Zentrum für Europäische Integrationsforschung
Center for European Integration Studies
Rheinische Friedrich-Wilhelms Universität Bonn

Agnes Kasper / Alexander Antonov

Towards Conceptualizing EU Cybersecurity Law

Discussion Paper

C253
2019

Rheinische
Friedrich-Wilhelms-
Universität Bonn

Center for European
Integration Studies

Genscherallee 3
D-53113 Bonn
Germany

Tel.: +49-228-73-1810
Fax: +49-228-73-1818
http://www.zei.de

ISSN 1435-3288 ISBN 978-3-941928-96-1

Dr. Agnes Kasper is a Senior Lecturer of Law and Technology at the Tallinn University of Tallinn, Department of Law. She has been teaching legal aspects of cybersecurity to law students, as well as to IT students in the cybersecurity program at TalTech since 2012. Dr Kasper holds diplomas in international business, law and management. She has received additional formal trainings on technical aspects of cybersecurity and digital evidence. Dr Kasper served at embassies, human rights organizations and she was leading the legal department in an IT consultancy and development company. She has also acted in advisory capacity in consultations with governments on issues relating to cybersecurity. Her research focuses on regulatory aspects of cybersecurity; in particular, she is interested in emerging technologies. She is a frequent speaker in events, seminars, conferences focusing on aspects of law, technology and security. In 2015 the Estonian Ministry of Defence awarded Dr Kasper with the first prize for her doctoral thesis „Multi-Level Analytical Frameworks for Supporting Cyber Security Legal Decision Making“.

Alexander Antonov is a doctoral student at the Department of Law at TalTech University, Estonia. He holds a Master Degree in ‘’M.Sc. International Security and Law’’ from the University of Southern Denmark. His main research areas are Public International Law and International Humanitarian Law. In his Ph.D. project he scrutinizes the tools International Law provides for the regulation of the use of emerging technologies in warfare.

Agnes Kasper / Alexander Antonov

Towards Conceptualizing EU Cybersecurity Law

1. Introduction

The European Union has a wide spectrum of legal instruments addressing various aspects of cybersecurity, ranging from electronic communication laws, data protection regulations through network and information security legislation to instruments dealing with cybercrime and recommendations on coordinated response to large scale cyber incidents – all this without having a commonly accepted definition of cybersecurity.

The 2013 Cybersecurity Strategy describes cybersecurity in general terms in a footnote as the "safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure". [1] The proposed Cybersecurity Act purports to define cybersecurity as it "comprises all activities necessary to protect network and information

1 European Commission, "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," 7 February, 2013.

systems, their users, and affected persons from cyber threats",[2] however the definition is not explained in available preparatory documents, although the word cybersecurity is used 462 times in the impact assessment.[3] According to these existing wordings, which are overly broad, cybersecurity is a process or activity. Other instruments, such as the 2017 Communication on Resilience, Deterrence and Defence: Building strong cybersecurity for the EU[4], also refer to cybersecurity as it was an attribute or a desired state to be achieved. The lack of clarity about this core concept raises questions about coherence and consistency of already adopted and newly proposed legislative acts in the field of cybersecurity. Precisely what harms EU cybersecurity-related laws seek to prevent? Understanding the harms is essential to prioritizing goals, limits and scope of the relevant legal framework.

Therefore, we propose to take a step back and examine the subjects, methods and reasons behind relevant EU regulatory acts in order to determine the scope and goals of EU laws that aim to promote cybersecurity. It is also expected that "EU cybersecurity law" as a legal framework is constrained by the competences of the EU, as well as by the principles of subsidiarity and proportionality, hence will necessarily differ from that of a federal state or that of a Member State. Conceptualizing EU cybersecurity law will also allow to examine how lawmakers can improve the legal framework for

2 COM (2017) 477: *Proposal for a Regulation of the European Parliament and of the Council* on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act").

3 See *Commission Staff Working Document Impact Assessment*. Accompanying the document *Proposal for a Regulation of the European Parliament and of the Council* on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurit. Act"), SWD/2017/0500 final – 2017/0225 (COD); opinion of the Regulatory Scrutiny Board, SEC/2017/0389 final. Online at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=pi_com:SEC(2017)389).

4 Joint Communication to the European Parliament and the Council, Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, JOIN/2017/0450 final.

cybersecurity and contribute to the stated need (by ENISA, 2012) to define common cybersecurity goals across the EU. In order to illustrate the challenges, we examine a high-profile cyber-attack (i.e. Wannacry ransomware 2017) to gain a fuller picture of the harms caused in or to Europe.

2. Wannacry crisis in the EU

2.1 The attack

Digital transformation, which is brought about by the rapid pace in technological change, challenges the regulatory framework of EU Member States' institutions, their private businesses and the EU as a whole.[5] Prior to forming a broad concept of "EU cybersecurity law", it is of utmost importance to scrutinize the severe impact a malicious cyber-attack can cause on different stakeholders.

To this end, we choose to study the large-scale cyber-attack "Wannacry", which "brought the issue of cyber resilience into the mainstream of public and political discourse", and we use it to shed some light upon what EU cybersecurity laws are about.[6]

On 13th May, 2017, the last business day of the week, a message reading *"Oops, your files have been encrypted"* appeared on more than 200.000 computer screens throughout the world demanding a ransom of between $ 300 and $ 600 being paid in Bitcoin in exchange

5 Maria Solarte-Vasquez and Katrin Nyman Metcalf, "Smart Contracting: A Multidisciplinary and Proactive Approach for the EU Digital Single Market", *Baltic Journal of European Studies,* vol. 7, no. 2 (2017), p. 218.

6 Julian King, "Commissioner King's keynote speech at the, 'WannaCry again? Making our businesses digitally great and cyberproof' conference", 15 February, 2018. Online at: https://ec.europa.eu/commission/commissioners/2014-2019/king/announcements/commissioner-kings-keynote-speech-wannacry-again-making-our-businesses-digitally-great-and_en. "Last year, the WannaCry malware did not just cause computers to freeze, but hospitals to close. It brought the issue of cyber resilience into the mainstream of public and political discourse."

for decrypting files stored on compromised devices.[7] Various major businesses in the European Union as the French carmaker Renault, the German transport company DB, or Spain's telecommunications operator Telefónica felt victim to the ransomware attack, which these companies could have avoided had they followed Microsoft's advise in March to close a vulnerable loophole in the Windows operating system by updating their computer software.[8] One of the gravest consequences of the disruptive attack was witnessed by the British National Health Service (NHS), where 80, or one third of all NHS trusts and 595 general practises were forced to cancel almost 19000 appointments, hundreds of surgeries and even cancer referrals.[9] Wannacry did not hold back from spreading to devices in critical infrastructure, disrupting information systems, which store laboratory data and radiographs.[10]

The malware had two components. The first, called EternalBlue, a tool exploiting a vulnerability in Windows operating systems enabling the worm to reach other computers without the end user's

7 Russell Goldman, "What We Know and Don't Know About the International Cyberattack," The New York Times, 12 May, 2017. Online at: https://www.nytimes.com/2017/05/12/world/europe/international-cyberattack-ransomware.html; see also: Chris Graham, "NHS cyber attack: Everything you need to know about 'biggest ransomware' offensive in history," *The Telegraph*, 20 May 2017. Online at: https://www.telegraph.co.uk/news/2017/05/13/nhs-cyber-attack-everything-need-know-biggest-ransomware-offensive/.

8 Sam Jones, "Timeline: How the WannaCry cyber attack spread," *FT*, 14 May, 2017. Online at: https://www.ft.com/content/82b01aca-38b7-11e7-821a-6027b8a20f23; consider also: Handelsblatt, "Cyberangriff legt 450 Bahn-Computer lahm,", 16 May 2017. Online at: https://www.handelsblatt.com/unternehmen/handel-konsumgueter/wanna-cry-cyberangriff-legt-450-bahn-computer-lahm/19809190.html?ticket=ST-2221470-N9RWTH0YgdtJ5A3foRbK-ap2); see further: Michael Schilliger, "Elf Antworten zur Cyberattacke 'WannaCry'," *NZZ*, 13 May, 2017. Online at: https://www.nzz.ch/digital/globaler-cyberangriff-sieben-antworten-zur-cyberattacke-wanacrypt-20-ld.1292982).

9 National Audit Office, *Investigation: WannaCry cyber attack and the NHS*, 25 April, 2018. Online at: https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf; see further: Graham, *supra* note 7; see also: BBC, "NHS 'could have prevented' WannaCry ransomware attack," 27 October, 2017. Online at: https://www.bbc.com/news/technology-41753022.

10 Schilliger, *supra* note 8.

permission through channels created to transmit and share data.[11] As soon as a recipient opened an enclosed file in an email, which contained the malicious programme, the malware started spreading at an unprecedented speed to other Windows systems linked to the infected computer.[12] The second element pertains to the encryption of the files stored on the computer, locking down data and systems. A message box popped up on the screen demanding the user to pay in cryptocurrency to restore the accessibility of one's data.[13]

It is worthwhile mentioning that the disruptive component of Wannacry, EternalBlue, was initially written by the N.S.A. to take advantage of Windows's vulnerability for spying activities on companies and foreign intelligence services.[14] One month prior to the

11 Qian Chen & Robert Bridges, "Automated Behavioral Analysis of Malware: A Case Study of WannaCry Ransomware," Conference Paper (2017), at 2: "The dropper of the malware carries two components. One uses the "EternalBlue" exploit against a vulnerability of Windows' Server Message Block (SMB) protocol to propagate, and the other is a WannaCry ransomware encryption component."; see further: Liliy Hay Newan, "The Ransomware Meltdown Experts Warned About Is Here," *Wired*, 5 December, 2017. Online at: https://www.wired.com/2017/05/ransomware-meltdown-experts-warned/ "Once WannaCry enters a network, it can spread around to other computers on that same network, a typical trait of ransomware that maximizes the damage to companies and institutions.".

