Chapter Nine

EU Cybersecurity Governance – Stakeholders and Normative Intentions towards Integration

Agnes Kasper

Abstract

In the last decade, the EU's policy on cybersecurity has changed significantly, both as to its referent objects and priority level. While the 2013 Cybersecurity Strategy focused almost exclusively on the importance of cybersecurity for the proper functioning of the single market, its 2017 version also contained an analysis of malicious cyber activities that threaten the political integrity of Member States and the EU as a whole. As the field's level of complexity grows and forward-looking initiatives are constantly being proposed in order to promote cyber resilience across the EU, it is increasingly challenging the Union in the process of coordinating and implementing the planned actions.

Cybersecurity has also become a national security issue entangling private and public, external and internal, civilian, and military issues making it necessary, but very challenging to widen and deepen ties among stakeholders in the EU. Yet cybersecurity governance is fragmented at the EU level, and there is an evident lack of trust that prevents effective cooperation among stakeholders on crucial aspects of the process. This contribution argues that as a result, cybersecurity policy in the EU remains unsystematic and predominantly reactive in nature, addressing the issue-specific incidents that have already occurred, although in our technology-dependent societies more emphasis should be placed on prevention. Therefore, in a natural scholarly quest for explanations, this chapter focuses on the development and main elements of the EU's cybersecurity policy, followed by mapping the attitudes of cybersecurity stakeholders and their normative objectives in the context of EU integration in this domain.

Introduction

The EU, a technological powerhouse, is of colossal significance for the world's economy, although it is still debating its relevance as such in terms of cybersecurity and struggles with its dependence on external technology providers. The recent

debate and controversies concerning Huawei's influential presence for the supply of 5G technology for next generation wireless networks has brought about the issue of cyber-geopolitics, and the entanglement of civilian and military domains has started to feature more prominently on the political horizon (Kaska, Beckvard and Minarik, 2019). Choices concerning fundamental digital infrastructure that the European information society is dependent on have critical implications and are strategic questions at both national and European level. However, the EU has been rather the subject and recipient of global powers' national policies of technological superiority.

Certainly, when the issues of geo-strategy are left aside for others to deal with, the EU's positive competence (in all possible senses of the word) in operationalizing both trade and technology is undisputed in terms of volume. Therefore, it was not surprising when the EU's 2013 Cybersecurity Strategy (European Commission, 2013), adopted at an unpredictable time of recondite change, was emphasizing the special significance of cybersecurity for what the EU became globally respected for – the single market and its proper functioning. Four years later, the Strategy's revision (European Commission, 2017) effectively made a step further to clearly outline the EU's understanding that a range of malicious activities in cyberspace represents a threat to its political integrity. At the same time, the EU, while leading the world in a high number of economic indicators, has not come closer to establishing a common-for-all-Member-States method of governance on cybersecurity. In this EU-wide debate, cybersecurity is still loosely defined (for a lawyer, it is still undefined), and is the EU not able to establish a governance mechanism that would shield the domain from the underlying factors to the highest levels of responses, and to cyberattacks.

This underlines the argument that the EU's cybersecurity policy remains predominantly reactive (be it normatively or operationally), having no particular system-driven approach and generating plenty of post-factum activities, while selectively providing for prevention. It does so by dividing cybersecurity into three conventional areas – not very consistently – and still separates cybersecurity, cyber resilience and cyber defence issues, leaving significant gaps where the preventive mindset does not apply. Christou (2019, p. 281) notes that the EU cybersecurity policy is "fragmented and differentiated temporally across three areas – cybercrime, network and information security, and cyber-defence". Dunn Cavelty (2012) describes three interlocking cybersecurity discourses namely the technical, cybercrime/cyberespionage, and military/civil defence, all with different main actors and referent objects. All of these are touched upon in the EU's cybersecurity strategies, however the proper linkages between these domains still have to be mapped in detail. While entanglement of private and public, external and internal, civilian and military issues in the cyber domain makes a good case for further integration in many relevant policy areas, the same entanglements pose significant challenges to widen and deepen ties among stakeholders in the EU. In the EU's case, as already noted, though technology is an issue, and there is a gap with the major powers, here we question the willingness and readiness to address key issues of cybersecurity at

policy level and from the perspectives of stakeholders – which according to different integration theories may be considered as key actors driving the process.

