Chapter 10
Cybersecurity and the State

Eva Schlehahn

Abstract This chapter provides an overview on state actor's opinions and strategies relating to cybersecurity matters. These are addressed on the EU level as well as on the level of the individual European Member States while the focus is on legislation, policy and political approaches to cybersecurity. In this context, many different measures and approaches are taken both in the Union and nationally to streamline knowledge, resources, and measures to combat cybercrime. Furthermore, the role of the new European data protection framework is addressed, and it is explained why data protection has a close relationship to security matters. The main tensions and conflicts in relation to IT and cybersecurity are depicted, which evolve primarily around the frequently negative effect of IT and cybersecurity measures on the rights of data subjects. However, the issue of governmental surveillance is also addressed, with its implications for the fundamental rights of European citizens. Solution approaches to align the two domains of data protection and cybersecurity are explored, since cybersecurity incidents often involve the loss or compromise of an individual's personal information. To this end, overlaps and synergies are examined that seem promising for a more holistic approach to cyber threats. For instance, this could be achieved by applying principles such as data protection by design and default in IT more thoroughly. In addition, methodologies of data protection impact assessments as well as a more broad deployment of technical and organisational measures while using well-known information security best practices and standards can help to enhance cybersecurity across the European Union.

Keywords European Union · General data protection regulation · State actors · Surveillance

E. Schlehahn (✉)
Unabhängiges Landeszentrum für Datenschutz (Independent Centre for Privacy Protection), Kiel, Schleswig-Holstein, Germany
e-mail: uld67@datenschutzzentrum.de

M. Christen et al. (eds.), *The Ethics of Cybersecurity*, The International Library of Ethics, Law and Technology 21,
https://doi.org/10.1007/978-3-030-29053-5_10

10.1 Introduction

Within the European Union, the EU Member States have a crucial role in maintaining and fostering Cybersecurity by policy regulations and institutional work. It has been widely acknowledged that Cybersecurity needs to be addressed in earnest to mitigate the risks of the increasing digitisation nationally, as well as within Europe and globally. These risks mostly affect European citizens in their everyday lives, but can also affect industries and nation states alike. Notably, the North Atlantic Treaty Organization (NATO) countries published in July 2016 a *Cyber Defense Pledge*, which recognises security threats and reaffirms the support and enhancement of the cyber defenses of their national infrastructures and networks.[1] This chapter provides an overview on the correlating cybersecurity opinions and presents various state actor's strategies to address cybersecurity on EU as well as on the national level within the European Union (see also Chap. 5). In this context, state actors are understood here as official governmental institutions at EU and EU member state levels. Furthermore, solution approaches for cybersecurity issues are examined, which do not aim only to address merely the security perspective but also to integrate the data protection perspective. As for the research methodology for this chapter, only little insight could be drawn from literature and studies. Therefore, our sources consist mostly of legislation, policy documents, official statements and other information directly coming from the above-mentioned state actors.

10.2 Cybersecurity Strategies at the European Union Level

Cybersecurity threats are a global issue, a fact that was recognised by the EU and its individual institutions relatively early. Furthermore, it was accepted that this issue can only be addressed via global responses, necessitating international communication, harmonised legislation and effort coming from both the public and private sectors. Nonetheless, cybersecurity matters have a quite complex nature, making a unified approach sometimes difficult. Working towards resolving this difficulty, the European Commission issued a communication already in 2001 addressing Europe's transition to an information society. This communication referenced a number of already existing approaches and proposed some further action items in order to protect information and communication infrastructures. It called for a comprehensive policy initiative, a unified definition of cybercrime, more in-depth communication with different stakeholders, and more R&D funding to address such threats.

[1] NATO (2016): This pledge entails a general commitment of NATO to allocate adequate resources nationally, foster interaction of stakeholders and improve awareness and understanding of cybersecurity threats overall, including in education and training of NATO and Alliance forces. It is meant to reinforce collaboration and better exchange of best practices across the Alliance, including with the EU.

With the drafting of its *Cyber Security Strategy* in 2013, the EU had detailed its earlier position regarding cooperation and communication related to cybersecurity matters (European Commission, COM 7 Feb 2013). Based on this position, the Commission committed itself to launching a new public-private partnership on cybersecurity with industry to better equip Europe against cyber-attacks and to strengthen the competitiveness of its cybersecurity sector. This occurred as a common platform, called the 'NIS Platform' (platform on network and information security solutions), in order to develop incentives for the adoption of secure ICT solutions and to increase the cybersecurity performance of ICT products used in Europe. This platform was most active in 2013 and 2014, where it involved the European Agency for Network and Information Security (ENISA) as well as various public and private stakeholders. Its purpose was to achieve insight into possible technical guidelines, recommendations, industry standards and general information exchange to enhance cybersecurity.

More concrete legislative action by the European Union followed, such as Directive 2008/114/EC on the identification of European critical infrastructures, or a directive on the security of network and information systems, which got adopted in 2016.[2] While the former is aimed at critical information infrastructure protection, the latter foresees rules, preconditions, and measures meant to ensure a high common level of NIS across the Union. Furthermore, the European Commission encouraged the European member states to make the most of the NIS coordination mechanisms enabled by this legislative act (COM 2016). So far, the NIS Directive has been addressed for national transposition in a multitude of European Member States.[3]

In 2015, the European Commission released its Digital Single Market Strategy, which also reinforced the importance of trust and security in digital services and in the handling of personal data (COM 2015). In the outcome of its mid-term review published May 2017, the Commission identified cybersecurity challenges as one of three main areas where further EU action would be needed.[4] Therefore, the Commission adopted a cybersecurity package in 2017. This package consists of a number of various recommendations and calls for action. An example would be recommendations related to the establishment of stronger and better networked institutions concerned with cybersecurity on EU level as well as on national EU Member States level. Moreover, it entails the endorsement of an EU-wide cybersecurity certification scheme, ideas for optimised incident responses, a call for legislation and frameworks focused on combatting fraud and counterfeiting of non-cash means of payment in order to reduce cyber-crime, as well as joint EU responses to malicious

[2] 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. This is in the following abbreviated as *NIS Directive*.

[3] See for more detail the Directive 2008/114/EC overview page of the EUR-Lex: https://eur-lex.europa.eu/legal-content/EN/NIM/?uri=CELEX:32008L0114

[4] European Commission, press release: '*Digital Single Market: Commission calls for swift adoption of key proposals and maps out challenges ahead*', Brussels, 10 May 2017. The other two areas in need of being addressed are the fostering of the European data economy and promoting online platforms.

cyber activities on diplomatic level. Moreover, the Commission calls for better international cooperation on cybersecurity (including EU and NATO), fostering the development of cybersecurity skills both for civilian and military professionals, and for a set-up of a cyber-defence training and education platform (COM 2017: 2).