12 Nicole Perlroth and David E. Sanger, "Hackers Hit Dozens of Countries Exploiting Stolen N.S.A. Tool," *The New York Times*, 12 May, 2017. Online at: https://www.nytimes.com/2017/05/12/world/europe/uk-national-health-service-cyberattack.html?hp&action=click&pgtype=Homepage&clickSource=story-heading&module=first-column-region&region=top-news&WT.nav=top-news: "The malware was circulated by email. Targets were sent an encrypted, compressed file that, once loaded, allowed the ransomware to infiltrate its targets. The fact that the files were encrypted ensured that the ransomware would not be detected by security systems until employees opened them, inadvertently allowing the ransomware to replicate across their employers' networks."; see also: Graham, *supra* note 7: "Hackers have been spreading "ransomware" called WannaCry, also known as WanaCrypt0r 2.0, WannaCry and WCry. It is often delivered via emails which trick the recipient into opening attachments and releasing malware onto their system in a technique known as phishing".

13 See e.g.: Goldman, *supra* note 7.

14 Schillinger, *supra* note 8; see also: The International Institute for Strategic Studies, "The WannaCry ransomware attack," *Strategic Comments*, vol. 23, no. 4 (2017), at vii-viii.

attack, this crucial element of the code turned out to have fallen into the hands of a cyber criminal group, known as "Shadow Brokers" who leaked it to the public on their webpage in April.[15] Various actors, there under Microsoft, heavily criticised the N.S.A. and some even claimed that it should incur responsibility for the cyber-attack.[16]

2.2 Response and impact

Amid the outbreak of the virus, Microsoft provided an emergency patch to Windows XP, Windows 2003 and Windows 8 users that helped prevent the malware from spreading further.[17] Additionally,

15 The International Institute for Strategic Studies, *supra* note 14; consider also: Andy Greenberg, "Hold North Korea Accountable for Wannacry – and the NSA, too," *Wired*, 19 December, 2017. Online at: https://www.wired.com/story/korea-accountable-wannacry-nsa-eternal-blue/: "WannaCry's origins stretch back to April, when a group of mysterious hackers calling themselves the Shadow Brokers publicly released a trove of stolen NSA code. The tools included an until-then-secret hacking technique known as EternalBlue, which exploits flaws in a Windows protocol known as Server Message Block to remotely take over any vulnerable computer".

16 Brad Smith, "The need for urgent collective action to keep people safe online: Lessons from last week's cyberattack," The Al Blog, 14 May, 2017. Online at: https://blogs.microsoft.com/on-the-issues/2017/05/14/need-urgent-collective-action-keep-people-safe-online-lessons-last-weeks-cyberattack/sm.001p0mwmqc3 ld351 07z1pj4ntjs26: "{E}xploits in the hands of governments have leaked into the public domain and caused widespread damage. An equivalent scenario with conventional weapons would be the U.S. military having some of its Tomahawk missiles stolen. And this most recent attack represents a completely unintended but disconcerting link between the two most serious forms of cybersecurity threats in the world today – nation-state action and organized criminal action."; see also: Greenberg, supra note 15; see further: Ellen Nakashima and Craig Timberg, "NSA officials worried about the day its potent hacking tool would get loose. Then it did.," The Washington Post, 16 May, 2017. Online at: https://www.washingtonpost.com/ business /technology/nsa-officials-worried-about-the-day-its-potent-hacking-tool-would-get-loose-then-it-did/2017/05/16/50670b16-3978-11e7-a058-ddbb23c75d82_story. html? noredirect=on&utm_term=.ececf4d96f19.

17 Mark Scott and Nick Wingfield, "Hacking Attack Has Security Experts Scrambling to Contain Fallout," *The New York Times*, 13 May, 2017. Online at https://www.nytimes.com/2017/05/13/world/asia/cyberattacks-online-security-.html: "Microsoft took the unusual step of releasing free security patches for older versions of Windows, including Windows XP, that it no longer routinely updates. It said the patches could help protect users from attacks, which have not targeted Windows 10, the latest edition of the software." Greenberg, *supra* note 15.

by coincidence a security analyst from the UK found a ‘’kill switch“ in the code, which he activated by purchasing a web address the ransomware inquired.[18] The attack subsided significantly after a few days, but the vulnerability in the systems remained for those computers that had still not been updated since the hackers could easily rewrite the code and infect other systems without a kill-switch implanted. It was also for this reason the European Cybercrime Centre (EC3), Europol, distributed awareness materials on social media platforms and created an information webpage outlining key strategies on how to protect private data from malware attacks.[19] In addition, it referred to the NoMoreRansom initiative, which primarily informs and dissuades consumers affected by ransomware from financing cybercrime activities.[20] The majority of large corporations did not give in to the demands of the cyber criminals and spend most resources on either rebuilding or restoring data from backups.[21]

The cyber-assault has been attributed to the State sponsored North Korean cybercrime group called “Lazarus” and affected thousands of

18 Jones, *supra* note 8: “Security analysts stress it could have been worse but for the actions of an anonymous British security researcher. After lunch on Friday, a 22-year-old cyber analyst, who writes online under the pseudonym MalwareTech, returned to his desk and spotted something crucial in WannaCry’s code — the first stage of its infection process. The obscure web address the ransomware was querying, he noticed, was unregistered and inactive. So he bought it for $11 and activated it. It turned out to be a form of “kill switch” baked into WannaCry by its creators. Activating the address told the ransomware, upon each new infection, not to proceed any further. Once he had control of it, WannaCry was stopped in its tracks”.

19 Europol, “How does the WannaCry ransomware work?,” 4 December, 2018. Online at: https://www.europol.europa.eu/wannacry-ransomware); see also: General Secretariat of the Council of the European Union, Cybersecurity – Information from the Commission, 9621/17, 31 May, 2017, at 2: “In the context of the public response to the WannaCry attack, Europol (via its European Cybercrime Centre [EC3]) created a dedicated information page 3 and disseminated flyers and awareness materials via Europol social media channels”.

20 General Secretariat of the Council of the European Union, *supra* note 19, at 2.

21 Jonathan Beer, “WannaCry” ransomware attack losses could reach $4 billion,” *CBSNews*, 16 May, 2017. Online at: https://www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses/: “Most of the organizations won’t pay {…} “They will rebuild and recover from their backups or other sources.”

companies and public services worldwide.[22] In an interview with the German news service "Tagesscha" the head of Europol, Steven Wilson, described the events as the "largest cyber-attack the world witnessed so far" taking a great toll on the economy.[23] In the same vein, leading IT experts as Mikko Hyppönen spoke of the "largest ransomware-epidemic in history".[24] Ransomware attacks were not a new phenomenon in 2017. The magnitude of Wannacry, however, was "unprecedented" with over 230.000 computers in 150 countries being targeted in total.[25] It was not without reason why also the director of the European Union Agency for Law Enforcement Cooperation, Rob Wainright, classified the virus as a novel type of malicious attack.[26]

Considering the EU's efforts on strengthening stability of cyberspace through international cooperation, one month after Wannacry unfolded, the Council of the European Union approved the "Draft Council Conclusions on a Framework for a Joint EU Diplomatic

22 BBC, "Cyber-attack: US and UK blame North Korea for WannaCry," 19 December, 2017. Online at: https://www.bbc.com/news/world-us-canada-42407488; see also: Reuters, "Britain believes North Korea was behind 'WannaCry' NHS cyber attack," 27 October 2017. Online at: https://uk.reuters.com/article/us-britain-security-northkorea/britain-believes-north-korea-was-behind-wannacry-nhs-cyber-attack-idUKKBN1CW153.

23 Tagesschau, "Europol zu WannaCry: Das ist der größte Cyberangriff bisher," 17 May, 2017. Online at: https://www.tagesschau.de/ausland/europol-wannacry-101.html.

24 Spiegel Online, "WannaCry" – Attacke – Fakten zum globalen Cyberangriff," 13 May, 2017. Online at: http://www.spiegel.de/netzwelt/web/wannacry-attacke-fakten-zum-globalen-cyber-angriff-a-1147523.html.

25 Europol, *supra* note 19: "The recent attack is at an unprecedented level and requires a complex international investigation to respond effectively and identify the culprits." Consider also: Julian King, "Commissioner King's speech at the EU Cybersecurity *Conference Digital Single Market, Common Digital Security 2017*," 15 September, 2017. Online at: https://ec.europa.eu/commission/commissioners/2014-2019/king/announcements/commissioner-kings-speech-eu-cybersecurity-conference-digital-single-market-common-digital-security_en.

26 CBS, *supra* note 21: "There is no precedent for a ransomware attack of this kind of scale," {…}. This is the first one that we have seen … that has been able to attack computers directly with this kind of success."

Response to Malicious Cyber Activities", the so-called "Cyber Diplomacy Toolbox".[27] With this initiative, the EU member states reiterated that cyber-attacks do not occur in a legal vacuum and agreed that the EU will respond with restrictive measures against individuals affiliated with cybercriminal gangs or even against states which promote such malicious activities by providing either sanctuary for them or hire them for political purposes.[28]

As stated by the General Secretariat of the Council of the EU, the Wannacry ransomware attack triggered cooperation between Member States within the framework of the NIS directive.[29] For the first time since its adoption, the affected EU countries exchanged intelligence on a cyber-attack on this legal basis.[30] In the State of the Union Address in 2017, the president of the EU Commission, Jean-Claude Juncker, mentioned cyber security as the EU's fourth policy priority of the subsequent year.[31] In summer 2018, the Council of the EU

27 Council of the European Union, *Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox") – Adoption*, 7923/2/17 REV 2, 7 June 2017.

28 *Ibid*: "The EU affirms that malicious cyber activities might constitute wrongful acts under international law and emphasises that States should not conduct or knowingly support ICT activities contrary to their obligations under international law, and should not knowingly allow their territory to be used for internationally wrongful acts using ICTs, as it is stated in the 2015 report of the United Nations Groups of Governmental Experts (UN GGE). {...}. The EU affirms that measures within the Common Foreign and Security Policy, including, if necessary, restrictive measures, adopted under the relevant provisions of the Treaties, are suitable for a Framework for a joint EU diplomatic response to malicious cyber activities and should encourage cooperation, facilitate mitigation of immediate and long-term threats, and influence the behavior of potential aggressors in a long term."