In view of the above, the idea behind our observations is firstly, to outline the main building blocks of the EU's cybersecurity policy, focusing on its roots, as they likely define the EU's attitude and approach to cybersecurity. The next step is to understand who is involved in the process, the stakeholders. This approach lays the groundwork for further systematic enquiries on integration theories and EU cybersecurity policies. This chapter thus contributes to existing knowledge by outlining the emergence of an EU wide cyber security architecture and policy, and provides a useful analysis of the main institutional arrangements and structures.

Cybersecurity Policy of the EU: Basic Notions and Current Understandings

Defining the notion of cybersecurity

When discussing cybersecurity policy, one should be conscious of the terminology that is used by various actors and at many levels. A range of technical notions that are established by the industry have infiltrated policy and legal discourses related to technological advances, however it appears to be a challenge to establish a consistent vocabulary specifically related to cybersecurity. Data or information security, network security and cybersecurity are related concepts, yet they appear to differ in their scope. 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 being "concerned with the design, implementation and operation of networks for achieving the purposes of information security on networks within organisations, between organisations, and between organisations and users". However, when addressing national, EU-level or international policy issues at large, one may encounter inconsistencies giving rise to confusion about the scope and purposes of a policy in question. The issue of 'information security' has been on the UN agenda since 1998[25], but the EU would refer to this discussion as related to 'cybersecurity'. Naturally, 'cybersecurity' may not be used by other major international actors, such as Russia or China, in the same way as in the EU, and hence the terminological content of this notion depends on the context.

The EU has been struggling to find a commonly agreed working definition of cybersecurity, one that "enables identifying the common goals across the EU" (ENISA, 2012). While in the 1951 Treaty of Paris, European states were clearly able to identify the potential harms to be prevented (bloody conflicts), in the current context

25 See more in 'The Role of Science and Technology in the context of International Security and Disarmament'. *The United Nations Office for Disarmament Affairs*. Available at: https://www.un.org/disarmament/topics/informationsecurity/

of interdependent cyber societies, cybersecurity remains a field where differing levels of dependencies on information and communication technologies determine different perceptions and priorities for actors. To exemplify the different approaches, the 2013 Austrian Cybersecurity Strategy describes cybersecurity as a process; the 2011 German strategy refers to it as "the desired objective of IT security situation"; the 2013 Spanish strategy states that "cybersecurity is a necessity of our society and our economic model"; the 2017 Swedish strategy refers to a "set of security measures to preserve the confidentiality, authenticity and availability of information"; while the recent Estonian cybersecurity strategy uses three Estonian language-specific definitions that all translate to English as 'cybersecurity'. This leaves us with contextual definitions; contributing little to the clarity on what harms the EU, and what policies aim at preventing this from happening. At the same time, the working definition used in the 2013 EU Cybersecurity Strategy notes 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. Cyber-security strives to preserve the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein."

However, the recently adopted Cybersecurity Act (Regulation (EU) 2019/881) defines cybersecurity for the purposes of the act as "all activities necessary to protect network and information systems, their users, and affected persons from cyber threats" (Article 2), which signifies a departure from the previous working definition in the EU strategy, because it includes in its scope the protection of persons, and not only cyberspace in itself.

Emergence of EU cybersecurity policy

Since data and information security certainly form part of cybersecurity, one can trace back the EU's policy on cybersecurity to the Bangemann Report addressing the topic of Europe and the global information society (High Level Group on Information Society, 1994), and the EU's precarious personal data protection policy from the mid-1990s. The Bangemann Report predicted the game-changing nature of digital technologies, argued for the liberalization of the telecommunication sector, and mentioned the repercussions of misuses. Article 17 of the Personal Data Protection Directive (Directive 95/46/EC) imposed an obligation – through national implementing measures – on regulators to implement appropriate technical and organisational measures to protect personal data. In searching for justification of the measure, one encounters in the preamble of the Directive the need for the establishment and functioning of the internal market.