Based on these recommendations, the ENISA, founded in 2004, is endorsed as a core European Union Cybersecurity Agency to play a crucial role mainly by providing information and guidance, e.g. on cyber crisis management.[5] In June 2019, the EU Cybersecurity Act came into force which establishes a permanent mandate for the ENISA with increased responsibilities and resources. Moreover, this legislative act reinforces the previously proposed EU-wide cybersecurity certification framework for ICT products and regulates its governance.[6] Alongside the European Commission and ENISA, the Cybercrime Convention Committee (T-CY) of the Council of Europe[7] represents the state parties to the Budapest Convention on Cybercrime. The consultation of the T-CY aims at facilitating the effective use and implementation of the Convention, the exchange of information and the consideration of any future amendments. The T-CY has published a number of different assessments and reports on cybercrime.[8] All these institutions at the European level aim to achieve comprehensive and harmonised governance of cybersecurity-related issues, whereby efforts are undertaken in various areas, such as policy/legislation, finances and operational measures. Yet, those institutions still struggle with divisive factors on the national, pan-European and extra-European/transatlantic level, mostly caused by the diverging willingness of the EU member states to commit resources, the lack of clarity regarding the understanding of cybersecurity and cybercrime, and partially significant disparities in governance strategies and focus. The European Union has acknowledged those difficulties already by beginning several initiatives to address cyber threats. Therein, a strong focus lies on strengthening the resilience of democracy, especially by measures to enhance the security of the electoral infrastructure and campaign information systems. Moreover, guidance on the application of EU data protection law will be pursued further as well as legislative proposals to foster EU Member States coordination on cybersecurity matters (COM 2018: 1). For example, on 12 September 2018, the European Commission made a proposal for a regulation to pool resources and expertise in cybersecurity technology, which involves creating a network of National Coordination Centres for cybersecurity cooperation, research and innovation (COM 2018b).

[5] See e.g. the ENISA overview of recommended publications on that matter: https://www.enisa.europa.eu/topics/cyber-crisis-management?tab=publications

[6] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).

[7] The Council of Europe (CoE) is not an official EU body, but a human rights organisation that was established in 1949 after World War II. It now comprises 47 member states, 28 of which belong to the European Union. See their website here: http://www.coe.int/en/web/about-us/who-we-are

[8] https://www.coe.int/en/web/cybercrime/tcy

10.3 Cybersecurity Strategies at the National Level

At the national level, the EU member states have developed their own cybersecurity strategies, the goals of which correlate with those of the EU strategy, with varying detail and a focus on specific aspects. For example, Luxembourg's cybersecurity strategy foresees a number of important objectives for the country, plus an additional action plan naming in detail the responsible authorities, as well as the anticipated timeframe for realisation. These objectives include strengthening national cooperation (also with the academic and research sphere), increasing the resilience of digital infrastructures, the determination of measures to fight cybercrime, the implementation of norms, standards certificates, labels and frames of references for government and critical infrastructure requirements. Furthermore, this strategy recommends and calls for the information, training, and awareness of cyber risks (Luxembourg 2015: 23ff). In an update in 2018, this was emphasised further, demanding that measures be taken to strengthening public confidence in the digital environment and that digital infrastructures get protected better (Luxembourg 2018: 15ff). Therein, the Luxembourg 2018 strategy is one of the few newer ones in comparison to other EU Member countries.[9]

As an example of a larger country, France's cybersecurity strategy focuses on specific details in some areas, such as increasing the security of state information systems (including the development of cybersecurity requirements for public contracting and support), providing local assistance to victims of cyber-malevolent acts, measuring cybercrime, and protecting the digital lives, privacy and personal data of French citizens. Moreover, France's approach to eliminate and mitigate cybersecurity threats includes operational mechanisms for international administrative assistance and educational measures, the support of security services and products, and knowledge transfer including the education of the general public. However, for the individual objectives mentioned, the French strategy does not provide action items as detailed as the Luxembourg one (France 2015: 15, 21ff, 26f, 31ff).

As already mentioned, it is proving difficult that many countries still have a different understanding of what the terms 'cybersecurity' and 'cybercrime' mean and convey in scope, if they have such a tangible understanding at all. For instance, Spain has a rather strong focus on the country's capability to investigate and prosecute cyber terrorism and cybercrime, yet its cybersecurity strategy does not specify which kind of acts and deeds are exactly considered a cybercrime (Spain 2013: 11, 29). As for Croatia's cybersecurity strategy, it provides a definition of cybercrime, yet this definition is rather broad and vague (Croatia 2015: 16). Thus, there are large differences in the level of detail and commitment made in those national cybersecurity strategies. This issue will probably require some time, additional pan-European communication and a stronger harmonisation effort for remedy.

[9] For direct comparison per country, the ENISA provides an interactive EU map with detail information and links to the individual documents: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map

Most of the EU member states have established institutions dedicated to cybersecurity issues, such as for example the German BSI (Federal Office for Information Security). This institution is tasked with investigating current IT security risks and creates yearly situation reports of the IT security landscape in Germany. It also functions as a cyber-defence centre and reporting office for security incidents. Together with another institution, the BBK (Federal Office of Civil Protection and Disaster Assistance), the BSI provides an Internet platform for the protection of critical infrastructures.[10] The German operators of critical infrastructures in the sectors of energy, information technology and telecommunications, water and nutrition, are required to report security incidents to the BSI and to demonstrate legal compliance every 2 years by providing a detailed protection concept corresponding with the state of the art.[11] Other operators (not active in the aforementioned sectors) can make such reports on a voluntary basis.

Besides institutions like the BSI, many EU countries have national expert groups focusing on security incidents, which are organised in computer emergency response teams (CERTs), sometimes also called computer emergency readiness teams or computer security incident response teams (CSIRTs). They are cross-linked globally and across the EU, offering warnings and problem resolution on security issues, especially involving product security teams from the government, commercial and academic sectors.[12]

However, when it comes to addressing cybersecurity nationally and on institutional level, there are many open questions with regard to coherent policy and strategy decisions (see also Chap. 18). For example, there might be issues of competence area conflicts and institutional mission dichotomies in relation to the German BSI, which pursues both offensive as well as defensive goals. Moreover, other institutions have been established by the German government in 2017 and 2018 that are now tasked with developing offensive as well as defensive cybersecurity strategies and measures. For example, the German government established the 'Zentrale Stelle für Informationstechnik im Sicherheitsbereich (Zitis)' in August 2017, which aims to develop new tools for law enforcement and intelligence (Beuth 2017). Furthermore, in August 2018, it was announced that a new cybersecurity agency will be established that will be concerned with research on cybersecurity and key technologies (Hegemann 2018). Whereas Germany, as only one of many EU countries, serves just as an example here, this illustrates how governments struggle with effectively determining, coordinating and institutionally streamlining potentially overlapping or even conflicting competence areas.

