "Critical Infrastructure Sector", available on the Internet at <https://www.cipedia.eu> (last accessed 7 May 2015).

10 EU's Telecoms package consists of five Council Directives and two Regulations, available on the Internet at <http://ec.europa.eu/digital-agenda/en/telecoms-rules> (last accessed on 7 May 2015).

11 Also known as (Data) Privacy.

12 HSPD7, *supra* note 6 at paras. 15 and 16.

13 Eric Luiijf, "Are we in love with cyber insecurity?", 7 International Journal of Critical Infrastructure Protection (2014), pp. 165 et sqq. at p. 166.

14 Mark Goldstein and Gregory Wilshusen, "Federal Facility Cybersecurity: DHS and GSA Should Address Cyber Risk to Building and Access Control Systems", GAO-15-6, (Washington DC: GAO, 2015), at p. 23.

15 Council Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, OJ 2008 L 345/77, *supra* Art. 2.a.

16 Hardware most often includes firmware. Firmware is "the combination of persistent memory and program code and data stored in it" according to IEEE, *Authoritative Dictionary of IEEE Standards Terms (IEEE 100)*, (IEEE, 2007), at p. 438.

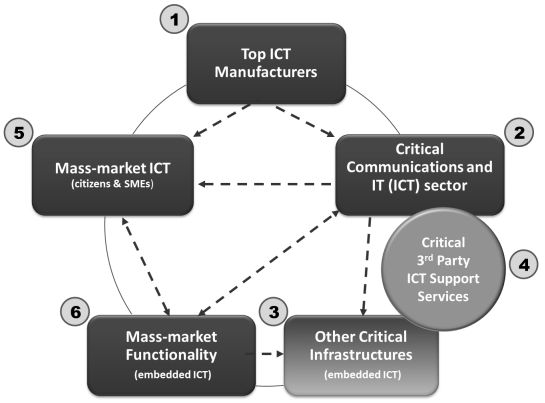

Figure 1: Division of the critical ICT infrastructure in six elements

ating manufacturers is both used by the mass consumer market and in the networks and services of critical infrastructure operators. When a serious security flaw is found in the many hundreds of million copies of an operating system or application, cyber criminals and Trojans exploit the vulnerability within hours after it becomes public knowledge. This may affect the systems of millions of innocent end-users across many nations who are late to protect themselves. This may be the cause of serious socio-psychological impact and social unrest and may cause major disruptions of the everyday life[17].

When a serious vulnerability is detected in key network or server systems, or in process control systems, the risk of a global infrastructure disruption cannot be neglected. Actually, some narrow escapes have occurred in the core of the Internet.[18] In one case[19], very strict control and discrete dissemination of the vulnerability and the related mitigation software ("patch") firstly removed the security vulnerability from the core of the Internet infrastructure. Next, key Internet Service Providers (ISP) discretely received the vulnerability information and got the chance to patch their networks before Computer Emergency Response Teams (CERTs)[20] disseminated the information about the critical vulnerability to the next wider circle.

Experiences show that the top manufacturers in general administer their products in a paternal way. Microsoft even issued a critical patch[21] for Windows/XP systems after its thirteen year support period ended on 8 April 2014. Microsoft took into account of the fact that Windows/XP at that time was still in use on a considerable number of PCs[22], for example those embedded in ATM systems.

Another vulnerability which may have global impact is the use by the "top" manufacturers of the same basis of open source software modules and libraries. In case of a major flaw in such a module or library, many important and critical ICT services all over the world may be vulnerable at the same time to cyberattack. The Heartbleed flaw and its global impact is a case in point[23]. It affected for instance all registered users of Blogger/Blogspot, Dropbox, Facebook, Electronic Frontier Foundation, Etsy, Google, Imgur, Instagram, Netflix, OKCupid, Pinterest, Stack Overflow, Wikipedia, Woot, Wordpress.com/Wordpress.org, and YouTube[24]. Privacy-sensitive data of 4.5 million patients at 206 USA hospitals in 29 States were stolen[25] because this vulnerability was quickly exploited by cyber criminals after the information about the vulnerability became public. Millions of end-users using services from some 600,000 flawed servers worldwide were at risk. Actually, two months after the vulnerability became publicly known, some 300,000 systems were