Entering the new millennium, the EU's legislative activity intensified addressing security issues in the telecommunications field, the Telecom market was liberalized by the regulatory framework adopted in 2002, and following the developments in the Council of Europe (2001) the Budapest Convention on Cybercrime was adopted. The early EU policies in the field, which we can now treat as cybersecurity, had three main considerations: protection of privacy, cybercrime and harmonisation in specific, electronic data-related fields (Commission Communication, 2001). The latter included telecom market policies, exemption from liabilities of service providers (e-commerce directive), and e-signatures.

Parallel to these EU processes, the concern for national security implications of information and communication technologies arose, prompting the U.S. to include cybersecurity aspects in its national security strategy in the aftermaths of the 9/11 attacks and, in Europe, the adoption of the Data Retention Directive (2006/24/EC) as a response to the 2004 Atocha bombing in Madrid. Yet, it still took a few years for the EU to take the issue of cybersecurity to the highest level of its agenda. The 2007 cyberattacks against Estonia captured the attention of most of the EU Member States (Haataja, 2017), and cybersecurity as such was for the first time expressly addressed in the High Representative for the CFSP, Javier Solana's 2008 report (Council, 2008). A process was ignited in the EU that resulted in the adoption of the first comprehensive EU Cybersecurity Strategy in 2013, and, with the intensifying diffusion of information and communication technologies, it further culminated in the second, revised cybersecurity strategy in 2017 aiming at integrating various cybersecurity considerations into all relevant EU policies.

As of today, more than 70 nations have formally raised issues of cybersecurity to the level of national policy and national security, adopting national cybersecurity strategies. A list of countries, which are active in this field, includes those from both the developed and developing worlds, regardless of the regional economic integration they belong to. Therefore, issues of cybersecurity at the national level raise questions about the correlations between economic development and the need for regional cooperation and integration. Placing cybersecurity issues at the forefront also raises the question of whether we should consider ourselves to be in a crisis; or rather, we accept that cybersecurity is a continuous quest for stability in cyberspace.

Cybersecurity Strategies of the EU

Prior to 2013, the EU's approach to different aspects of cybersecurity had been widely criticised for its fragmentation, lack of clear direction and overlapping competences between institutions (Bigo et al., 2012). As a response to a changing security environment, the 2013 EU Cybersecurity Strategy thus consolidated the relevant policy areas into one framework and indicated factors that are operating regardless of state borders, as well as arising from complex economic interdependencies. It needs to be stressed that the main elements of the strategy could already be found in a

2009 Communication on Critical Information Infrastructure Protection (European Commission, 2009).

Cybersecurity has become a buzzword in the last decade, and despite the alarm bells on militarization of cyberspace[26], and discussions on the use of information and communication technologies in the context of international security (UN GA A/RES/53/70 of 4 January 1999; UN GA A/RES/58/32 of 8 December 2003; UN GA A/RES/60/45 of 6 January 2006; UN GA A/RES/66/24 of 13 December 2011), the EU's first cybersecurity strategy in 2013 remained focused primarily on economic implications of cyber threats. Interdependencies in operating, maintaining the reliability and interoperability of cyberspace, and complexities between smooth functioning of information systems and key economic sectors were highlighted. Although the strategy noted that cybersecurity is an increasingly important international issue, it significantly played down the points on how global power struggles were moving online, and how they were affecting the EU as such.

The 2013 document emphasized two main aspects of cyberspace: its role for political and social inclusion, and its importance as a critical resource and backbone of economic growth. In these respects, the strategy identified four categories of potential harm associated with cybersecurity incidents: the loss of a user's trust and confidence in participating in the Digital Single Market; disruption of essential services that rely on information and communication technologies, such as water, healthcare, electricity, mobile services; negative effects of cybercrime on the EU economy manifested in stealing data and economic damages; and the curtailment of fundamental rights online by foreign governments outside the EU. On a more concrete note, it stipulated that "(t)hreats can have different origins — including criminal, politically motivated, terrorist or state-sponsored attacks as well as natural disasters and unintentional mistakes" (EU Cybersecurity Strategy, 2013, p. 3). Hence, cyber threats are construed in the EU's 2013 policy framework as existential threats emanating mainly from the economic fields, although it can be argued that misuses of cyberspace for surveillance and control of a country's citizens is presented as an existential threat in terms of the constitutional principles of the EU; hence an existential threat emanating from the political sphere. Additionally, some concerns were raised about essential services, which could be targeted by terrorists and state-sponsored groups, suggesting that some threats could be perceived as being crucial to national security.