29 General Secretariat of the Council of the European Union, *supra* note 19: "The recent WannaCry cyberattack where a wave of ransomware attacks impacted organizations and citizens across the globe was the first time where Member States exchanged information on cybersecurity incident within the mechanism for operational cooperation under the NIS Directive, the so-called Computer Security Incident Response Teams network. This is yet another real-life example that proves how important cooperation in the area of cybersecurity is."

30 *Ibid*.

31 Jean-Claude Juncker, "Fourth priority for the year ahead: I want us to better protect Europeans in the digital age." Online at: http://europa/eu/rapid/press-release_SPEECH-17-3165_en.htm.

recalled the Commission's 2017 recommendation on creating a "Coordinated Response to Large-scale Cybersecurity Incidents and Crises" and underlined, *inter alia*, that EU Member States "need to make use of the existing crisis management mechanisms, processes and procedures at national and European level".[32]

Debating malicious cyber activities in the EU, eleven months after the attack, the Foreign Affairs Council of the EU "condemn{ed} the malicious use of information and communications technologies (ICT), including in Wannacr" and "stresse{" that cyber-attacks "undermin" the EU's "stability, security and the benefits provided by the internet and the use of ICT".[33]

Considering the harms caused by Wannacry, even though none was injured or killed nor data had been stolen in the attack, (1) the economic damage was significant.[34] Whereas Cyence Risk Analytics estimated the costs at $ 4 billion, others predicted a loss of hundreds of millions of dollars.[35] (2) Not only did the assault temporarily hamper the companies' productivity, (3) but it also worsened their business reputation. Looking at the case of the NHS, the British public was seriously concerned about its national health service and questioned its failure to keep up with modern cybersecurity standard.[36] The image of the NHS suffered further when the UK

32 General Secretariat of the Council, *supra* note 19, at 2-3.

33 Council of the European Union, *Council conclusions on malicious cyber activities – approval*, 7517/18, 16 April 2018: "The EU firmly condemns the malicious use of information and communications technologies (ICTs), including in Wannacry and NotPetya, which have caused significant damage and economic loss in the EU and beyond. Such incidents are destabilizing cyberspace as well as the physical world as they can be easily misperceived and could trigger cascading events. The EU stresses that the use of ICTs for malicious purposes is unacceptable as it undermines our stability, security and the benefits provided by the Internet and the use of ICTs."

34 Suzanne Barlyn, "Global cyber attack could spur $53 billion in losses: Lloyd's of London," *Reuters*, 17 July 2017. Online at: https://www.reuters.com/article/us-cyber-lloyds-report-idUSKBN1A20AB.

35 Beer, *supra* note 21: "Cyber risk modeling firm Cyence estimates the potential costs from the hack at $4 billion, while other groups predict losses would be in the hundreds of millions."

36 Graham, *supra* note 7; see also: BBC, *supra* note 22.

Department of Health and Social Care made public that Wannacry resulted in a loss of £ 92 million in British taxpayers money.[37] (4) Decreased public confidence into e-services, which many EU-citizens rely on in their everyday-life[38], and into the security of computer systems in general, that store vast amount of sensible private data of millions of clients and patients, constituted additional harms. (5) Taking a broader view on the effects of the attack, it can be said that cyberspace and the physical world in general was destabilized. (6) Critical infrastructures were affected in the EU, which is concern for the sovereignty and territorial integrity of the Member States.

Despite the Commission's multidimensional approach in improving the EU member states' cyber resilience, there is no commonly accepted definition of cybersecurity in the EU, leaving each of the EU governments room for different interpretation of this increasingly important legal area. Juncker's statement that cyber threats could destabilize the economy of democracies more effectively than ''guns and tanks" given the speed and virulence malware spread with, serves as further proof for the need to formulate the idea of EU cybersecurity law.[39] With European cybersecurity being challenged every day, the EU's goal to harmonize national law systems of member states in regard to cyber security and therefore increase the EU's resilience against cyber-attacks can be better attained if the affected states identified the multifarious harmful effects on their economy and society. With six main harms caused by Wannacry being established, the subsequent chapters set out the core elements of EU cybersecurity law.

37 Matthew Field, "WannaCry cyber attack cost the NHS £92m as 19.000 appointments cancelled," *The Telegraph*, 11 October 2018. Online at: https://www.telegraph.co.uk/technology/2018/10/11/wannacry-cyber-attack-cost-nhs-92m-19000-appointments-cancelled/.

38 Tanel Kerikmäe (ed.), *Regulating eTechnologies in the European Union: Normative Realities and Trends*, 2014, p. 1.

39 Jean-Claude Juncker, *supra* note 31: "Cyber-attacks can be more dangerous to the stability of democracies and economies than guns and tanks{…} Cyber attacks know no borders and no one is immune".

3. Cybersecurity: lost in translation?

3.1 Lack of consistent terminology

The cybersecurity field in general uses many concepts from neighbouring domains, but it has been infiltrated with terms from political science as well.[40] Cybersecurity is not synonymous with security of network and information systems, although for the last few years there has been some confusion for a good reason, which was also pointed out in a recommendation by the European Network and Information Security Agency (ENISA): Member States should "[a]gree on a commonly accepted working definition of cyber security that is precise enough to support the definition of common goals across the EU".[41] Cybersecurity remains a field where different perceptions and narratives determine its content for the respective actor, in particular that EU Member States emphasize certain aspects of cybersecurity in their strategic and policy documents, while downplaying others.[42] Terminology used in international forums, such as the UN, where discussion is held about 'information security' (although certainly deals with issues above the micro-level), reflects on the lack of coherent conceptual framework in this field.[43]

40 For example it is customary to label some hacker groups as 'Advanced Persistent Threat' or APT, in addition to giving them descriptive fantasy names, such as APT29 or Cozy Bear – a Russian hacker group believed to be associated with Russian intelligence.

41 ENISA, National Cyber Security Strategies – Setting the course for national efforts to strengthen security in cyberspace, 2012. p. 12. Online at: https://www.enisa.europa.eu/publications/cyber-security-strategies-paper)

42 See the different national concepts in the cybersecurity strategies of EU Member States, collected at ENISA website. Online at: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map.

43 The UK in its 2017 Response to General Assembly resolution 71/28 "Developments in the field of information and telecommunications in the context of international security" stated that "The United Kingdom uses its preferred terminology of 'cybersecurity' and related concepts throughout its response, to avoid confusion given the different interpretations of the term 'information security' in this context." Online at: https://www.un.org/disarmament/topics/informationsecurity/.

The difference between data security and network and information security[44] also needs to be emphasized, since although data security is a vital component of cybersecurity, for instance the Wannacry attack compromised more than just the availability of data and affected European critical infrastructure operators in the health, energy, transport, finance and telecom sectors, manufacturers and service providers throughout Europe.[45] Data and information is held in systems and transmitted through networks, which are increasingly relied on for everyday services, in particular when put into the context of Internet of Things era, where billions of appliances are connected to the internet. Focusing on information and data security, as well as systems and network security ensures that threats to cyber-physical systems, such as smart grids, autonomous automobiles, medical monitoring, industrial control systems, robotic surgery systems, etc. are also addressed. In turn, this enables regulators to link security compromises of systems and networks to their consequences, such as potential physical injuries or property damages.

A working definition of cybersecurity has been used in the 2013 Cybersecurity Strategy of the European Union, which in footnote no. 4 states that "Cyber-security commonly refers to the safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure. Cybersecurity strives to preserve the availability and

44 The ISO/IEC 27000: 2017 standard defines information security as the 'preservation of confidentiality, integrity and availability of information'. ISO/IEC 27032:2018 refers to network security as it 'is concerned with the design, implementation and operation of networks for achieving the purposes of information security on networks within organizations, between organizations, and between organizations and users'. ISO/IEC 27032:2018 defines cyberspace security as 'Preservation of confidentiality, integrity and availability of information in Cyberspace', and it emphasizes that cybersecurity is not synonymous with information, network, internet security or critical information infrastructure protection.

45 ENISA, WannaCry Ransomware: First ever case of cyber cooperation at EU level, 15 May, 2017. Online at: https://www.enisa.europa.eu/news/enisa-news/wannacry-ransomware-first-ever-case-of-cyber-cooperation-at-eu-level.

integrity of the networks and infrastructure and the confidentiality of the information contained therein." [46] The High Level Scientific Advisors on cybersecurity in the European digital single market has also added the same definition to their glossary, but felt that this needs to be complemented by a reference to "prevention and law enforcement measures to fight cybercrime".[47]

These approaches made little distinction between the technically oriented concepts, such as network and information security, and the emerging understanding seems to be that cybersecurity addresses concerns beyond the micro level of organizations and businesses. ENISA has also concluded that "[c]ybersecurity is an enveloping term and it is not possible to make a definition to cover the extent of the things Cybersecurity covers", however contextual definitions are already in use.[48] Therefore, we do not aim to define cybersecurity in this paper, but we work with existing understandings, in order to put cybersecurity into context for the legal community.

3.2 Cyberspace elements - what needs to be secured?

In order to unlock the concept of cybersecurity law, we need to find the constitutive elements of cyberspace that needs to be secured. We adopt the definition by Ottis and Lorents, who stated that "cyberspace is a time-dependent set of interconnected information systems and

46 European Commission, "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," 7 February, 2013.

47 SAM High Level Scientific Advisors, Scientific Opinion, no. 2/2017, Cybersecurity in the European Digital Single Market, 27 March 2017, p. 97. Online at: https://ec.europa.eu/research/sam/pdf/sam_cybersecurity_report.pdf#view=fit&pagemode=none.