17 Jasper van der Horst, Erik Pruyt, Diederik Wijnmalen et al., *Working with Scenarios, Risk Assessment and Capabilities in the National Safety and Security Strategy of the Netherlands* (Netherlands Ministry of Security and Justice, 2012), at p. 64 *and* pp. 67 *et sqq.*, at p. 70.

18 CERT.ORG, "Microsoft ASN.1 Library improperly decodes constructed bit strings", 10 February 2004, available on the Internet at <http://www.kb.cert.org/vuls/id/583108> (last accessed on 7 May 2015).

19 CERT.ORG, "Cisco IOS contains DoS vulnerability in MPLS packet processing", 26 January 2005, available on the Internet at < http://www.kb.cert.org/vuls/id/583638> (last accessed on 7 May 2015).

20 A synonym of CERT is Computer Security Incident Response Team (CSIRT).

21 Gareth Halfacree, "Windows XP gets first post-EOL security patch", 2 May 2014, available on the Internet at <http://www.bit-tech.net/news/bits/2014/05/02/winxp-eol-patch/1> on 7 May 2015)

22 Tony Bradley, "Windows XP use declining, but millions still willingly at risk", 16 April 2014, available on the Internet at <http://www.techrepublic.com/article/windows-xp-use-declining-but-millions-still-willingly-at-risk> (last accessed on 7 May 2015).

23 Ben Grubb, "Heartbleed disclosure timeline: who knew what and when", 15 April 2014, available on the Internet at <http://www.smh.com.au/it-pro/security-it/heartbleed-disclosure-timeline-who-knew-what-and-when-20140415-zqurk.html> (last accessed on 7 May 2015).

24 Paul Wagensell, "Heartbleed: Who Was Affected, What to Do Now", 9 April 2014, available on the Internet at <http://www.tomsguide.com/us/heartbleed-bug-to-do-list,news-18588.html> (last accessed on 7 May 2015).

25 Sam Frizell, "Report: Devastating Heartbleed Flaw Was Used in Hospital Hack", 20 August 2014, available on the Internet at <http://time.com/3148773/report-devastating-heartbleed-flaw-was-used-in-hospital-hack/> (last accessed on 7 May 2015).

still vulnerable.[26] Another example was the ASN.1 flaw.

As the impact of a serious failure in ICT produced by the "top" manufacturers may cause serious unwanted effects to society, or even worse, societies, these ICT products qualify as critical assets according to the various national definitions of critical infrastructure. In 2005 a report for the World Bank substantiated that governments need to develop procurement policies which require ICT manufacturers to deliver secure out-of-the-box software and critical infrastructure components.[27] However, as far as we know, neither product liability legislation exists for software and ICT-functions embedded in hardware, nor any legal requirements for manufacturers to speedily remove identified security flaws from their products. In short, governance of this critical ICT element is currently left to the discretion of the manufacturer. As it concerns critical ICT, nations should at least have direct access to these manufacturers in case of ICT disasters. Moreover, nations shall consider the pros and cons of introducing ICT liability at an international scale. A strict legal and regulation regime often blocks innovation, something which is unwanted in the ICT domain which is based on fast innovation cycles. A stick and carrot approach or an approach which looks for a joint approach towards more secure products is preferred. In this respect, the notion of privacy and security-by-design is gaining momentum in the ICT domain. Nations may stimulate this momentum by acting as the first customer of products designed on the basis of such principles. Such a move will create market pressure which in a later phase can be followed by making this good practice a requirement for all acquired ICT products.