[10] https://www.bsi.bund.de/EN/TheBSI/Functions/functions_node.html

[11] Artikel 8a Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz or BSIG).

[12] See the information website of the global CERT association platform FIRST (Forum of Incident Response and Security Teams): https://www.first.org/about

10.4 The EU Data Protection Framework Addressing Cybersecurity

Already in 2013, the European Data Protection Supervisor (EDPS) Peter Hustinx commented both the *European Cyber Security Strategy* and the NIS Directive in an opinion, highlighting that a high level of Internet security will also improve the security of personal information. Nonetheless, the EDPS highlighted that there is a threat of cybersecurity measures interfering with individuals' rights to privacy and the protection of their personal data. He called for ensuring that every cybersecurity measure deployed complies with article 52(1) of the Charter of Fundamental Rights of the European Union. Thus, all relevant fundamental rights should be considered in the EU's Cybersecurity Strategy, which includes all its implementing actions (EDPS 2013: 4). In 2015, the following EDPS in office, Giovanni Buttarelli, further emphasised this demand in a follow-up opinion on the topic of national security in 2015 (EDPS 2015: 3).

By that time, the EU has also acknowledged that the protection of individual's personal information needs to be improved. This is a major reason why the EU triggered its reform process for its data protection framework, while a new regulation on privacy and electronic communications is still underway. By the time of writing this book chapter, the legislative proposal of the Commission and the amendments suggested by the Parliament and the Council are still within the Trilogue process, without any clear progress forecast.[13]

As for the European data protection reform so far, the 2009 Treaty of Lisbon and the now binding EU Charter of Fundamental Rights[14] enabled the European Commission to trigger a legislative reform process in January 2012. With the intention of harmonising the fragmented legal data protection framework across the European Union (COM 2012), this data protection reform produced two instruments coming into force on 27 April 2016, namely the:

- 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 (General Data Protection Regulation)[15]
- 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[16]

[13] The draft proposal has been made by the European Commission on 10 January 2017. For more information, see: https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation

[14] Charter of Fundamental Rights of the European Union, OJ C 364, 18.12.2000, pp. 1–22.

[15] The General Data Protection Regulation (EU) 2016/679 is the main framework directly applicable in the EU member states. It is in the following abbreviated as *GDPR*.

[16] In contrast to the GDPR, the regulatory instrument for the police and justice sectors comes in form of a directive, which needs to be transferred into correlating national law by the European countries. It is in the following abbreviated as *Directive (EU) 2016/680*.

Both the GDPR, as well as Directive (EU) 2016/680, became applicable by 25 May 2018.

From a data protection perspective, the responsibilities of the data controllers are most relevant in the context of cybersecurity. According to Art. 4 no. 7 GDPR, controllers are those entities determining the purposes and means of the processing. These responsibilities include the legal obligation of controller(s) and processor(s) to effectively implement appropriate technical and organisational measures to protect the personal information they intend to collect and process (GDPR, Art. 24(1) and 28(1); Directive (EU) 2016/680, Art. 19(1) and 22(1)).

The individually necessary technical and organisational measures may vary depending on the case, situation and state of the art in specific areas. Thereby, they can entail preventive as well as reactive security measures such as access control, encryption, data separation, records of processing activities, technical and organisational procedures for backup and restore, or data breach notification procedures, while this list is not conclusive. Typical standards already known in classical IT security, such as ISE/IEC 27001, can also be considered.

Especially noteworthy are Article 32 GDPR and corresponding, Article 29 in Directive (EU) 2016/680, which manifest specified requirements to ensure the security of processing. These also mention exemplary measures, such as e.g. pseudonymisation or measures to ensure the confidentiality, integrity, availability, and resilience of systems and services in the context of personal data processing.

Furthermore, under certain circumstances, the responsible controller has to conduct a data protection impact assessment (DPIA, see Art. 35 GDPR and Art. 27 Directive (EU) 2016/680). Yet it is very important to note that while the risks assessment as known classical in IT security, the data protection perspective is very different. For example, IT security departments of companies are used to assess risks based on which financial or reputation damage for the company could be expected. But in a proper data protection based risk assessment, the perspective of the concerned data subject is paramount. A number of aspects play a role, such as the nature, scope, context and purpose of the processing, the inherent risks of varying likelihood and severity for the rights and freedoms of the concerned data subjects, as well as the state of the art and implementation costs of the needed measures. In cases where the processing is deemed to result in a high risk to the rights and freedoms of natural persons, an additional data protection impact assessment must be conducted (GDPR, Art. 35; Directive (EU) 2016/680, Art. 27).

Based on these assessments, the controller is required to determine the concrete technical and organisational measures needed to sufficiently protect the personal data. Specific examples of technical and organisational measures are also made in both legal frameworks in various places, such as pseudonymisation, encryption, the proper documentation of processing operations, access control and logging.[17] Such

[17] See for those examples in the GDPR: Articles 6 (4) e (Lawfulness of processing), 30 (Records of processing activities), while the Directive (EU) 2016/680 has in parts even more technically specific requirements e.g. for logging, access control and other security measures, cf. Articles 25 (Logging) and 29 (Security of processing).

measures can also be part of a data protection by design and by default approach as also demanded by the respectively applicable legal frameworks (GDPR, Art. 25; Directive (EU) 2016/680, Art. 20).

Beyond the preventive and reactive technical and organisational measures to protect the data, controllers and processors are required to make data breach notifications under certain circumstances and within specific timeframes. According to Article 4 (12) GDPR, *'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed*. Therefore, the GDPR directly refers to security incidents with a negative effect on the protection of personal data, which may also play a role within the cybersecurity domain. According to Article 33 GDPR, a notification of a personal data breach to the supervisory authority is required no later than within 72 h, unless a risk to the rights and freedoms of natural persons is unlikely. However, if there is a high risk (see Art. 34 GDPR), the notification must also be made directly to the data subject without undue delay, unless specific technical and organisational measures are in place to render the personal data unintelligible to any person who is not authorised to access it, such as encryption. Moreover, a notification may be omitted if the controller has taken subsequent measures to ward off this high risk, or if the notification would involve disproportionate effort. However, in the latter case, a public communication or similar measure may be required of the controller nonetheless.

In contrast to the formerly applicable Directive 95/46/EC, non-compliance is now more likely to lead to negative consequences for the controllers, since they are now required to demonstrate compliance with the legal framework.[18] The competent data protection supervisory authorities now have increased enforcement powers due to the new legal framework, which includes a broader range for fine amounts. Therefore, it might be advisable for each data controller to establish an effective data protection management procedure within the own organisation. Moreover, making use of yearly security checks, audits and best practices in technology, such as penetration tests and performance indicators, seems to be reasonable to demonstrate compliance.