48 ENISA, "Definition of Cybersecurity – Gaps and overlaps in standardisation", December 2015. Online at: https://www.enisa.europa.eu/publications/definition-of-cybersecurity.

human users that interact with these systems".[49] It is thus revealed that two elements of the system (cyberspace) are information systems and human users, and the properties of these elements are interconnectedness and interaction with information systems respectively. Cybersecurity laws can relate to either of these elements, i.e. addressing the state of information systems or conduct of human users. Norms expressed in regulatory instruments aim to influence these elements, by stating that "something ought to or may or must not be or be done".[50]

As to the first element, information systems, we can find that concepts of network- and information security and relating industry standards have already elaborated on how to approach the task of securing interconnected information systems (which necessarily include infrastructure, networks, data and information). [51] Cybersecurity professionals commonly refer to three security requirements, confidentiality, integrity and availability, known as the "CIA Triad"[52], which can relate not only to data and information in systems and networks, but also to systems and networks themselves.[53]

As to the second element of cyberspace, the human user, however, it also becomes clear that the technically-oriented approach to cybersecurity, when nearly-equated with network and information security, might lose sight of a constitutive element of the system: the human user that interact with information systems.

49 Ottis, R., Lorents, P., Cyberspace: Definition and Implications. In Proceedings of the 5th International Conference on Information Warfare and Security, Dayton, OH, USA, 8/9 April, 2010. Reading: Academic Publishing Limited, pp. 267-270.

50 G. H. v. Wright, Norm and Action, 1963.

51 See a reference material for relevant standards in ENISA, Definition of Cybersecurity, Gaps and overlaps in standardization, 2015. Online at: https://www.enisa.europa.eu/publications/definition-of-cybersecurity.

52 According to ISO/IEC 27000/2017. Confidentiality refers to a property that information is not made available or disclosed to unauthorized individuals, entities or processes; Integrity is the property of accuracy and completeness; and Availability is the property of being accessible and usable upon demand by an authorized entity.

53 See also this approach in Jeff Kosseff, Defining Cybersecurity Law, Iowa Law Review, vol. 103: 985, 2018, pp. 985-1031.

Solms and Niekerk held that while information security refers to the human users' role in the security process, in cybersecurity humans become targets or inadvertent participants of cyber-attacks, hence there are threats that fall outside the scope of information security.[54] Examples include cyber bullying, which does not (necessarily) constitute loss of confidentiality, integrity and availability of data, systems or networks, but causes a direct harm to the person being bullied.[55] Another case in point would be interference with automated home appliances, such as a security system, which can be remotely turned off in order to burgle the home, where again it can be argued that there is no impact on confidentiality, integrity and availability of information assets and system of the victim.[56] Affected are other assets of the person. Accordingly, cybersecurity is more than the mere protection of networks and information systems, it also covers the protection of functions and assets that rely on or can be reached via cyberspace.[57]

Therefore the process of cybersecurity should have aims and objectives that goes beyond the mere protection of confidentiality, integrity and availability of information, systems and networks themselves, and address the harms that may result as a consequence of degradation of functioning of computer systems, or due to interference with some interactions between information systems and their users. Yet, we should be more focused on aggregate interactions, from the perspective of the society. In the cyber-enabled society, where information's importance is equivalent to that of money, energy, etc. and computerized systems are used to govern the society, in the center of focus are threats, risks, incidents, unlike in approaches

54 Rossouw von Solms, Johan van Niekerk, From information security to cyber security, Computers & Security, 38, 2013, pp. 97-102.
55 Ibid. 99.
56 Ibid.
57 Ibid. 102.

to information society, e-society or IT society etc.[58] In other words the main point of concern for cybersecurity is the functioning of societies that - to any degree - depend on computerized systems to the extent that severe degradation in the functioning of these computerized systems can pose an existential threat to that society.[59] But interference with interactions between the society and computerized systems can also have similar impact.

Examples can include the degradation of the functioning of the information systems in the financial sector as a whole, in a society, where 98% of all financial transactions are completed via electronic means. The consequences of such events in 2007 in Estonia were felt not only on the level of the individual financial institutions, such as the interruption of their operations and unavailability of internet banking interfaces for customers, etc. but it affected the financial sector as a whole. Similarly, the Wannacry attack bore significant influence on individual companies and institutions, but the scale of disruption also affected the normal existence of the society in the UK, 80 out of 236 hospital trusts' services were impacted, and 8% of General Practitioners practices felt victim to the attack.[60]

However, degradation of the functioning of computer systems may not always be involved, where we can still detect interference with interactions between society and information systems, in particular taking into account the recent years technological developments in the field of artificial intelligence. For example in case using troll armies (automated, or potentially artificial intelligence based) in social media networks to polarize audiences on social and political issues, do not necessarily degrade the functioning of information systems and

58 Lorents P., Ottis R., Rikk R., Cyber Society and Cooperative Cyber Defence, in: Aykin N. (eds) Internationalization, Design and Global Development, IDGD, 2009. Lecture Notes in Computer Science, vol. 5623, Springer, Berlin/Heidelberg.

59 Ibid, p. 180.

60 UK, NHS Report, "Lessons learned review of the WannaCry Ransomware Cyber Attack", 2018. Online at: https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf .

networks, but aims to influence the interactions between the systems and users. A recent media report in 2018 stated that Russian troll factories have been used to discredit life-saving vaccines.[61] Shortly before this, the World Health Organization also published worrisome statistics indicating record high measle cases, including at least 37 fatal infections in Europe in 2018, although vaccination provides effective protection against the disease.[62] We are not able, nor have the intention to show a causal link between the troll's action and the measles outbreak in this particular case, nevertheless it suggests the magnitude of impact of a potentially effective campaign by trolls to manipulate the population into self-harming behaviour, or as we see it interfering with the interactions between the society and computerized systems, without degrading the functioning of these systems.

3.3 Towards a consequences-based approach to cybersecurity in the EU

The EU's cybersecurity efforts as a whole reflect a comprehensive understanding and approach, however it has been characterized by commentators as fragmented, and patchwork.[63] The EU has recently reached a political agreement on the Cybersecurity Act that signifies a global landmark in cybersecurity legislation.[64] Article 2 (1) of the (still) draft defines cybersecurity for the purposes of the regulation as "all activities necessary to protect network and information systems,

61 Harry de Quetteville, "How Russian troll factories used Twitter to discredit life-saving vaccines", *The Telegraph*, 13.10.2018. Online at: https://www.telegraph.co.uk/news/0/inside-story-russian-troll-factories-using-twitter-discredit/.

62 World Health Organization Regional Office for Europe, "Measles cases hit record high in the European Region", 20.08.2018. Online at: http://www.euro.who.int/en/media-centre/sections/press-releases/2018/measles-cases-hit-record-high-in-the-european-region.

63 Maria Garzia Porcedda, "Patching the Pathchwork: appraising the EU regulatory framework on cybersecurity breaches", *Computer Law and Security Review,* 34, 2018, pp.1077-1098.

64 European Commission, "EU negotiators agree on strengthening Europe's cybersecurity", 11.12.2018. Online at: https://ec.europa.eu/commission/news/cybersecurity-act-2018-dec-11_en.

their users, and affected persons from cyber threats".[65] This definition departs from the previous ones in a very significant way, since in addition to networks and information systems, it views the human user as the constitutive element of the system to be secured. It also implies a two-way of interaction[66] between human users and information systems, and it recognizes that information and interaction with information systems can influence events and human behaviour and society outside cyberspace. Therefore, the definition encompasses both the user's effect on information systems and the information systems' effects on users, however it would be plausible to think that the main concern is not about isolated cases.

The Wannacry incident's scale and immediate consequences resulted in significant disruption of a service as a whole in the healthcare system in the UK. Therefore, due to the reliance on computerized systems in the provisions of healthcare services the interaction between users and respective information systems was compromised – some due to infection by the Wannacry cyptoworm, but others due to turning off systems and devices as a precaution.[67] In particular in the cases of turning off the systems as a precautionary measure in order to avoid infection, we can argue that the availability of information is not compromised (the computers and devices can be turned back on and usage may continue), yet the service that is underlied by these systems is hampered.

In 2017 the Estonian ID card crisis also demonstrated that concern about *potential* authenticity and integrity breaches can lead to

65 Interinstitutional File: 2017/0225(COD), Final version of the text on Proposal for *Regulation of the European Parliament and of the Council* on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act"). Online at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_15786_2018_INIT&from=EN.

66 Oxford dictionary defines interaction as reciprocal action or influence.

67 National Audit Office, Investigation: WannaCry cyber attack and the NHS, 25 April, 2018. Online at: https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf.

significant disruptions in the delivery of e-services, although there are no reports about actual misuses.[68] Also in this case the interaction between society and the Estonian information systems was significantly disrupted, raising additional questions about trust in the systems, although the integrity and authenticity of the services and data was not actually compromised, and systems could perform their functions just as before the discovery of the vulnerability. Again, as a precautionary measure Estonian authorities blocked digital certificates of 760 000 ID cards, and started to update those persons' certificates first, who need their ID cards for their work, such as doctors, justice officials, civil servants, etc.[69] The Estonian lessons learned show that a non-incident can create a significant crisis, comparable to that of an incident.

The definition of cybersecurity in the draft Cybersecurity Act resonates with the service-oriented approach of Solms and Niekerk.[70] It covers technical and non-technical activities, however in the absence of a clear definition of cybersecurity it is difficult to devise legal tests for the purposes of determining precisely what activities would fall into the above category. While functions of and services that networks and information systems should perform can relatively easily be identified in technical terms, what can be considered as adverse effect on users and other persons is more challenging to identify given the endless ways cyberspace can be used. The analysis of the Wannacry case has already pointed towards some harms that may be considered, therefore protective measures and activities should address, *inter alia*, the potential and actual economic damages, decrease in productivity, reputational damages, decrease of trust in computer systems, destabilization of physical world, and potential losses in sovereignty.

68 Tallinna Tehnikaülikool, ID-kaardi kaasuse õppetunnid, 2018. Online at: https://www.ria.ee/sites/default/files/content-editors/EID/id-kaardi_oppetunnid.pdf.
69 Ibid.
70 See 54.

We claim that what is to be secured by EU cybersecurity regulation are *interconnected information system*s, including data, information systems and networks, and aggregate *interactions* between human users and these information systems. In our view, what distinguishes network and information security regulation from cybersecurity regulation is that cybersecurity regulation aims to protect not only confidentiality, integrity and availability of data, information systems and networks[71], but also certain *interactions* between these and the society involving two or more Member States.