2. Critical Communications and IT (ICT) sector

This is the critical ICT element which provides the national critical core services and functions of the classical communications sector (wireline and cable infrastructure, mobile telecommunications, navigation systems, satellite ground and space segments infrastructure, and broadcast). Over the last fifteen years "internet access" services have been added to this set of critical infrastructure products and services by an increasing number of nations, The Netherlands being the first in 2001.[28] The Internet subsector comprises key backbone providers, Internet Service Providers (ISPs), Application Service Providers, and internationally operating cloud services. Despite the fact that the Internet and its services are critical to modern societies, many nations do not pursue the governance of this subelement of the critical ICT sector. Nations take the stance that private industry has the lead. It is only when market failure occurs, that regulators and government may reluctantly step in.

An example of such an intervention by nations was after the bankruptcy filing by KPNQwest in May 2002. As the KPNQwest network was one of the fastest and most interconnected at that time, 67 country code top-level domains (ccTLD) were serviced by servers connected to the KPNQwest network.[29] Several nations even had both their primary and secondary ccTLD servers only connected to that network.[30] Authorities in various nations silently "pulled strings" to gain time for coordinating the relocation of their critical ccTLD naming services, whereas the official position was that of a private company failure governments did not want to intervene with. The risk for societies, however, was unclear for weeks as electronic services of over hundred thousand businesses and public authorities using the KPNQwest network services were at stake.[31]

The traditional telecommunication market is well regulated due to governments keeping track of the

26 Tom Brewster, "More than 300k systems "still vulnerable" to Heartbleed attacks", 23 June 2014, available on the Internet at <http://www.theguardian.com/technology/2014/jun/23/heartbleed-attacks-vulnerable-openssl> (last accessed on 7 May 2015).

27 Robert Bruce, Scott Dynes, Hans Brechbuhl, et al., "International Policy Framework for Protecting Critical Information Infrastructure: A Discussion Paper Outlining Key Policy Issues", (The Hague: TNO, 2005) & (Dartmouth: Center for Digital Strategies at Dartmouth, 2005), at p. 73.

28 Staatssecretaris van Verkeer en Waterstaat, "Brief aan de Tweede Kamer der Sten Generaal over Kwetsbaarheid op internet (KWINT)", (9 July 2001) 26 643 No. 30, available in Dutch on the Internet at <https://zoek.officielebekendmakingen.nl/dossier/26643/kst-26643-30> (last accessed on 7 May 2015), ["Letter to the House of Representatives on the vulnerability of Internet"].

29 ICANN/DNSO, "IANA Handling of Root-Zone Changes", 9 October 2002, available on the Internet at <http://www.dnso.org/clubpublic/council/Arc11/msg00123.html> (last accessed on 7 May 2015).

30 De Telegraaf, "Bankroet KPNQwest kan zakenwereld ontwrichten", 1 June 2002, available on the Internet at <http://krant.telegraaf.nl/krant/archief/20020601/teksten/fin.kpnqwest.netwerk.faillissement.html> (last accessed on 7 May 2015).

31 Hans de Bruijn, Mark de Bruijne, Michel van Eeten et.al., "Verschuiving in de publieke belangen: Van toegang naar gebruik", 9 Reflecties op elektronische communicatie (July 2007), pp. 39 *et sqq.*, at p. 41.

liberalisation and privatisation of the former government telecommunication services. Currently, the European national telecommunication and privacy regulators oblige telecommunication operators to report cyber security breaches and privacy related breaches to the national regulatory authorities (NRA) based on Council Directive 2002/58/EC Article 4 (2)[32] which is part of EU's Telecoms Package.[33] Moreover, based on Article 13a of the Telecoms Package, EU Member States mandate or require by binding minimum measures that their telecommunication operators have a continuity plan and report any service continuity disruption that has a serious societal impact or cause high economic losses.[34] This legal and regulatory approach to the private telecoms/ICT industry works as long as it is balanced with the approach to other ICT service risk to the nation(s). This paper debates the risk that an imbalance may occur in near future.