10.5 Tensions Between Cybersecurity and Data Protection

Cybersecurity is a matter of concern not only in the context of police and national security, or solely for EU-located state actors. Instead, it is a global issue, motivating private and state actors alike to think about optimal cybersecurity strategies in order to mitigate risks (see e.g. Atlantic Council 2017). Therein, governmental strategies and policies relating to cybersecurity matters strongly concern the European citizens in such a way as cybersecurity incidents often involve the loss, compromise, or unauthorised disclosure of their own personal information.

[18] See e.g. articles 24 (1), 25 (1) + (2), 28 (1) + (3) (e), 30 (1) (g) + (2) (d), 32 (1) GDPR.

With regard to cybersecurity challenges in general, the European Union Agency for Network and Information Security (ENISA) developed a taxonomy classifying different threat types and individual threats at various level of detail. The purpose of this taxonomy is to establish a point of reference in a living structure (ENISA 2016a). According to this document, a number of high-level threat types have been identified, such as physical attacks, unintentional damage/loss of information or IT assets, disaster (natural, environmental), failures/malfunction, outages, eavesdropping/interception/hijacking, nefarious activity/abuse and legal. Many of these threats are closely linked to the cyber domain, for example hacking, Internet of Things (IoT), botnets, ransomware or doxxware (ENISA 2016a, p 8ff).

The World Economic Forum (WEF), a Swiss non-profit foundation committed to bringing business, political, academic and other leaders together for dialogue on global, regional and industry agendas, has also taken a stance on cybersecurity. From their perspective, incidents can cover a very wide spectrum, ranging from e.g. hacking and blackmail encryption to data or identity theft. They can be caused by the most diverse entities for a number of different reasons, and with varying, often unforeseeable impact. Furthermore, the WEF identified in its Global Risk Report 2017 twelve key emerging technologies playing a role in the cybersecurity landscape of the future. These are: 3D printing, advanced materials and nanomaterials, artificial intelligence and robotics, biotechnologies, energy capture, storage and transmission, blockchain and distributed ledger, geoengineering, ubiquitous linked sensors, neuro-technologies, new computing technologies such as quantum computing or neural network processing, space technologies, and virtual and augmented realities (WEF 2017: 42).

An example of a typical cybersecurity incident affecting a broad range of the world population could be the so-called Mirai botnet. This malware was created and distributed in 2016 by students in the US who originally wanted to gain advantages in the online game Minecraft by creating a large-scale distributed denial of service (DDoS) attack. However, the botnet got out of control and infected a large number of IoT devices worldwide, such as IP cameras and home routers. This attack and the distribution of the malware was possible because Mirai exploited the fact that customers and users of IoT devices rarely change the manufacturer's default usernames and passwords on their newly bought machines. Once infected, an IoT device would become part of the botnet, being remotely controlled for large-scale network attacks. In October 2016, the attack got to a point where it almost completely brought down the Internet in the entire eastern United States. The device owners themselves seldom noticed the malware infection because the machine continued to function normally, except for some lagging response time and increased usage of Internet bandwidth.

Therefore, many different technology areas both in the civilian as well as in the governmental spheres are affected by cybersecurity incidents, making appropriate responses crucial in order to succeed in ensuring the availability, integrity and confidentiality of those technologies.[19] This also includes the personal data of

[19] This was explicitly acknowledged by the European Union in COM (2013, p. 3).

individuals which is being collected and processed by digital technologies, and which may be exposed to risks.

While private actors may conduct cyberattacks for monetary or social motives, governmental activities usually extend to wider dimensions, which include Law Enforcement Agency (LEA) cyberspace activities for purposes of crime investigation or prevention, as well as further intelligence activities focused on national security (see also Chap. 12). The targeted entities can also be varied, whereas the attack of critical infrastructure is to be considered the most concerning for all countries worldwide, closely followed by attacks on the governmental structures themselves, e.g. by various types of election fraud (see also Chap. 11).

When focusing on governments specifically as potential cybersecurity attackers, the use of so-called surveillance-oriented security technologies (SOSTs) plays a significant role. Many states, also within the EU, allow to varying degrees and with different preconditions the deployment of such technologies (e.g. Pietrosanti and Aterno 2017), which is often criticised by the media and human rights activists.[20] Media reports about technology used by governments to infiltrate citizen's devices brought into discussion their inherent risks of misuse and bias, usually coming along with a severe lack of transparency.

One example is the governmental deployment of software that infiltrates citizen's devices to gain access to communications and files. In Germany, a Trojan Horse malware (named 'Bundestrojaner', translated: 'Federal Trojan' or 'State Trojan') was discovered by the German Chaos Computer Club (CCC) in 2011 which employed surveillance functionalities on targeted devices. The software was enabled for backdoor remote control and was proved to generally weaken the security of the targeted device. The revelation of the use of this malware triggered a significant public debate around the legality of such technologies in democratic societies (CCC 2011; see also Chap. 15).

Also criticised often by medias and civil rights organisations is the use of so-called zero-day exploit acquisition by governmental institutions to gain leverage in the field of domestic as well as foreign intelligence. Such approaches have received critical attention due to making the whole IT landscape more insecure, while leaving security loopholes open for the obtainment and potential exploitation not only by agencies with lawful national security interests, but also by malicious outsiders.[21]

In this context, also relevant is the general debate around so-called 'lawful access' of police as well as intelligence agencies. Many such institutions have long been demanding access to encrypted devices via backdoor functionalities. Thereby, legal obligations imposed on companies to implement such access might in future affect all types of software and even hardware. Furthermore, the impact of weakened

[20] Cf. Amnesty International (2017). The report heavily criticises the digital surveillance of European governments as negatively affecting the cybersecurity of citizens' devices.

[21] A recent example is the theft of some of the US National Security Agency's most powerful espionage tools by the Shadow Brokers group. These were hoarded by the NSA's TAO (Tailored Access Operations) department, yet outsiders from the mentioned hacking group published them in August 2016, causing significant media reaction. See e.g. Nakashima (2016).

encryption permeates all deployment sectors, including the financial sector, due to the increasing use of cryptocurrencies such as Bitcoin. Similar to zero-day exploits, there is some risk of proliferation beyond the LEA sphere. Furthermore, the legal and factual preconditions for the access to encrypted information are not always clear, requiring clarification. Among security experts, there seems to be a growing recognition of the need to establish mandatory warrants and additional safeguards against misuse (Bellovin et al. 2014). However, even beyond the mere scientific area, encryption has been acknowledged as presenting a number of different challenges for the criminal justice sector.