However, this line of thought and the proposed definition of cybersecurity by the EU Cybersecurity Act also opens a Pandora's box. What exactly is considered as a threat that can affect information systems' users and persons so that it becomes a concern for the EU? Which regulatory measures are best suited to address this issue? In which areas of cybersecurity management (i.e. prevention, detection, response, recovery) the EU is best placed to regulate? What oversight, supervision and enforcement measures ensure achievement of the objectives of the cybersecurity policy of the EU and respect the rule of law and fundamental human rights at the same time? The next part of this paper looks for some answers to these questions in the existing EU framework.

4. Cybersecurity laws

General legal frameworks and challenges

Gercke proposed a catalogue of "mandatory" and "optional" cybersecurity laws: the former category comprises of definitions, cybercrime laws and data protection legislation; while the latter optional areas include network and critical infrastructure protection, reporting obligations, international cooperation, electronic evidence,

71 This is a simplified view from us in respect of security requirements that can also include authenticity, non-repudiation, accountability, reliability, etc. depending on the precise standard, context and needs.

electronic transactions, digital signatures, child online protection, liability of internet service providers and potential restrictions on the use of certain technology.[72]

Gercke offered a comprehensive view on cybersecurity legal framework and also noted that cybersecurity was often conflated with cybercrime, however not all cybersecurity incidents are criminal acts.[73] Wannacry used a known vulnerability for which Microsoft had issued a security patch in March 2017 for supported Windows versions[74], and spread to devices that have not applied the update. Not applying this patch, or other similars, generally does not constitute a criminal act, but may give rise to disciplinary or negligence claims, or non-compliance with data protection regulations, etc. However, precisely the unpatched vulnerabilities in systems were exploited by the creators of the Wannacry cryptovirus, which can already be described in the terms of the Cybercrime Convention. Fight against and preventing cybercrime is but one component of cybersecurity.[75]

Cybersecurity is still often seen as a purely technical or awareness problem, not a legal one. Available reports on the reactions and lessons learned from Wannacry did not address legal issues at the affected organizations' level.[76,77] Nevertheless, there are significant information gaps, often framed as problems in cybersecurity information sharing among private sector players, between private and public sector and between countries. These issues reach beyond

72 Marco Gercke, Content of a Comprehensive Cybersecurity Legal Framework, Cri, 2/2014.

73 Marco Gercke, Content of a Comprehensive Cybersecurity Legal Framnework, Cri, 2/2014, p. 34.

74 See online at: https://support.microsoft.com/en-us/help/4013389/title.

75 Marco Gercke, Content of a Comprehensive Cybersecurity Legal Framework, Cri, 2/2014, p. 34.

76 See UK NHS Report, "Lessons learned review of the WannaCry Ransomware Cyber Attack", 2018. Online at: https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf .

77 See Deutsche Bahn Interim Report, January-June 2017. Online at: https://www1.deutschebahn.com/resource/blob/1047480/1f573efc5d5d1f119dba29a882272eea/zb2017_dbkonzern_en-data.pdf.

technology, and concern exceptions in the data protection regulation, breach notification obligations of operators (private or public) and information exchange on potentially national security-related questions between EU Member States when collectively planning prevention, detecting, responding to or recovering from cyber incidents and events.

In EU context it also needs to be clarified which issues fall within the competence of EU law and what aspects remain within the competence of Member States, how the two levels interact, respecting the main principles of subsidiarity and proportionality. This involves mapping of cross-border interdependencies of cyber societies, since while an availability crisis can hit across sectors, the Estonian ID-card (chip vulnerability) crisis appears to be more contextual in the absence of pan-European information systems for the support of relevant societal functions.

It would be expected that the EU's primary concerns are rather the generic and strongly interlinked services, however local cybersecurity management should also remain a high priority. In the light of the EU's own modest operational capabilities in this regard (such as ENISA still has only very limited resources and performs advisory, training and support functions, although there are plans to increase EU level capabilities[78]), the EU's role in securing cyber societies will probably remain mainly complementary and supportive to that of Member States, including coordination, providing platforms for information exchange and cooperation, harmonization, mediating capacity building, research and development, etc. The more intensive role will be confined to areas, were the EU has exclusive competence or shares competences with Member States, most prominently concerning the Digital Single Market. In the following chapters we outline the main existing and proposed EU documents and legislation

78 European Commission, "EU negotiators agree on strengthening Europe's cybersecurity", 11.12.2018. Online at: https://ec.europa.eu/commission/news/cybersecurity-act-2018-dec-11_en.

pertaining to cybersecurity, analyze what harms they aim to address and how, and point out pertinent issues legislators would have to devote further scrutiny on.

5. Conceptual shifts in EU cybersecurity policy

5.1 Initial place of cybersecurity concerns in EU legislation

The EU has demonstrated intensifying legislative activity in the field of network and information security since the early 2000's.[79] It was emphasized from the beginning that "security is becoming a key priority because communication and information have become a key factor in economic and societal development"[80] and many of the currently binding EU laws have their non-binding predecessors from 10-15 years ago addressed in the third pillar[81] of the EU[82].

Generally the provisions dealing with security in networks and information systems in early EU regulations had two main considerations: protection of privacy and personal data[83], and harmonizing requirements for the sake of completing the single

79 The first instrument with specific focus on security was the Commission's, 26.1.2001, Communication (COM(2000) 890 final), 'Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime'.

80 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 /COM/2001/0298 final/.

81 From 1993 until 2009 in the EU's 'three pillar system' the first pillar referred to economic, social and environmental policies; the second pillar stood for Common Foreign and Security Policy; and the third pillar consisted of Police and Judicial Cooperation in Criminal Matters.

82 See for example in the field of fighting cybercrime Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems, which was replaced by Directive 2013/40/EU of the European Parliament and of the Council of 12 August, 2013 on attacks against information systems.

83 See for example *Directive 97/66/Ec of the European Parliament and of the Council* of 15.12.1997, concerning the processing of personal data and the protection of privacy in the telecommunications sector.

market. However, the establishment of ENISA sparked a debate on the conceptual framework of network and information security in the EU, which was considered by the EU's court,[84] and it held that these measures also form "part of a normative context circumscribed by the Framework Directive and the specific directives and directed at completing the internal market in the area of electronic communications". [85] Therefore it can be claimed that the EU's primary concern was data security, and the broader network and information or cybersecurity aspects were rather incidental in special legal regimes[86], having to do more with the completion of the internal market, than with the potential harms that can result from misuses or degradation of functioning of computer systems. These provisions set

84 The legal basis for EU action in the 'first pillar' in the areas of network and information security has been addressed in case C-217/04 UK vs. EU Parliament and Council. More precisely, the establishment of ENISA by Reg. No 460/2004, its objectives and the tasks assigned to it by Regulation EC No. 460/2004 were regarded as measures for approximation in the meaning of Art. 114 of TFEU (ex Article 95 TEC).

85 C-217/04 United Kingdom vs. European Parliament and Council, paras. 59-60.

86 Several legal provisions were listed in the judgment that "express concern of the Community legislature in relation to network and information security". These included Article 8 (4) (c) and (f), framework dir. 2002/21/EC, which state the need for high level of protection of personal and privacy, as well for maintaining the integrity and security of public communications networks. The Authorization Directive 2002/20/EC briefly refers to security and personal data protection as part of those maximum conditions that may be attached to general authorization to provide electronic communication networks and services, and Article 23 of the Universal Service Directive 2002/22/EC refers to integrity and availability of public telephone services, in particular emergency services in cases of catastrophic events. More detailed provisions can be found in the e-Privacy Directive 2002/58/EC, which in Article 4 and 5 deals with network security and confidentiality of communications. Noteworthy in Article 4 that it requires service providers to take technical and organizational measures having regard to the state of the art, costs, appropriateness of measures and risks present, a language that reflect focus on prevention and will appear more prominently later and outside the narrow field of electronic communications. In addition to these, the Personal Data Protection Directive and the e-Signatures Directive also touched upon security issues within their specific contexts, in Article 17 and 3 (4) respectively. Certain other security aspects of digital assets, protection of intellectual property in the information society, are addressed by the EU's specialized regulatory regimes on copyrights, patents, database protection, etc.

out some vague and overall requirements for information and network security, but their scope was limited to the telecommunication sector, personal data protection and e-signatures. Therefore many information society services as they emerged fall outside the scope of these laws, such as most cloud services, search engines, e-marketplaces, internet telephony services, unless they were in the specific signal transmission business, which qualifies as electronic communications service for the purposes of the telecom regulations[87], or processed personal data and relevant data protection rules (eventually) came into play[88].

However, the legislative landscape has significantly changed since the first elements of cybersecurity-related provisions were put in place and whereas network and information security used to be understood as merely complementary to the electronic communications field, today the picture is more complex, in particular that cybersecurity is a broader concept than network and information security. Virtually the entire legal framework has already been revised and updated, yet a significant EU reform in cybersecurity has just begun. Today there are numerous legal instruments of the EU having a bearing on cybersecurity and several proposals are pending.

87 Article 2 (c) of the Framework Directive defines that "electronic communications service" means a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, but exclude services providing, or exercising editorial control over, content transmitted using electronic communications networks and services; it does not include information society services, as defined in Article 1 of Directive 98/34/EC, which do not consist wholly or mainly in the conveyance of signals on electronic communications networks.

88 Although some provisions of the Personal Data Protection Directive needed clarifications by the courts, for example in the Google vs Spain case (Case C-131/12), popularly known as addressing the ‘right to be forgotten’.

5.2 Cybersecurity becomes a priority

In the context of the second pillar of common foreign and security policy the 2007 cyber-attacks against Estonia have led to a turning point, and cybersecurity was identified as a security issue in the report on the implementation of the European Security Strategy (ESS) submitted by SG/HR Javier Solana to the European Council in December 2008.[89] The term "cybersecurity" turned into a policy buzzword after the adoption of the EU's 2013 Cybersecurity Strategy[90] and cybersecurity is now an integral part of EU policies. The document addressed cybersecurity in a comprehensive fashion and foresaw that proposed activities would operate within different legal frameworks, notably network and information security, law enforcement and defence, and on two levels, the national and EU level.[91] It established five priorities: achieving cyber resilience; drastically reducing cybercrime; developing cyber-defence policy and capabilities related to the Common Security and Defence Policy (CSDP); develop the industrial and technological resources for cybersecurity; and establish a coherent international cyberspace policy for the European Union and promote core EU values. The 2013 strategy is centered mostly on the importance of cybersecurity for economic reasons, but also mentions some particular concerns, thereby implying what harms are considered: economic losses both in terms of damages and decreased productivity, decreased confidence of citizens to use e-services, physical and impalpable harms to citizens, and the loss of autonomy for citizens outside the EU.