3. Other Critical Infrastructure Sectors

All CI sectors (other than the "pure" ICT sector), such as the energy, food, drinking water, financial, transport, and health sectors, are increasingly becoming ICT-intensive. Vital processes of these critical sectors depend on the undisturbed functioning of ICT, being either commercial off-the-shelf (COTS) software and hardware from the small number of top globally operating manufacturers discussed in section II.1, process control systems[35] from a limited set of globally operating manufacturers, or specialised ICT and ICT-based equipment. However, the main focus of authorities, legislation and regulation is on the classical physical security and safety aspects of these critical sectors and their infrastructures failing to notice the ICT (cyber) related risk.

The targeted Stuxnet worm[36] attack on the Siemens process control equipment of the nuclear enrichment plant in Naṭanz, Iran, was a wake-up call for owners of critical infrastructures with process control systems. Derived from Stuxnet, a whole generation of new malware evolved which attacks the critical systems that control our utilities and many other critical functions of well-organised and prosperous societies.[37]

Apart from the ICT systems in use for administrative purposes, e.g. data security of hospitals systems, governance of the critical ICT elements in the aforementioned critical infrastructure sectors is not yet well-developed. It is only recently that governance steps have been taken in the USA towards manufacturers with respect to the cyber security of (implantable) medical devices such as pacemakers and insulin pumps, which are considered to be part of USA's public health critical sector.[38] Other nations lag behind in their ICT risk governance of their non-ICT critical infrastructure sectors, for instance, a heart monitoring system in an emergency ward of a Dutch hospital took part in a Kazaa – peer-to-peer sharing of multimedia –network.[39]

Legislators and regulators for non-ICT critical sectors such as health, transport and energy should include cyber security aspects as an integral part of their regulatory frameworks in addition to the physical security and safety laws and regulation. This may include security requirements for and standards on the devices with embedded ICT. It also may include standards and regulations for the organisational structure, processes, reporting schemes, and information provision about security and privacy breaches to potentially affected people and to the public. As a starter, a regulatory authority may issue awareness and good practices to the stakeholders. An example is the U.S. Food and Drug Authority (FDA) safety com-

32 Council Directive 2002/58/EC on privacy and electronic communications, OJ 2002 L201/43.

33 EU's Telecoms package, *supra* note 10.

34 ENISA, "Shortlisting network and information security standards and good practices" (Heraklion: ENISA, 2012), at pp. 18-24, available on the Internet at < https://resilience.enisa.europa.eu/article-13/shortlist-of-networks-and-information-security-standards> (last accessed on 7 May 2015).

35 In this paper, the notion process control systems includes Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), Industrial Control Systems (ICS), Industrial Automation Control Systems (IACS) and alike.

36 Nicholas Falliere, Liam O Murchu, and Eric Chien, "W32.Stuxnet dossier", version 1.4, February 2011, available on the Internet at <http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf> (last accessed on 7 May 2015).

37 Eric Luiijf and Bert Jan te Paske, *Cyber Security of Industrial Control Systems*, (TNO, 2015), pp. 10, available on the Internet at <http://www.tno.nl/ICS-security> (last accessed on 7 May 2015).

38 Food and Drug Administration (FDA), "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices - Guidance for Industry and Food and Drug Administration Staff", 2 October, 2014, available on the Internet at <http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM356190.pdf> (last accessed on 7 May 2015).

39 Anne-Greet Haars, "Beveiliging apparatuur van ziekenhuizen schiet tekort", 2 October, 2014, available on the Internet at <http://www.bnr.nl/nieuws/tech/759869-1304/beveiliging-apparatuur-van-ziekenhuizen-schiet-tekort> (last accessed on 7 May 2015).

munication on Cybersecurity for Medical Devices and Hospital Networks.[40] To avoid the risk of conflicting sector specific laws and regulation, cross-sector harmonisation and -if possible- a wider ICT "umbrella" regulation on ICT (cyber) security should be strived for.