In November 2016, the Council of the European Union[22] proposed the launch of a reflection process on such challenges, led by the European Commission (Council of the European Union Presidency 2016: 7). Encryption was then further addressed in the Council Meeting on the 8th and 9th December 2016, at which the Ministers acknowledged that this is an area to be approached carefully to take into account the risks to privacy and cybersecurity.[23] Furthermore, the ENISA published an opinion paper on encryption in December 2016, coming to the conclusion that weakening encryption to enable lawful interception is not an optimal approach. The ENISA explicitly warned of unintended consequences, e.g. weakening digital signatures, and recommended some further benefits and risks analysis, as well as a more in-depth exploration of alternatives before any legislative actions should be taken (ENISA 2016a: 5). Similarly, the European Group on Ethics in Science and New Technologies (EGE)[24] published an opinion already in 2014 on security and surveillance technologies, highlighting the dangers of such technologies. It highlighted that whereas foreign state actors may pose a problem, it should not be forgotten that the deployment of intrusive surveillance technologies domestically is risky as well. Therefore, European and democratic principles and values must be considered carefully (EGE 2014: 87ff).

Therefore, specifically in the national security context, it ultimately comes back to the question of boundaries and which goals domestic surveillance should be allowed to pursue, considering the necessity and proportionality of measures (Austin 2015). This however, is not an issue reserved exclusively to the matter of backdoors in encryption but to all governmental activities involving SOSTs. Especially with the increasing use of Big Data analysis tools by LEAs, there is much concern related

[22] The *Council of the European Union* is an official EU body, whose members are the ministers from each EU country, based on the respective policy areas that are addressed. It should not be confused with the *European Council*, which is another EU body consisting of the 28 EU member state government leaders, the European Council President and the President of the European Commission. The European Council defines the EU's strategic short- and long-term policy agenda. For the sake of completeness, confusion should also be avoided with the *Council of Europe (CoE)* that was mentioned above in this chapter.

[23] Outcome of the 3508th Council meeting, document 15391/16 and press release 67 by the Justice and Home Affairs department, section '*Criminal justice in Cyberspace*', Brussels, 8th and 9th December 2016, p. 7.

[24] The European Group on Ethics in Science and New Technologies is an independent advisory body of the President of the European Commission.

Fig. 10.1 Simplified overview of cybersecurity issues

to citizens having only limited possibilities to defend themselves against any mistreatment or security risks based on algorithmic-founded suspicion. The same counts not only for LEA activity in the context of specific crime prevention or investigation, but also for intelligence in the interest of national security.

Naturally, all intelligence institutions aim to use IT vulnerabilities to target individuals and organisations endangering national security. However, depending on their competences and objectives, these institutions may sometimes have several, contradicting goals. For instance, it appears doubtful whether both SIGINT[25] and COMSEC[26] missions can be pursued by the very same institutions without triggering unexpected internal dichotomies regarding cybersecurity issues.

In conclusion, discrepancies between offensive and defensive strategies are particularly striking with regard to any legislative acts requiring technology to generally undermine the privacy and security of citizen's computers and communications. This is evident when observing the on-going political and public debate around governments collecting personal information of their citizens (see also Fig. 10.1). Examples are the EU-level and national controversies around data retention, counter-terrorism legislation, and the expansion of intelligence services' competences and cooperation. Combating crime and terrorism definitely plays a role in the political and legislative landscape of the European member countries and will continue to do so.

10.6 Recommended Realignment and Solution Approaches

It is increasingly acknowledged that the cybersecurity issues landscape can change very fast, leaving policy-makers, data protection and cybersecurity experts at a strategical and operational disadvantage. The increase of interconnectedness in the digital era also means an increase of involved actors and recipients of data, with ever greater networks of entities and stakeholders involved. More data also leads to more

[25] Signals Intelligence, for example getting access to the content of people's emails.

[26] Communications Security, with the ultimate goal of protecting communications, e.g. of government officials.

possibilities of analysis with big data tools, thus scaling up risks of re-identification of individuals, profiling and disrupted power balances. Furthermore, there is a growing recognition that cybersecurity risks do not only come from the outside, but malicious insiders may cause significant damage as well.[27] Within the cybersecurity domain, the effectiveness of offensive measures taken mostly by governmental actors is often questioned. This is due to doubtful allocation of cybersecurity attacks and related insecurities regarding accurate forensic evidence to target the true attackers for retaliation purposes.[28] Therefore, some cybersecurity experts advise focusing more on defensive strategies in order to protect valuable assets. This is where the above-mentioned implementation of technical and organisational measures required by new European data protection framework may contribute to better protected devices and systems.

The responsibilities of the controller and processor entities as well as principles such as data protection by design and default (GDPR, Art. 25; Directive 2016/680, Art. 20) are focused strongly on either eliminating or at least mitigating any risks for the personal information of individuals, regardless of the type of attack. This is a considerable approach because even though the cybersecurity domain provides much collaboration and information on the national level of the EU member countries, it still lacks a clear, organised mandate to enforce the implementation of protective measures on the European level.

Against this background, the national DPAs publish their own statements and opinions on cybersecurity issues to bring in their perspective. In 2015, the French national data protection authority Commission Nationale de l'Informatique et des Libertés (CNIL) published an analysis of personal data protection in the context of cybersecurity. It found that privacy is a crucial aspect in the digital era and that a more holistic approach to both cybersecurity and privacy is sorely needed, while baseline security rules have not yet been sufficiently established (CNIL 2015: 14ff; see also Chap. 14). In July 2017, the CNIL published its stance on encryption, stating that the protection of the confidentiality of communications is essential to maintain the balance between the protection of an individual's personal data, technological innovation and monitoring. Especially with regard to the Edward Snowden NSA mass surveillance revelations, robust encryption solutions would contribute to the security of the whole digital ecosystem, whereas backdoors would endanger citizens, organisations and states alike (CNIL 2017). In 2018, the CNIL published a guideline related to the security of personal data, giving recommendations related to specific technical and organisational measures that controllers and processors may take (CNIL 2018). In Italy, the Italian DPA strives for better cooperation with other Italian governmental institutions concerned with cybersecurity.[29] The Information

[27] See ENISA Threat Landscape Report (2018a), subchapter 3.9 about insider threats, pages 64ff.

[28] This was explicitly acknowledged by many cybersecurity experts, also abroad, see as an example the cybersecurity policy/approach of the US Obama administration (Marks 2017).