Measures proposed by the European Commission in the 2013 Strategy build on the principles outlined in 1.2. of the document: the EU core values apply as much

26 Quoting *the US-Russia Joint Statement on Common Security Challenges at the Threshold of the Twenty-First Century*, 2 September 1998: "We recognize the importance of promoting the positive aspects and mitigating the negative aspects of the information technology revolution now taking place, which is a serious challenge to ensuring the future strategic security interests of our two countries".

in the digital as in the physical world; protecting fundamental rights, freedom of expression, personal data and privacy; access for all; democratic and efficient multi-stakeholder governance; a shared responsibility to ensure security. It is centered around five strategic priorities, however leaving cybersecurity predominantly for the Member States to deal with, and identifying the EU's role as merely supportive and complementary in: a) achieving cyber resilience; b) drastically reducing cybercrime; c) developing cyber defence policy and capabilities related to the Common Security and Defence Policy (CSDP); d) developing the industrial and technological resources for cybersecurity; and e) establishing a coherent international cyberspace policy for the European Union and promoting core EU values.

The 2017 EU Cybersecurity Strategy (European Commission, 2017), however, represents a significant policy shift from a comprehensive to an integrated approach, clearly referring to threats in the economic, political and military spheres in nearly equal proportions. The priorities remain similar in their essence to previous strategies, but the Strategy also states that "(w)hile Member States remain responsible for national security, the scale and cross-border nature of the threat make a powerful case for EU action providing incentives and support for Member States to develop and maintain more and better national cybersecurity capabilities, while at the same time building EU-level capacity". The document proposed a set of concrete measures, which, for example, included the strengthening of the European Network and Information Security Agency; the introduction of EU-level standards and the setting up of an EU cybersecurity certification framework; limiting foreign acquisitions on critical technologies; integrating cybersecurity into EU crisis management mechanisms; the establishment of the Cybersecurity Emergency Response Fund; the adoption of technological and normative measures to combat cybercrime; the implementation of the framework for a joint EU diplomatic response to malicious cyber activities; engagement in international cybersecurity processes on the part of the EU, and similar objectives. Evidently, the strategy signified a deepening of EU integration in a matter of few years, moving from the uncoordinated isolated policies (where cybersecurity aspects were often incidental) to a horizontal policy with significant political implications at Member State as well as EU levels.

Although the new strategy may strengthen resilience as a whole, it certainly makes only baby-steps to integrate defence issues into the whole picture. The division between cybersecurity and defence is paramount in the 2017 strategy, and is even more palpable in its implementation. The need for a truly integrated policy is demonstrated by recent cyberattacks; it is not the first and probably not the last time that a malware such as Wannacry or NotPetya was rampaging across Europe, heavily affecting the private sector. This malware was publicly attributed to North Korea and the Russian military respectively by some European states and the U.S., demonstrating interconnections and entangled relationships between private and public sectors (as well as digital single market policy and defence), although the EU as such has not attributed these attacks (Ivan, 2019, p. 5). The EU's response as a whole

was tested in these cases – and some might say that the technical level cooperation was good. However, the Council of the EU admitted that it was not enough, and more needed to be done (Council of the European Union, 2018).