89 EEAS, "Report on the implementation of the European Security Strategy – Providing Security in a Changing World", 11.12.2018. Online at: https://europa.eu/globalstrategy/en/report-implementation-european-security-strategy-providing-security-changing-world.

90 *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, JOIN/2013/01 final.

91 Ibid. p. 17.

5.3 Raising the stakes: EU's new cybersecurity strategy

The overall strategy is currently formulated in the European Commission's Joint communication on Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, which updated the 2013 strategy document.[92] The new vision is moving from the comprehensive approach towards a more integrated one, where economic, political and strategic threats enjoy equal attention, and cybersecurity can be seen as a horizontal policy issue, or a common societal challenge, having elements in multiple layers of government, economy and society. Therefore, the updated strategy goes beyond the previously stated areas of network and information security, cybercrime, cyber defence and external relations, and proposes measures in product liability, consumer protection, labour market, financial services, education, trade and investment fields as well. Emphasis is on building resilience and deliver better EU response to cyber-attacks, signifying a shift from a reactive to a proactive approach.

The threats outlined in the introduction part of the Communication imply that the EU is ready to address potential harms by different measures. The concern about negative economic impact of misuses and degradation in the functioning of computer systems is still central, however the issue has grown in magnitude and worries are expressed about potential economic destabilization, decreased political autonomy, disrespect for territorial integrity, physical harms, decrease in consumer trust and the decreased ability of states to provide order in the society by enforcing their laws.

In the next section we identify legal measures that are either already available or are proposed and, if and when adopted, can be used in the future to address the potential and actual harms identified so far.

92 JOIN (2017) 450.

6. EU Cybersceurity Laws

6.1 Information society laws and cyber resilience

6.1.1 Electronic Communications

In 2009 several provisions requiring operators of electronic communications networks and services to implement security measures were incorporated into the EU's Telecom regulatory framework. The "Better Regulation Directive" established a regime for undertakings providing public communications networks or publicly available electronic communications services imposing requirements to implement risk-based security management practices, state-of-the-art technical and organizational measures, as well as to notify national authorities of a breach of security or loss of integrity incidents with significant impact.[93]

The newly adopted European Electronic Communications Code (EECC) kept the underlying structure of the security regime, however now it clearly includes security of networks and services and end-user benefits[94], whereas the EECC also extends to services that fall outside scope of the previous framework[95], adds definitions of "security of networks and service" and "security inciden", and clarifies a number of important points on the breach notification obligations, roles and powers of authorities and relevant institutions. This brings a significant expansion of the EU's oversight on the electronic

93 Articles 13a and 13b of *Directive 2009/140/Ec Of The European Parliament And Of The Council* of 25 November 2009, amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorization of electronic communications networks and services.

94 Art. 1 (2) (a) of the EECC, Proposal for a *Directive of the European Parliament and of the Council, E*stablishing the European Electronic Communications Code, COM/2016/0590 final – 2016/0288 (COD).

95 It was unclear whether i.e. if or to what extent internet telephony services or electronic processing services (for email service) fall under the regime. See for example Case C-142/18, Case C-193/18.

communications field, which will cover not only those service providers that operate the core communication infrastructures, but also those that built up new business models relying on the core infrastructures for the provision of their services, but not engaging in the "signal conveyance" business, hence did not fit the definition in Article 2 (c) of the Framework Directive[96]. The EECC redefines the meaning of "electronic communication service", now expressly including internet access service, interpersonal communication services (both number-based and number independent ones), as well as traditional signal conveyance.[97] This will result in higher-level security requirements imposed on a new layer of service providers in the field of communications in the EU, filling another gap in cybersecurity-related legislation. The EECC is to be implemented by the end of 2020.

6.1.2 Electronic Signatures and Trust Services

Significant piece of the cybersecurity puzzle lays with the eIDas Regulation[98] that replaced the 1999 e-signatures directive. It is hard to overestimate the role of the eIDas Regulation, since it lays down the foundations for mutual recognition and assessment of electronic identification or eID means, and it also defines assurance levels, i.e. criteria for assigning a degree of confidence for claimed or asserted

96 According to Directive 2002/21/EC, the Framework Directive, "electronic communications service" means a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, but exclude services providing, or exercising editorial control over, content transmitted using electronic communications networks and services; it does not include information society services, as defined in Article 1 of Directive 98/34/EC, which do not consist wholly or mainly in the conveyance of signals on electronic communications networks.

97 Article 2 (4) of the EECC.

98 Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July, 2014, on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

identity of persons by electronic identification means.[99] The second part of the eIDAS Regulation details the conditions and requirements for providing various trust services.[100] These trust services serve as points of reference for digital security, which include creation and verification of electronic signatures, website authentication, guaranteeing the origin and integrity of electronic seals, electronic time-stamps, etc. The Regulation establishes security requirements for trust service providers, referring to technical and organizational measures and risk-based approach[101], as well as breach notification obligations similarly to the EECC and NIS Directive. Our societies need reliable authentication and e-identification just as much as anonymity in cyberspace.

6.1.3 ISP liability

The e-commerce directive provides another pillar in cybersecurity-related legislation, more precisely it exempts intermediary service providers from liability for information transmitted, based on their neutral role[102]. Furthermore ISP's are not obliged to monitor their services and seek for illegal activity therein. The limits of this framework have been elaborated on in a series of court cases[103] and additional self-regulatory arrangements were established by concerned service providers in order to bridge the disconnect between illegal content online and enforcement mechanisms. However, the current regime is increasingly difficult to sustain, as these services can

99 Chapter II of *Regulation (Eu) No. 910/2014 of the European Parliament and of the Council* of 23 July, 2014, on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

100 Chapter III of the *Regulation (Eu) No 910/2014 of the European Parliament and of the Council* of 23 July, 2014, on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

101 Article 19.

102 Articles Directive 2000/31/EC of the European Parliament and of the Council of 8 June, 2000, on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market.

103 See for example ECJ cases Google vs Louis Vuitton and the others Joined Cases C-2366/08 and C-238/08; L'Oreal vs eBay Case C-324/09; Delfi vs Estonia at ECHR.

be abused by third parties and presence of illegal content online has serious consequences for users, potentially for societies.

There is abundance of illegal material online, and media frequently reports on one or another ISP failing to remove such content.[104] Illegal material can come in different forms and shapes, can range from copyright-infringing audiovisual media, hate-speech and information relating to terrorism, and child exploitative content. Recent EU legislation qualifies the liability exemption regime and accommodates the particularities of different illegal content online. Specific responses were designed in this respect, for example amending the Audiovisual Media Services Directive [105] and in Chapter XIa of setting forth rules particularly addressed to video-sharing platform services to protect the public from harmful material online, practically imposing an obligation on these providers to apply proactive measures to identify illegal activity and content online, albeit also encouraging co- and self-regulation. In addition the Commission has issued a recommendation to support this policy.[106] However the EU is drawing some red-lines in this field, since clear-cut rules were proposed in 2018 for cases when service providers have been informed about illegal activity, including the obligation of hosting service providers to remove terrorist content or disable access to it within one hour from receipt of a removal order issued by a competent authority. [107] These examples demonstrate the ongoing

104 See for example BBC report on Facebook failing to remove child exploitation images https://www.bbc.com/news/technology-39187929 or Business insider report on You tube's slow reaction to notifications about illegal content https://www.businessinsider.com/youtube-purges-over-400-channels-millions-of-videos-to-address-child-exploitation-concerns-2019-2.

105 Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November, 2018, amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) in view of changing market realities PE/33/2018/REV/1.

106 Commission Recommendation of 1 March, 2018, on measures to effectively tackle illegal content online (C (2018) 1177 final).

107 Proposal for a *Regulation of the European Parliament and of the Council* on preventing the dissemination of terrorist content online COM (2018) 640 final.

policy shift, where the liability exemptions of the neutral gatekeepers are curtailed – short of a better solution to address the proliferation of illegal online content.

6.1.4 Consumer protection

Generally the EU's consumer protection framework does not address problems of cybersecurity in specific terms, however some sporadic provisions already require that certain products are constructed so as to ensure the protection of personal data and privacy of users and subscribers. Article 3 and 4 of the Radio Equipment Directive contain broad requirements for data security for connected consumer products, such as smart watches, connected toys[108], drones, etc., however its operational range is still unclear.[109] Issues of basic encryption, software updates, weak or lack of authentication in connected consumer products, and product liability remain highly-debated open questions despite initiatives in this field.[110]

6.1.5 Payment Services

Among the sectoral measures the Second Payment Services Directive (PSD2)[111] should also be mentioned as contributing to building strong cybersecurity in Europe. In the PSD2 an additional element, strong customer authentication is emphasized[112], besides the risk-based management and incident reporting obligations imposed on payment

108 See for example a recent security alert for childrens' smart watches. Online at: https://ec.europa.eu/consumers/consumers_safety/safety_products/rapex/alerts/?event=viewProduct&reference=A12/0157/19&lng=en.

109 European Commission, *Report from the Commission to the European Parliament and the Council* on the operation of the Radio Equipment Directive, 2014/53/EU, COM(2018), 740 final.

110 See for example Proposal for a *Directive of the European Parliament and of the Council* on certain aspects concerning contracts for the supply of digital content, and the Commission is also reviewing the Product Liability Directive (Directive 85/374/EEC)

111 *Directive (Eu) 2015/2366 of the European Parliament and of the Council* of 25 November, 2015, on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No. 1093/2010, and repealing Directive 2007/64/EC.