[29] See the following article on askanews.it: '*Cyber security, protocollo Garante-Dis su dati personali*', 6 October 2017, http://www.askanews.it/cronaca/2017/10/06/cyber-security-protocollo-garante-dis-su-dati-personali-pn_20171006_00134/

Commissioner of the United Kingdom (ICO UK) also focuses on information security, detailing on his website the relevant technical and organisational measures required by the national and EU data protection frameworks.[30] Moreover, the ICO UK regularly publishes current data security incident trends, covering various issues relating to information security in the cyber domain. Therein, the ICO differentiates per sector, such as justice, education, finance, insurance and credit, general business, local government, legal, and health sector. Examples of issues mentioned are cryptographic flaws (e.g. failure to use HTTPS), exfiltration of data, key-logging software, phishing, cybersecurity misconfiguration (e.g. inadvertent publishing of data on website), loss/theft of an only copy of encrypted data or the loss/theft of an unencrypted device, diverse DDoS and others.[31]

Many institutions within the EU, at both national and European levels, recommend taking initial steps for IT systems and networks with the definition of processes, the close monitoring of their execution, supplemented by preventive and reactive measures compliant with the state of the art.[32] This includes the consideration of information security best practices and standards, such as ISO, COBIT or ITIL. From a data protection perspective, the above-mentioned technical and organisational measures often correlate and their implementation should be much more prevalent in many areas and sectors.

Essential from data protection perspective is the conduct of a data protection impact assessment (DPIA) in advance of certain intended personal data processing operations. The GDPR regulates in Article 35 (1) that a DPIA is required when "*a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a* ***high risk to the rights and freedoms of natural persons*** *[…]*". Many national DPAs in the EU have developed own DPIA methodologies.[33] However, some of these methodologies have their own shortcomings and weaknesses. For example, some fail to properly determine what a risk actually is, or reduce the assessment to a mere risk-based IT security approach which lacks the fundamental rights perspective required by the EU data protection laws. An example of a methodology integrating this perspective is the German Standard Data Protection Model (SDM), which has a strong fundamental rights underpinning and which has been acknowledged by all national

[30] See the ICO website information: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/security/

[31] These examples come from the reports of the July–September 2016 period (https://ico.org.uk/action-weve-taken/data-security-incident-trends/) and of the Q4 2017/18 (https://ico.org.uk/action-weve-taken/data-security-incident-trends/).

[32] This is also reflected in the private sector as well, reacting to the governmental encouragement. See for example the recommendations of the industry-sector-driven ECSO (2016, chapter 6).

[33] See e.g. the ICO UK guidelines on their website: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/ or the methodology explanations by the French CNIL: https://www.cnil.fr/en/privacy-impact-assessment-pia

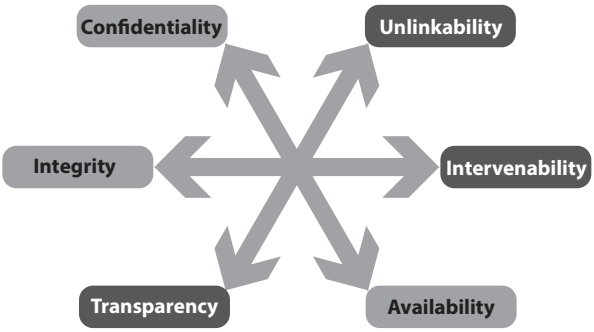

Fig. 10.2 Data protection goals (darker grey) integrating the IT security goals (lighter grey) that require balancing. The classical IT security goals are described from an individual data subject perspective; unlinkability includes data minimisation

data protection supervisory authorities in Germany.[34] It is based on protection goals that build and extend upon classic IT security goals[35] (see also Chap. 2), but can still be linked directly to the applicable data protection framework.[36] The underlying concept was developed much earlier than the GDPR (Hansen et al. 2015) yet it still provides a methodology that is based on the GDPR directly and thus is useable all across the EU. Briefly summarised, three additional data protection goals supplement the IT security focused ones, namely: *unlinkability* (data minimisation), *intervenability* and *transparency* (see also Fig. 10.2).

These additional, privacy-focused goals can be used together with the classic IT security goals to assess and evaluate data protection and data security objectives and risks. The objective is to map the (often rather vague and broad) legal requirements of the European data protection framework to more concrete functional and organisational requirements. Therefore, the above mentioned SDM approach for a DPIA seems to be a candidate methodology to broaden the view of IT security and to be aligned with the perspective of personal data protection.

Howsoever, regardless of which DPIA methodology is being used, it must always be aimed at determining the necessary operational measures to resolve data protection issues (GDPR, Art. 35(7)). Furthermore, it requires the responsible entity to consider the whole processing lifecycle, including all data, formats, IT systems, processes and functions.

While addressing both security and data protection, it appears reasonable not to invent the wheel anew but to refer to known standards and instruments such as ISO/IEC 27001 and/or code of conducts, as well as to process-oriented approaches (plan, do check, act). Since technological and security challenges are continuously evolving,

[34] See Germany (2016) – Unanimously and affirmatively acknowledged (under abstention of Bavaria) by the 92. Conference of the Independent Data Protection Authorities of the Bund and the Länder in Kühlungsborn on 9–10 November 2016. See for a very first English version: https://www.datenschutzzentrum.de/sdm/. A second and improved English version is currently in the works.

[35] The classic '*CIA triad*' (abbreviation for the protection goals confidentiality, integrity, and availability).

[36] Germany (2016), see the pages 23 ff. for the direct linkage of the individual protection goals to the requirements of the GDPR.

it is advisable to earnestly assess the whole lifecycle of IT product manufacturing processes. Such processes usually range from design, development, testing, procurement, operation, management, and to the product phase-out and deployment. All of these stages need to be subjected to security risk assessments and countermeasures deployment (ENISA 2018a: 21). To this end, an effective assignment of clear responsibilities, time periods, as well as a prioritisation of measures implementation should be the primary goal. To plan, implement and evaluate processes, procedures and measures in an optimal way, a data protection management system should always make clear cross-references to an eventually already existing IT security management system (ISMS) to avoid divergences, conflicts, contradictions and unnecessary overlaps.

Moreover, a close observation of the still active legislative process for the future ePrivacy Regulation is advisable since it will be relevant for the area of electronic communications. The original European Commission draft[37] has been criticised significantly by relevant stakeholders in the data protection domain, such as the Article 29 Working Party[38] and the European Data Protection Supervisor (EDPS 2017). What might matter most in the context of cybersecurity and more general IT security issues is that the draft has been found faulty for vagueness in the scope definition. Also, for having weakened requirements in relation to information about security risks and data breaches, as well as regarding privacy by design and by default in comparison to the GDPR. Thus, it provides a lack of consistency.[39]

Acknowledgments The chapter was created in the context of the research project CANVAS (Constructing an Alliance for Value-driven Cybersecrutiy), with funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 700540. This work was co-supported (in part) by the Swiss State Secretariat for Education, Research and Innovation (SERI) under contract number 16.0052-1.