Although the 2017 strategy gives the impression of a well-integrated policy, the role of the EU as an advisory body is unclear therein, let alone any strategic or operational mandates in the area of cyber defence. In the absence of a clear function assigned to the EU in cyber defence – an issue which lies at the heart of sovereignty – the forward-looking initiatives, such as the General Data Protection Regulation (Regulation (EU) 2016/679) or GDPR, which can be viewed as one of the most important preventive measures in cybersecurity, the cybersecurity policy remains incomplete unless it is further developed to cover all levels from the bottom to the highest national security. While the GDPR and the NIS Directive commonly impose some significant obligations to secure personal data and networks in the majority of the EU's – and related private sector – entities, the Police Directive (Directive (EU) 2016/680) takes a rather moderate view on data protection in the public sector (focused on criminal investigations and proceedings). However, these come with notable exceptions in, for example, national security issues and there is no guidance on how these levels are interrelated, or what is the competence, if any, of the private sector in this regard[27]. Having a policy that does not fully appreciate the private sector's role across the board, and remains reactive to major breaches mainly in the form of fines, cannot be categorized as a forward-looking EU cybersecurity policy, given the private sector's importance not only in the digital single market, but also beyond that. This EU posture may change with the newly adopted Cybersecurity Act (EU 2019/881), which promises efforts in standardization, although they remain mostly within the boundaries of the EU's market-oriented competences. It is not clear whether the 2017 cybersecurity strategy is aimed at moderating the adversary's behaviour or takes a more ambitious (and likely impossible) posture to eliminate adversarial behaviour. Yet the recent EU policy-making and legislative activity in cybersecurity represents a consolidation as well as a path-finding effort, not short of a significant leap in European integration.

It could be suggested that the contributing factors for this leap in EU integration exist (at least, partially), firstly, outside the usual framework of economic interdependence, and, secondly, the Member States' associated preferences and bargaining habits. While integrating national economies in the EU has certainly not been exhausted in the field of cybersecurity, the integration of relevant policies is accelerating. Thus, having detected the EU's normative objectives on the issue, this contribution is now ready to start addressing the 'relationships-framework' question – in other words,

27 Although the detailed analysis of the particular cybersecurity legislation of the EU is omitted here, we emphasise the importance of the GDPR and other relevant acts. For a more detailed review on the EU's cybersecurity legislation, see, for example, Kasper and Antonov, 2019.

who are the interrelated actors on the issue and in what framework can the policy application productively take place? Keeping in mind the obvious need to be selective in covering relevant issues, this analysis focuses on the overall picture, bringing some examples and arguments for the sake of provoking a discussion rather than providing elaborated accounts on all elements of cybersecurity.

In order to cover the former part of the question, an observation on stakeholders is required. As for the latter part, a search for a theory-bound framework will be performed in Chapter Seven of this book titled "Towards a 'Cyber Maastricht". Should a 'Cyber Maastricht' become a goal that the EU begins to aim for, the process will need a robust model, consisting of meaningful elements ('building blocks', factors, or pillars). As argued, theories of regional cooperation and integration generally point to contributing factors, such as security interdependence, political instability, need for legitimacy, institutional lock-in of reforms and involvement of informal institutions (Börzel and Risse, 2018). In this context, there is a likelihood that technological interconnectedness and diminishing importance of geographical proximity can become risk multipliers as well.

Stakeholders or 'Who You Are With'

Evidently, EU cybersecurity policy spans through and overlaps with several sectors and policy areas, both on the economic as well as political levels. This implies that relevant stakeholders and institutions are diverse and numerous, often representing sharply opposing interests, hence the multitude of participants in decision-making processes will certainly be a significant factor that may affect outcomes.

Multiplicity of Supranational Institutions in EU Cybersecurity

To illustrate the breadth of the policy, the following departments of the Commission are involved in cybersecurity: Directorate-General for Communications Networks, Content and Technology (DG CONNECT), Directorate-General for Migration and Home Affairs (DG HOME), Directorate-General for Energy (DG ENER), Joint Research Centre (JRC), Directorate-General for Mobility and Transport (DG MOVE), Directorate-General for Financial Stability, Financial Services and Capital Markets Union (DG FISMA), Directorate-General for the Internal Market, Industry, Entrepreneurship and SMEs (DG GROW). Furthermore, the main actors also include the European Network and Information Security Agency (ENISA), CERT-EU, European Defence Agency, and EC3 at Europol.

A range of new actors which are gaining experience in cybersecurity include the European Agency for the Cooperation of Energy Regulators (ACER); the European Aviation Safety Agency (EASA); the European Union Agency for Railways (ERA); the European Securities and Markets Authority (ESMA); the European Insurance and Occupational Pensions Authority (EIOPA). Additionally, cybersecurity is being

integrated into research and training frameworks for example at the European Centre of Excellence for Countering Hybrid Threats, the European Union Institute for Security Studies, the European Union Agency for Law Enforcement Training, the European Security and Defence College, the European Cybercrime Training and Education Group, the European Cybersecurity Research and Competence Center, et cetera.