112 Articles 97 and 98.

service providers. The European Banking Authority is currently working on a draft for regulatory technical standards on strong customer authentication and common and secure communication under Directive 2015/2366 (PSD2).[113]

6.1.6 Personal Data Protection

In several EU regulatory instruments preventive measures are dominant, paying less attention to incident response, recovery and business continuity aspects. The General Data Protection Regulation[114] can be seen as a cybersecurity instrument, essentially aiming to prevent misuses of personal data by imposing heavy limitations on their processing in the first place. Additionally the GDPR dedicates Article 32-34 to security of personal data, setting forth technical requirements and a breach notification regime. In this context, the Police Directive[115] applies a similar approach, prescribes security measures and notification obligations, however the scope is different [116] and it is complementary to the GDPR, within the competences of the EU. The above instruments, however say little about responding to security incidents and recovery from them. These aspects are apparently left for the particular organizations implicated and to standards to be applied.

113 See online at: https://eba.europa.eu/documents/10180/1761863/Final+draft+ RTS +on+SCA+and+CSC+under+PSD2+%28EBA-RTS-2017-02%29.pdf.

114 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April, 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

115 *Directive (Eu) 2016/680 of the European Parliament and of the Council* of 27 April, 2016, on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision, 2008/977/JHA.

116 The Directive applies to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

6.1.7 High Common Level Network and Information Security

Slightly more concern is given to incident response in the EU's first cybersecurity law, the Network and Information Security Directive[117], which obliges Member States to adopt national strategies for network and information security, aims to establish appropriate structures for national level management and cooperation among these in the EU, as well as it imposes important security requirements for operators of essential services and digital service providers. Although the NIS Directive signifies an important effort for harmonization in the field of cybersecurity, its effects are expected to be far weaker than it was intended in the original proposal put forth by the Commission, since public sector information systems as well as a portion of providers of information society services have been excluded from its scope and cooperation measures, including information sharing mechanisms, were reduced to the very minimum based on voluntary action by member states.[118]

This regulatory framework leaves the question of response and recovery aspects mainly open, however the European Commission has issued a Recommendation that serves as a blueprint for action in case of cyber incidents with EU-wide effects.[119] This plan was tested during the Wannacry incident first time, with reportedly positive results[120] and the case pointed out how important cooperation in the area of cybersecurity is. Yet cooperation in incident response is just one piece of the puzzle, as the 'non-incident' of the ROCA

117 *Directive (Eu) 2016/1148 of the European Parliament and of the Council* of 6 July, 2016, concerning measures for a high common level of security of network and information systems across the Union.

118 Compare the current NIS Directive to the Commission Proposal for a *Directive of the European Parliament and of the Council Co*ncerning measures to ensure a high common level of network and information security across the Union/* COM/2013/048 final – 2013/0027 (COD) *.

119 Commission Recommendation (EU) 2017/1584 of 13 September, 2017, on co-ordinated response to large-scale cybersecurity incidents and crises, C/2017/6100.

120 Online at: https://www.bna.com/wannacry-provided-first-n73014451505/.

vulnerability discovery caused a crisis situation in Estonia.[121] The Estonian experience with the naturally constrained flow of research and scientific information also makes the case for the establishment of European level network in this area.[122]

6.1.8 Cybersecurity Act

However, the European plans are more ambitious and cybersecurity is elevated to a significant policy issue, which requires appropriate coordination and enforcement mechanisms. The Commission has proposed the Cybersecurity Act, establishing a permanent mandate for the EU Cybersecurity Agency and a framework for cybersecurity certification.[123] The Explanatory Memorandum of the Cybersecurity Act mentions a number of policy areas, sectors and refers to legal acts, where the EU's Cybersecurity Agency (currently ENISA) will have assigned tasks.

These include, naturally the policy area of network- and information security, but also sectors with "cybersecurity element", such as

121 In 2017 the discovery of a vulnerability in the chips used in the Estonian ID-card led to serious concerns about the security of the infrastructure underlying the Estonian digital state. Although no security breaches or misuses were identified, the case pointed out some shortcomings in preparedness and unknown societal dependencies on current technologies. To mention a few points, the concentration of critical competences into a small number of experts and the unexpected dependency of the public sector and critical infrastructures on the ID-card for the performance of their tasks were brought to light. For an overview see online at: https://www.ria.ee/sites/default/files/content-editors/kuberturve/roca-vulnerability-and-eid-lessons-learned.pdf or the more detailed Estonian version online at: https://www.ria.ee/sites/default/files/content-editors/EID/id-kaardi_oppetunnid.pdf.

122 Proposal for a *Regulation of the European Parliament and of the Council* establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres. A contribution from the European Commission to the Leaders' meeting in Salzburg on 19-20 September, 2018, COM/2018/630 final.

123 Proposal for a *Regulation of the European Parliament and of the Counci*l on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act").

finance, transport, energy.[124] It is also foreseen that the Agency will support policy and law in electronic communications, electronic identity and trust services. The Network and Information Security (NIS) Directive has already been expressly tied to ENISA, entrusting it the coordination of CyberEurope cycle of exercises with Member States, assisting the Member States and the Commission with expertise, advice, guidelines and facilitating the exchange of best practices.[125] ENISA also has significant role in assisting in the implementation of legal and regulatory requirements of network and information security arising from the NIS Directive or any other legal act,[126] as well as it will report on the implementation of the EU legal framework. ENISA will be tasked to prepare a candidate European cybersecurity certification scheme. This process should result in establishing points of reference for the ''duty of care" principle and lead to the application of ''security by design and default" approach by producers of connected devices.

6.2 EU legal acts and cyber deterrence and defence

Since the adoption of the 2013 EU's Cybersecurity Strategy the legal framework tackling cybercrime has improved across the EU, whereas the substantive part of the Council of Europe Cybercrime Convention was practically implemented via the "Botnet Directiv".[127] The Directive does not address questions of self-defense and remedies for

124 Proposal for a *Regulation of the European Parliament and of the Council* on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act") COM(2017) 477 final, 13 September, 2017, p. 7.

125 *Directive (EU) 2016/1148 of the European Parliament and of the Council* of 6 July, 2016, concerning measures for a high common level of security of network and information systems across the Union.

126 Article 2 (3) of *Regulation (EU) No 526/2013 of the European Parliament and of the Council* of 21 May, 2013, concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004.

127 Directive 2013/40/EU of the European Parliament and of the Council of 12 August, 2013, on attacks against information systems and replacing Council Framework Decision 2005/222/JHA.

victims. The Botnet Directive is also complemented by another directive on combating sexual abuse and exploitation of children and child pornography.[128] Although there are still some open questions on implementation of the above Directives[129], the procedural and cooperation aspects of fighting cybercrime proved to be more controversial.

One of the major failures of EU legislators has been the Data Retention Directive[130], which was cancelled by the European Court of Justice due to its disproportionate measures obliging service providers to collect data on electronic communications. Since investigation, detection and prosecution of serious crimes is rather difficult when electronic communications data is unavailable or erased, imposing data retention obligations in the electronic communications sector appeared a reasonable step. However, in the Digital Rights Ireland case the Court pronounced that

> "[a]s regards the necessity for the retention of data required by Directive 2006/24, it must be held that the fight against serious crime, in particular against organised crime and terrorism, is indeed of the utmost importance in order to ensure public security and its effectiveness may depend to a great extent on the use of modern investigation techniques. However, such an objective of general interest, however fundamental it may be, does not, in itself, justify a retention measure such as that established by Directive 2006/24 being considered to be necessary for the purpose of that fight".[131]

128 Directive 2011/92/EU *of the European Parliament and of the Council* of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA

129 National transposition measures communicated by the Member States concerning: Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA. Online at: https://eur-lex.europa.eu/legal-content/EN/NIM/?uri=celex:32013L0040.

130 Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

131 Joined Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others, para 51.

The judgement opened the door for EU-wide fragmentation of data retention regulations, some Member States keeping their relevant national rules, some cancelling them, which also led the European Court to provide further guidance in two consecutive cases addressing details of and conditions of data retention.[132] However, pending the proposal for the e-Privacy Regulation and discussions on data retention ongoing in EU institutions, coupled with the strong requirements of the GDPR, which has already proven to be an obstacle for information sharing with entities outside the EU[133], the fate of the EU's data retention regime appears to be still uncertain.

Yet, rules on collection of data in cyberspace for the purposes of investigations and evidence remained a central issue, including for the purposes of attributing cyber-attacks to perpetrators. Just after the adoption of the US CLOUD Act[134], which confers jurisdiction on the US authorities to request data held overseas from US companies, the EU has came up with its e-Evidence proposals to create a European Production Order and a European Preservation Order[135], including allegedly strong, but controversial safeguards[136], as well as to oblige service providers to designate a legal representative in the Union for the purposes of the legislation. In addition, the Commission has presented further proposals, including one addressing fraud and counterfeiting of non-cash means of payments, extending the scope

132 Joined Cases C-203/15 and C-698/15, Tele2 Sverige and Case C-207/16 Ministerio Fiscal .

133 See for example European Data Protection Board, Letter to ICANN, 05 July, 2018. Online at: https://edpb.europa.eu/news/news/2018/letter-icann_en.

134 US, Clarifying Lawful Overseas Use of Data Act. Online at: https://docs.house.gov/billsthisweek/20180319/BILLS-115SAHR1625-RCP115-66.pdf#page=2201.

135 Proposal for a *Regulation of the European Parliament and of the Council* on European Production and Preservation Orders for electronic evidence in criminal matters COM/2018/225 final – 2018/0108 (COD).

136 For example Article 9 (5) of the proposal allows that private entities assess compliance with the Charter of Fundamental Rights of the European Union and object to cooperation on this ground.

of measures to virtual currencies.[137] The 2017 EU cybersecurity strategy addresses the question of deterrence as a mainly technical and capability issue, focussing on attribution, IPv6, forensic procedures and investigative capabilities of Member States' law enforcement authorities. In a recent initiative, the four EU cybersecurity organisations, ENISA, the European Defence Agency (EDA), the European Cybercrime Centre (EC3) and the Computer Emergency Response Team for the EU Institutions, Agencies and Bodies (CERT-EU) also signed a Memorandum of Understanding with a view to fostering cooperation and facilitating information exchange between the agencies.[138] In addition private-public cooperation is emphasized, but this overflows to the section dealing with cyber defence and external dimensions of cybersecurity – not without a point, since several global cases have already demonstrated the importance of cooperation between the private and public sectors.[139]

This leads us to the sphere of the EU, where coherence and common action is yet scarce: defence and international relations, the Common Security and Defence Policy. However, the EU has made significant steps in these areas approving the Cyber Diplomacy Toolbox[140], putting forward technology control proposals[141] and concerns for the

137 Proposal for a *Directive of the European Parliament and of the Council* on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHACOM/2017/0489 final – 2017/0226 (COD).