4. Critical Third Party ICT Support Services

Almost hidden, a set of third parties deliver critical ICT services to both the critical ICT infrastructure operators (second element of critical ICT), the non-ICT critical infrastructure sectors (third element of critical ICT), and indirectly to the citizens and Small and Medium Enterprises (fifth element of critical ICT). Firstly, one can recognise the registrars and operations of the registrar databases. These include the national telephone number database which allows number portability from one operator to another, and its equivalent for utilities where a utility connection at a premise, e.g. power, is linked with the current market supplier for that power distribution connection. Within the Internet realm, this concerns the domain name registrars. They register and guarantee the uniqueness of domain names, e.g. lexxion.de. The related domain name services (DNS) translate that name into a reachable internet address allowing authors to submit papers to this journal. A failing country code top-level domain (ccTLD) or other top level domain structure makes services by organisations globally unreachable after a while. The example KPNQwest case[41] [42] of ccTLD being critical to the continuity of Internet was outlined above.

Secondly, the electronic trust providers: trust on the internet is often provided through the use of a chain of certificates which trace back to a root certificate. When a certificate authority (CA) who issues electronically signed certificates becomes untrusted or is unable to provide its services, all depending trust relationships based on the issued certificates become untrusted. The DigiNotar case[43] in the Netherlands is a case in point of an ICT-crisis caused by a untrusted CA. A hacker break-in followed by inappropriate incident management at DigiNotar caused the compromise of all certificates of the Dutch government, its agencies, and of many municipalities of the Netherlands. Like the KNPQwest case, this incident came as a complete surprise to the authorities. As governance was lacking, there was no emergency plan at the affected organisations. Given the severity of the compromise and its risk to all electronic transactions of citizens, Small and Medium Enterprises (SMEs) and other organisations with (semi)government agencies, the Dutch government took the decision to nationalise the operations of DigiNotar. DigiNotar subsequently went bankrupt.[44] All DigiNotar certificates were revoked, although the revocation of the certificates by Microsoft was delayed in the Netherlands upon request of the Dutch government. Their municipalities needed time to investigate which of their services were affected, and time to acquire new certificates from other certificate providers and apply them.[45] Like the DigiNotar case in the Netherlands, the Turkish certificate authority TÜRKTRUST failed to secure their chain of trust in a short period of 2011 affecting ICT-products and services in late 2012.[46]

These kinds of hidden, but critical, ICT-services will only increase in importance in the near future whilst the impact of their failure may seriously impact many societal services. Some form of governance is required to ensure prevention of, and preparation for, incidents.

Because of the large scale impact of disruptions, some form of governmental oversight is essential for

40 U.S. FDA, "Cybersecurity for Medical Devices and Hospital Networks: FDA Safety Communication", 13 June 2013, available on the Internet at <http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm356423.htm> (last accessed on 7 May 2015).

41 ICANN/DNSO *supra* note 29.

42 De Telegraaf, *supra* note 30.

43 Ministry of Security and Justice, "Dossier Diginotar", 2011, available on the Internet at <https://www.ncsc.nl/english/services/expertise-advice/knowledge-sharing/files%5B2%5D/dossier-diginotar.html> (last accessed on 7 May 2015).

44 J.P.H. Donner and I.W. Opstelten, "Letter to the Speaker of the Lower House of the States General on Digital burglary DigiNotar", 5 September 2011, available on the Internet at <http://www.government.nl/files/documents-and-publications/letters/2011/09/06/digital-burglary-diginotar/microsoft-word-2011-sept-brief-minister-5-sept-2011-en.pdf> (last accessed on 7 May 2015). The Parliament reference to the (Dutch) letter is 26643 Nr. 188, 5 September 2011.

45 W. van Dijk, A. Könen, N. Svartz, "International Case Report On Cyber Security Incidents", 2014, The Hague, Bonn, and Stockholm: NCSC, BSI and MSB, pp. 7 *et sqq*. 11, available on the Internet at < https://www.gccs2015.com/nl/node/462 > (last accessed on 7 May 2015).