References

Amnesty International (17 Jan 2017) Dangerously disproportionate: the ever-expanding national security state in Europe. https://www.amnesty.org/en/documents/eur01/5342/2017/en/. Last access 7 July 2019

Article 29 Working Party (2017) Opinion 01/2017 on the proposed regulation for the ePrivacy Regulation (2002/58/EC). Adopted on 4 April 2017 (WP247). http://ec.europa.eu/newsroom/document.cfm?doc_id=44103. Last access 7 July 2019

[37] European Commission: '*Proposal for a Regulation on Privacy and Electronic Communications*', https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications

[38] The Article 29 Working Party, set up on account of Article 29 EU Data Protection Directive 95/46/EC, was an independent advisory group counselling the European Commission in data protection and privacy issues. Since 25 May 2018, the European Data Protection Board is its successor entity.

[39] See the Article 29 Working Party: '*Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC)*', adopted on 4 April 2017, WP247, pages 3 and 24. Furthermore, see the '*Opinion 6/2017 EDPS Opinion on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation)*', April 24th 2017, pages 3, 12 ff., 19, 22 f., and 34 f.

Austin LM (2015) Surveillance and the rule of law. Surveill Soc J 13(2). http://ojs.library.queensu.ca/index.php/surveillance-and-society/article/viewFile/law_rule/law_rul. Last access 7 July 2019

Bellovin SM, Blaze M, Clark S et al (2014) Lawful hacking: using existing vulnerabilities for wiretapping on the internet. Northwest J Technol Intellect Prop 12:1. http://scholarlycommons.law.northwestern.edu/njtip/vol12/iss1/1. Last access 7 July 2019

Beuth P (30 Aug 2017) Bundeshacker im Verzug. Zeit Online. https://www.zeit.de/digital/datenschutz/2017-08/zitis-eroeffnung-thomas-de-maiziere-bundeshacker. Last access 7 July 2019

CCC (2011) Chaos computer club: 'Chaos Computer Club analyzes government malware'. 8 October 2011. Available at: https://www.ccc.de/en/updates/2011/staatstrojaner. Last access 7 July 2019

Charter of Fundamental Rights of the European Union (2000) OJ C 364, 18 December 2000. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32000X1218 (01), pp 1–22

CNIL (2015) Commission Nationale de l'Informatique et des Libertés: 36th activity report 2015. https://www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_2015_gb.pdf. Last access 7 July 2019

CNIL (18 July 2017) Commission Nationale de l'Informatique et des Libertés: Encryption: security element of information assets. https://www.cnil.fr/en/what-cnils-position-terms-encryption. Last access 7 July 2019

CNIL (4 Apr 2018) Commission Nationale de l'Informatique et des Libertés: Security of personal data. https://www.cnil.fr/sites/default/files/atoms/files/cnil_guide_securite_personnelle_gb_web.pdf. Last access 7 July 2019

COM (26 Jan 2001) European Commission: Creating a safer information society by improving the security of information infrastructures and combating computer-related crime. Communication COM/2000/890 final, Brussels. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52000DC0890. Last access 7 July 2019

COM (2012) Safeguarding privacy in a connected world – a European data protection framework for the 21st century

COM (7 Feb 2013) European Commission*:* Cyber security strategy of the European Union: an open, safe and secure cyberspace. Joint communication JOIN/2013/1 final, Brussels. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52013JC0001. Last access 7 July 2019

COM (2015) European Commission: A digital single market strategy for Europe. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. COM/2015/192 final. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2015:192:FIN. Last access 7 July 2019

COM (5 July 2016) European Commission: Strengthening Europe's cyber resilience system and fostering a competitive and innovative cybersecurity industry. Communication COM/2016/410 final, Brussels, 5 July 2016. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016DC0410. Last access 7 July 2019

COM (2017) European Commission: Resilience, deterrence and defense: building strong cybersecurity in Europe. Fact sheet on the cybersecurity package. 19 September 2017. https://ec.europa.eu/digital-single-market/en/news/resilience-deterrence-and-defense-building-strong-cybersecurity-europe. Last access 7 July 2019

COM (2018a) European Commission: Communication from the commission to the European Parliament, the European Council and the Council – sixteenth progress report towards an effective and genuine security union. Brussels, 10 October 2018. COM (2018) 690 final. https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20181010_com-2018-690-communication_en.pdf. Last access 7 July 2019

COM (2018b) European Commission: 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. Brussels, 12 November 2018. COM(2018) 630 final. 2018/0328 (COD). https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-cybersecurity-centres-regulation-630_en.pdf. Last access 7 July 2019

Consolidated Version of the Treaty on the Functioning of the European Union (2012) OJ C 326, 26 October 2012, pp 47–390. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012E%2FTXT. Last access 7 July 2019

Council Decision 2009/371/JHA of 6 April 2009 establishing the European Police Office (EUROPOL) (2009) OJ L121/37, 15 May 2009, pp 37–66. http://eur-lex.europa.eu/eli/dec/2009/371/oj. Last access 7 July 2019

Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. OJ L 345, 23 December 2008, pp 75–82. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32008L0114. Last access 7 July 2019

Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union (2006) OJ L 386/89, 29 December 2006, pp 89–100. http://eur-lex.europa.eu/eli/dec_framw/2006/960/oj. Last access 7 July 2019

Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (2008) OJ L 350, 30.12.2008, pp 60–71. http://eur-lex.europa.eu/eli/dec_framw/2008/977/oj. Last access 7 July 2019

Council of the European Union – Justice and Home Affairs department (2016) Outcome of the 3508th Council meeting, Document 15391/16, section 'Criminal justice in Cyberspace and Press release 67, Brussels, 8 and 9 December 2016. http://data.consilium.europa.eu/doc/document/ST-15391-2016-INIT/en/pdf. Last access 7 July 2019

Council of the European Union Presidency (2016) Encryption: challenges for criminal justice in relation to the use of encryption – future steps – progress report. Note 14711/16 to the Permanent Representatives Committee/Council, Brussels, 23 November 2016. http://data.consilium.europa.eu/doc/document/ST-14711-2016-INIT/en/pdf. Last access 7 July 2019

Croatia (2015) The national cyber security strategy of the Republic of Croatia. Official Gazette No. 108/2015, Zagreb, 7 October 2015. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CRNCSSEN.pdf. Last access 7 July 2019

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (2002) OJ L 201, 31 July 2002, p 37. http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:32002L0058. Last access 7 July 2019

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. OJ L 119, 4 May 2016, pp 89–131. http://eur-lex.europa.eu/eli/dir/2016/680/oj. Last access 7 July 2019

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. (2016) OJ L 194/1 (NIS Directive). http://data.europa.eu/eli/dir/2016/1148/oj. Last access 7 July 2019