138 General Secretariat of the Council, *EU Coordinated Response to Large-Scale Cybersecurity Incidents and Crises - Council conclusions*, 100086/18, 26 June, 2018, at 3.

139 One of the first global cases include the spread of the Conficker worm, where the counter-action and clean-up initiatives were mainly rooted in the private sector.

140 Council of the European Union, "Cyber Diplomacy Toolbox", 07 July, 2017, 7923/2/17 REV 2. Online at: http://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/en/pdf.

141 European Commission, "Proposal for a *Regulation of the European Parliament and of the Council* setting up a Union regime for the control of exports, transfer, brokering, technical assistance and transit of dual-use items (recast)," COM (2016) 616 final, September 28, 2016. Online at: http://ec.europa.eu/transparency/regdoc/?fuseaction=list&coteId=1&year=2016&number=616&version=ALL&language=en.

origins of foreign direct investments[142]. Cybersecurity is also overlapping with other policy areas, such as countering hybrid threats[143] or development policy[144]. Although the EU has initiated cooperation and is engaged with international actors in discussing cybersecurity, significant legal measures currently adopted in this area are few.[145]

7. Conclusions

This paper has outlined some of the main cybersecurity legal challenges the EU is facing nowadays. Cybersecurity is an issue that will remain in the focus of the Member States and the EU, it will not be solved or go away miraculously. Yet, looking around ourselves, as users, members of organizations, people entrusted with carrying out societal functions, we should notice that we indeed depend on computer systems, which are not perfect and will never be. Yet, this dependency and inherent insecurity can be handled and managed, including by using legal tools, since cyberspace is human-created environment and serves human needs.

We reasoned that EU cybersecurity laws aims to protect not only confidentiality, integrity and availability of data, information systems and networks, but also certain interactions with these by the society. Although it is somewhat unclear what types of harms EU laws aim to prevent, hence it is difficult to assess what interactions should be in

142 European Commission, "Proposal for a *Regulation of the European Parliament and of the Council* establishing a framework for screening of foreign direct investments into the European Union," COM (2017), 487 final, September 13, 2017. Online at: https://ec.europa.eu/transparency/regdoc/rep/1/2017/EN/COM-2017-487-F1-EN-MAIN-PART-1.PDF

143 *Joint Communication to the European Parliament and the Council* Joint Framework on countering hybrid threats a European Union response JOIN/2016/018 final.

144 SWD (2017) 157 final, Commission Staff Working Document, Digital 4 Development: mainstreaming digital technologies and services into EU Development Policy.

145 Rehrl, Jochen, European Security and Defense College, Federal Ministry of Defence of the Republic of Austria, "Handbook on Cyber Security", 2018. Online at: https://publications.europa.eu/en/publication-detail/-/publication/63138617-f133-11e8-9982-01aa75ed71a1/language-en/format-PDF/source-81357173.

focus, we were able to observe that the policy framework developed from a protecting business interests and personal data to a more inclusive one eventually being concerned with harms to economic interests, individuals and national security. The potential harms include direct economic losses, decreased productivity, reputational damage, decreased consumer trust, physical and impalpable harm to citizens, but also economic destabilization, decreased ability to provide order in the society, decreased political autonomy, and losses in sovereignty.

Binding and stringent EU cybersecurity-related laws concern those private infrastructures that are at the core for the operation of cyberspace, in the electronic communications sector, as well as those that support the delivery of essential services for the society. Specific, cross-sectoral regulations regarding personal data protection also contribute to achieve cybersecurity aims in the EU and illegal or harmful content enjoys increasing attention from the EU regulators, generally raising the stakes for actors in the private sector in terms of liability. However, there are certain gaps and while implementation of security measures in the context of personal data processing extends to both private and public sectors, there are no EU level requirements to implement high-level network and information security measures in public administrations and for businesses other than the few listed in the NIS Directive. Social networks, app-stores, and most SME's, unless they are involved with the supply chain for those covered by the NIS Directive, fall outside the scope of the Directive. The EU also applies regulations that are coercive in nature in countering cybercrime as well as for establishing organizational structures in this field.

We can see from the regulatory choices that the EU does not impose strong authentication requirements easy-handedly and opts for alternative solutions, ultimately favouring user anonymity in other fields than payment services. The authors are inclined to attribute this choice to the fact that the functioning of the European society, as such, is less reliant on computerized systems for it basic functions, and it is

rather some individual Member States and certain sectors[146] where deep dependencies exist, which can justify the dominantly soft touch approach from EU level. Although strong authentication in general would presumably contribute to building trust in e-services, by making the case for misuse harder (one can just imagine the impact of strong authentication for the use of social networks, for example), this neither would solve all the problems nor markets seem to be ready for such steps.

Soft and collaborative instruments, voluntary and alternative measures are chosen by the EU for supporting and facilitating cooperation and information exchange among Member States. However, some hard law instruments are used when it comes to information flowing from private sector to public authorities, i.e. incident reporting obligations. These obligations do not extend to "non-incident", such as vulnerability discovery and disclosure, which are targeted by standardization efforts in the EU. Soft measures are applied for EU level coordination of responses in crisis situations, including large-scale cyber-attacks.

In the last few years the EU has made a great deal of progress in switching gears and moving from the reactive policy towards preventive and proactive approach in cybersecurity. In particular the adoption of the NIS Directive reflects this forward-looking nature of EU cybersecurity laws, which now oblige a range of actors to actually implement security measures, and do not leave room for alternative market-driven solutions (such as raising the prices of services/goods to compensate for the risks, or seeking insurance coverage, etc). However, there is little EU level guidance on private sector responses to cyber incidents, and recovery and business continuity aspects. The preventive approach is also visible in EU efforts to channel industry towards the adoption of "security by desig" practices and elaborating the content of "duty of car" principle. Yet, this way of thinking is not clearly identifiable when looking at the public sector and cooperation

146 Such as the financial sector and Critical Infrastructure Protection.

among Member States. EU legal instruments dealing with Member States' own and common effort to address cybersecurity challenges remain dominantly backward-looking, focusing on coordination of crisis response, imposition of criminal penalties, as well as political responses to cyber-attacks.

Although most of the challenges are global, the EU appears to be internally focusing, emphasizing technological solutions. The EU's approach to cybersecurity is centered on technological solutions for a good reason, however more attention should be paid to social and human aspects, as well as to higher level commitment to common standards and joint action, in particular collective preventive action, keeping in mind the potential harms that cybersecurity laws should address.

Das **Zentrum für Europäische Integrationsforschung (ZEI)** ist ein interdisziplinäres Forschungs- und Weiterbildungsinstitut der Universität Bonn. *ZEI – DISCUSSION PAPER* richten sich mit ihren von Wissenschaftlern und politischen Akteuren verfassten Beiträgen an Wissenschaft, Politik und Publizistik. Sie geben die persönliche Meinung der Autoren wieder. Die Beiträge fassen häufig Ergebnisse aus laufenden Forschungsprojekten des ZEI zusammen.

The **Center for European Integration Studies (ZEI)** is an interdisciplinary research and further education institute at the University of Bonn. *ZEI – DISCUSSION PAPER* are intended to stimulate discussion among researchers, practitioners and policy makers on current and emerging issues of European integration and Europe´s global role. They express the personal opinion of the authors. The papers often reflect on-going research projects at ZEI.

Die neuesten ZEI Discussion Paper / Most recent ZEI Discussion Paper:

C 239 (2017) Michael Gehler
Revolutionäre Ereignisse und geoökonomisch-strategische Ergebnisse: Die EU- und NATO-„Osterweiterungen“ 1989-2015 im Vergleich

C 240 (2017) Tapio Raunio/Matti Wiberg
The Impact of the European Union on National Legislation

C 241 (2017) Robert Stüwe
EU External Energy Policy in Natural Gas: A Case of Neofunctionalist Integration?

C 242 (2017) Ludger Kühnhardt
Weltfähig werden. Die Europäische Union nach dem Biedermeier

C 243 (2017) César Castilla
Perspectives on EU-Latin American Cooperation: Enhancing Governance, Human Mobility and Security Policies

C 244 (2017) Joe Borg
The Maltese Presidency of the European Union 2017

C 245 (2018) Ludger Kühnhardt
The New Silk Road: The European Union, China and Lessons Learned

C 246 (2018) Teodora Lađić
The Impact of European Integration on the Westphalian Concept of National Sovereignty

C 247 (2018) Wolfgang Reinhard
Die Expansivität Europas und ihre Folgen

C 248 (2018) Joseph M. Hughes
“Sleeping Beauty” Unleashed: Harmonizing a Consolidated European Security and Defence Union

C 249 (2018) Rahel Hutgens/Stephan Conermann
Macron’s Idea of European Universities. From Vision to Reality

C 250 (2018) Javier González López
Bosnia and Herzegovina: a Case Study for the Unfinished EU Agenda in the Western Balkans

C 251 (2019) Günther H. Oettinger
Europäische Integration aus historischer Erfahrung. Ein Zeitzeugengespräch mit Michael Gehler

C 252 (2019) Chiara Ristuccia
Industry 4.0: SMEs Challenges and Opportunities in the Era of Digitalization

C 253 (2019) Agnes Kasper/Alexander Antonov
Towards Conceptualizing EU Cybersecurity Law

Die vollständige Liste seit 1998 und alle Discussion Paper zum Download finden Sie auf unserer Homepage: http://www.zei.de. For a complete list since 1998 and all Discussion Paper for download, see the center‘s homepage: http://www.zei.de.