46 Paul Ducklin, "The TURKTRUST SSL certificate fiasco - what really happened, and what happens next?", 8 January 2013, available on the Internet at <https://nakedsecurity.sophos.com/2013/01/08/the-turktrust-ssl-certificate-fiasco-what-happened-and-what-happens-next/> (last accessed on 7 May 2015).

this type of critical service where a higher level of assurance is required. One might consider regulatory measures similar to those that apply to the more traditional telecommunication infrastructure services, as these may create proper checks and balances. These include the obligatory reporting on serious security breaches or disruptions of these services to a national authority based on Council Directive 2002/58/EC Article 4 (2)[47] which is part of EU's Telecoms Package[48] or by defining a minimum set of cyber security requirements a service provider is obliged to implement by law or regulation.

5. Mass-market ICT for Citizens and SMEs

Massive and long-duration insecurity of mass-market ICT of citizens and of SMEs due to fast-spreading malware, or the discovery of a major vulnerability, is not impossible. When larger numbers of citizens and SME distrust their ICT, cannot access their social networks, do electronic banking, etcetera, for more than a couple of days, the socio-psychological impact may come close or exceed the national criteria used to define critical infrastructure. A short technical disruption of Facebook even caused citizens in the USA to call 9-1-1.[49] The end-users cannot do more than installing and regularly updating an anti-malware package. On the one hand, the mass-market providing software manufacturers can properly implement security standards and take adequate preventive and response measures such as timely provision of patches in case of a vulnerability. On the other hand, ISPs may see it as their responsibility or be obliged by authorities[50] to block the spreading of malware in and from their networks.

Although this ICT element certainly may have large disruptive impact, most governance options, except cyber security awareness education of citizens, lie beyond the responsibility of this element. Cyber security awareness education nowadays starts at the elementary school; others, such as financial services, build on that base level with their cyber security awareness campaigns. However, one may wonder whether non-professionals will recognise new cyber threats in time and each time they are faced with a tempting promise. Despite the high risk of human failure, this issue is hard to counter by educational and awareness campaigns of both the private and public sectors.

6. Mass-market Functionality with Embedded ICT

Increasingly, consumer and professional product functions are based on ICT embedded in the product. Most often, these products connect to and interact with the internet, and with ICT that is part of the fifth element of critical ICT: "Mass-market ICT for citizens and SMEs". It is expected that the next innovation wave is the Internet-of-Things (IoT). The development of the products is predominantly by non-ICT manufacturers –certainly not the traditional ICT manufacturers– and aims at functionality. Think about manufacturers of trains, washing machines, digital TVs (e.g. Samsung, Philips), thermostat, carbon monoxide and smoke detector sets (e.g. Google Nest), toasters, home lighting, and home automation equipment (a.k.a. domotics). Cyber security is not a major consideration to these manufacturers, if indeed they understand the security issues and challenges at all.[51] A good example is the insecurity of wireless thermostats connected to the Internet[52] or home lighting using a pre-shared, non-replaceable cryptographic key.[53] As the ICT is embedded, the cyber security aspects will not be recognised until vulnerabilities are exploited on a massive scale and disrupt society. Nations, their policy-makers, legislation, and regulators currently do not proactively consider how to govern for example:

– millions of smart TVs affected by malware or acting as a denial-of-service attack platform,

47 Council Directive 2002/58/EC, *supra* note 32.

48 EU's Telecoms package, *supra* note 10.

49 JusticeNewsFlash.com, "Facebook outage sparks calls to 911", 8 January 2013, available on the Internet at <http://www.justicenewsflash.com/2015/02/02/facebook-outage-sparks-calls-to-911_20150202133988.html> (last accessed on 7 May 2015).

50 Claire Reilly, "AFP using site blocking laws to target malware", 22 October 2014, available on the Internet at <http://www.cnet.com/au/news/afp-using-site-blocking-laws-to-target-malware/> (last accessed on 7 May 2015).