ECSO (June 2016) European Cyber Security Organisation: European Cybersecurity Strategic Research and Innovation Agenda (SRIA) for a contractual public-private-partnership (cPPP). http://www.ecs-org.eu/documents/ecs-cppp-sria.pdf. Last access 7 July 2019

EDPS (14 June 2013) European Data Protection Supervisor (Peter Hustinx): Opinion on the Joint Communication of the Commission and of the High Representative of the European Union for Foreign Affairs and Security Policy on a "Cyber security strategy of the European Union: an open, safe and secure cyberspace", and on the Commission proposal for a Directive concerning measures to ensure a high common level of network and information security across the Union. Brussels. https://edps.europa.eu/sites/edp/files/publication/13-06-14_cyber_security_en.pdf. Last access 7 July 2019

EDPS (15 Dec 2015) European Data Protection Supervisor (Giovanni Buttarelli): Opinion 8/2015 on dissemination and use of intrusive surveillance technologies. Brussels. https://edps.europa.eu/sites/edp/files/publication/15-12-15_intrusive_surveillance_en.pdf. Last access 7 July 2019

EDPS (24 Apr 2017) European Data Protection Supervisor: Opinion 6/2017 EDPS opinion on the proposal for a regulation on privacy and electronic communications (ePrivacy Regulation). https://edps.europa.eu/sites/edp/files/publication/17-04-24_eprivacy_en.pdf. Last access 7 July 2019

EGE (2014) European Group on Ethics in Science and New Technologies: Ethics of security and surveillance technologies. Opinion No. 28, Brussels, 20 May 2014. Available at: https://bookshop.europa.eu/en/ethics-of-security-and-surveillance-technologies-pbNJAJ14028/. Last access 7 July 2019

ENISA (Dec 2016a) European Union Agency for Network and Information Security: ENISA's opinion paper on encryption – strong encryption safeguards our digital identity. https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisas-opinion-paper-on-encryption. Last access 7 July 2019

ENISA (Jan 2016b) European Union Agency for Network and Information Security: ENISA threat taxonomy – a tool for structuring threat information. Initial Version 1.0. https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/etl2015/enisa-threat-taxonomy-a-tool-for-structuring-threat-information. Last access 7 July 2019

ENISA (Jan 2018a) European Union Agency for Network and Information Security: ENISA threat landscape report 2017. Final Version 1.0. https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017. Last access 7 July 2019

ENISA (31 Jan 2018b) European Union Agency for Network and Information Security: Looking into the crystal ball – a report on emerging technologies and security challenges. Version 1.0. https://www.enisa.europa.eu/publications/looking-into-the-crystal-ball. Last access 7 July 2019

France (2015) République française. French National Digital Security Strategy. https://www.ssi.gouv.fr/en/actualite/the-french-national-digital-security-strategy-meeting-the-security-challenges-of-the-digital-world/. Last access 7 July 2019

Germany (2016) The standard data protection model – a concept for inspection and consultation on the basis of unified protection goals. German Data Protection Authorities, Kühlungsborn, 9–10 November 2016. https://www.bfdi.bund.de/DE/Datenschutz/Themen/Technische_Anwendungen/TechnischeAnwendungenArtikel/Standard-Datenschutzmodell.html. Last access 7 July 2019

Hansen M, Jensen M, Rost M (2015) Protection goals for privacy engineering. Security and privacy workshops (SPW), IEEE, 2015, pp 159–166. https://doi.org/10.1109/SPW.2015.13. Last access 7 July 2019

Hegemann L (29 Aug 2018) Deutschland bekommt eine Agentur für innere Netzsicherheit. Zeit Online. https://www.zeit.de/digital/internet/2018-08/cybersicherheit-bundesregierung-innovation-cyberagentur-netzpolitik. Last access 7 July 2019

High Representative of the European Union for Foreign Affairs and Security Policy (2013) Cybersecurity strategy of the European Union – an open, safe and secure cyberspace. Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Brussels 7 February 2013. JOIN (2013) 1 final. http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf. Last access 7 July 2019

Luxembourg (27 Mar 2015) Gouvernement du Grand-Duché de Luxembourg. National Cybersecurity Strategy II. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Luxembourg_Cyber_Security_strategy.pdf. Last access 7 July 2019

Luxembourg (26 Jan 2018) Gouvernement du Grand-Duché de Luxembourg. National Cybersecurity Strategy III. https://hcpn.gouvernement.lu/dam-assets/fr/publications/brochure-livre/national-cybersecurity-strategy-3/national-cybersecurity-strategy-iii-en-.pdf. Last access 7 July 2019

Marks J (17 Jan 2017) Obama's cyber legacy: he did (almost) everything right and it still turned out wrong. nextgov.com. http://www.nextgov.com/cybersecurity/2017/01/obamas-cyber-legacy-he-did-almost-everything-right-and-it-still-turned-out-wrong/134612/. Last access 7 July 2019

Nakashima E (16 Aug 2016) Powerful NSA hacking tools have been revealed online. https://www.washingtonpost.com/world/national-security/powerful-nsa-hacking-tools-have-been-revealed-online/2016/08/16/bce4f974-63c7-11e6-96c0-37533479f3f5_story.html?utm_term=.61735c899442. Last access 7 July 2019

NATO (8 July 2016) North Atlantic Treaty Organization. Cyber defense pledge. Press release (2016) 124. http://www.nato.int/cps/en/natohq/official_texts_133177.htm. Last access 7 July 2019

Pietrosanti F, Aterno S (15 Feb 2017) Italy unveils a legal proposal to regulate government hacking. https://boingboing.net/2017/02/15/title-italy-unveils-a-law-pro.html. Last access 7 July 2019

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 (General Data Protection Regulation) (2016) OJ L 119/1. http://data.europa.eu/eli/dir/2016/1148/oj. Last access 7 July 2019

Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing regulation (EU) No 526/2013 (Cybersecurity Act) (2019) OJ L 151/15. https://eur-lex.europa.eu/eli/reg/2019/881/oj. Last access 7 July 2019

Spain (3 Jan 2013) Gobierno de España. National cyber security strategy. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS_ESen.pdf

The Atlantic Council of the United States (2017) A nonstate strategy for saving cyberspace, Atlantic Council Strategy Paper No. 8, January

The H Security blog (11 Sept 2012) Federal Commissioner unable to audit Federal Trojan source. http://www.h-online.com/security/news/item/Federal-Commissioner-unable-to-audit-Federal-Trojan-source-1704460.html. Last access 7 July 2019

Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community. Signed at Lisbon, 13 December 2007. OJ C 306, 17 December 2007, pp 1–271. Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12007L%2FTXT. Last access 7 July 2019

WEF (2017) World economic forum: global risks report 2017, 12th edn, published within the framework of The Global Competitiveness and Risks Team