51 Eric Luiijf, *supra* note 13.

52 CyberGibbons, "Heatmiser WiFi thermostat vulnerabilities", 20 September 2014, available on the Internet at <http://cybergibbons.com/security-2/heatmiser-wifi-thermostat-vulnerabilities/> (last accessed on 7 May 2015).

53 IBM Security Systems, "Securing the new world of the Internet of Things", 4, IBM X-Force Threat Intelligence Quaterly (2014), pp. 3 *et sqq.*, at p. 7.

– millions of smart fridges, smart washing and dishwashing machines with a serious software glitch or exploited flaw which causes instabilities in the smart power grid,
– an exploited cyber security flaw or software failure affecting the safety of millions of vehicles taking part in collaborative driving[54] [55] or autonomous driving.

Moreover, it is questionable whether the policy-maker or regulator for energy markets and power grids will occupy themselves with ICT in consumer market products such as fridges? But, who else when they bring down the local power grid? If not by setting the standards and requirements, then at least by identifying the risk factors involved and developing ways to mitigate the effects when necessary. A case in point on how fast this ICT element come to the fore was the recent need for a firmware upgrade of almost 230,000 solar plants as the exploitation of the vulnerability could trigger a power blackout. Moreover, other power grid instabilities may also make firmware upgrades of solar panels a necessity[56]. The challenge is to convince a huge range of home owners, farmers and building owners to upgrade their sets of solar panels.[57] How does one convince and older generation of 80+ year olds to urgently upgrade their fridge or solar panel?

On the other hand, one could argue that critical sector operators, e.g. energy, are responsible to protect their grid against any threat from the IoT developments. A start-up today may deliver the vulnerable IoT chipset or product which is the "killing IoT application" we all want to have and use.[58] Such a IoT wave will exponentially penetrate our society with new risk that we have to experience and understand before it can be mitigated either by technical measures or by some form of regulation. Critical sectors may first experience a cyber impact stemming from exploited vulnerabilities in IoT before taking appropriate prevention, preparation and incident response measures.

III. Conclusions

Nations take governance measures to ensure the continuity of their critical infrastructures. Most nations identify (tele)communications and IT, or the combination "ICT", as national critical infrastructure. As we have outlined above, critical ICT falls apart into six critical elements. Often only one or two of these elements have been included in the national CI resilience and protection approaches by policy-makers, legislation, and regulatory frameworks. New governance challenges for critical ICT are on the horizon, if not already close. The overview of critical ICT elements outlined in this paper may support policy-makers, legislation, and regulators to reduce the current and future risk to society on the one hand and on the other hand to avoid focussing in an unbalanced way solely upon the traditional (tele)communication sector.

54 Tjerk Bijlsma, Sander de Kievit, Jacco van de Sluis, et al., "Security Challenges for Cooperative and Interconnected Mobility Systems", in: Eric Luiijf and Pieter Hartel (ed.), Lecture Notes in Computer Science, Vol. 8328, (Heidelberg: Springer, 2013), pp. 1 et sqq., at p. 15.

55 Collaborative driving is a form of intelligent transportation where vehicles communicate with each other and roadside systems. Benefits comprise risk reduction by sharing information, e.g., about fog, braking or stopped vehicles, and higher fuel efficiency.

56 J. C. Boemer, K. Burges, P. Zolotarev, et al., "Overview of German Grid Issues and Retrofit of Photovoltaic Power Plants in Germany for the Prevention of Frequency Stability Problems in Abnormal System Conditions of the ENTSO-E Region Continental Europe", October 2011, available on the Internet at <http://www.ecofys.com/files/files/ecofys_2011_paper_on_frequency_stability_challenge.pdf> (last accessed on 7 May 2015).

57 Darren Pauli, "Spotty solar power management platform could crash the grid", 12 May 2014, available on the Internet at <http://www.theregister.co.uk/2014/05/12/hackable_solar_systems_spurt_free_money/> (last accessed on 7 May 2015).

58 Consider Facebook which became a public service less than ten years ago and its Chinese equivalent Renren.