Given the number of responsible departments, agencies and actors for different aspects of cybersecurity in the EU, some of which may rather be recipients than shapers of the EU's cybersecurity policy, this research would venture with a dose of confidence to raise doubts about the neo-functionalist premise of political spillover, where particular significance is attributed to socialisation processes, and esprit de corps among officials. Although the visible efficiency of Commission policy formulation, decision-making processes, and enforcement authority should not be doubted purely on the basis of the number of parties involved, and we certainly do not intend to dwell upon a comparison with actual states, it is observed that the EU lacks a single centre of government and its governance system has been compared to no less than a "garbage can" by some influential scholars like Jan Zielonka (2012, p. 510).

However, the list of supranational institutions that actually influence the integration processes is longer still. Judicial or quasi-judicial authorities in the EU have significant influence on cyber-related policies; e.g. the European Court of Justice and the European Data Protection Board. In both cases, when it comes to cybersecurity policies, one may find not only contradictions – which would be natural in the course of the discussion within the EU – but also hesitance or outright disobedience by some of the Member States to comply with EU rules. In particular, while the EU Court with its 8 April 2014, Digital Rights Ireland judgement invalidated the Data Retention Directive (CJEU, Joined Cases C-293/12 and C-594/12), Member States still kept and keep on retaining the exact same categories of data, which led to further clarifications in the Tele2 Sverige case (CJEU, C-203/15). This shows the relative reluctance or incapability of the Member States to follow community rules and testifies to the limitations of influence of the supranational institutions.

Member States' attitudes to cybersecurity

The EU Cybersecurity Strategies push the main responsibility down to the national level. Currently all Member States have a national strategy as a key policy feature, where the central focus is on cybercrime, critical information infrastructure protection, digital literacy and cyber hygiene, capacity building and cooperation, both private-public and international. All states emphasize in their respective strategies that digitization has fundamentally changed the state, the economy and society, and that they need to ensure the smooth functioning of the information society. As a result of the fundamental changes driven by technology, internal and

external security cyberspace can no longer be clearly distinguished, and both state actors and criminal groups pose a threat. The 2016 Belgian document 'The Strategic Vision for Defence' points out for example that "(c)yber environment has not only become a part of everyday life, closely linked to the physical and social well-being of the Belgian and European population, it has also become the backbone of the Belgian and European economy (...) and has more and more security consequences" (Vandeput, 2016, p. 31). "In the future, the European countries will be less able to call in the strategic support capabilities of the U.S. such as... offensive cyber capabilities and intelligence gathering... which means that the European countries will have to invest more in these capability gaps in order to obtain the necessary autonomy" (Vandeput, 2016, p. 44).

In most national strategic documents cyber defence is complementary to other cyber-related policies, and the use of cyberspace is presented as a prerequisite for the operational capability of the armed forces.

Cybersecurity in Germany is defined as the desired state of IT, where the risks the country is facing from cyberspace are reduced to an acceptable and manageable level. "This objective can be achieved by means of cyber protection (measures against criminal cyber activities), cyber defence (measures taken against cyber-attacks mainly from abroad), cyber security policy, and cyber foreign policy". In the 2016 White paper on German Security Policy and the Future of the Bundeswehr, Germany pledged to prepare and enhance the Bundeswehr for the cyber and information domain, including high-value defensive and offensive capabilities (The Federal Government of Germany, 2016, p. 93).

Spain, in the 2019 National Cybersecurity Strategy, aims to strengthen capabilities to deal with threats from cyberspace and to implement measures, such as strengthening cyber defence and cyber intelligence capabilities, implanting active cyber defence measures in the public sector to improve response capabilities, as well as boosting the development of notification platforms, exchange of information and coordination to improve sector-based cybersecurity, and guarantee coordination, cooperation and exchange of information between the public sector, private sector and competent international organizations (Gobierno de España, 2019, p. 44). The Italian strategy also focuses on cyberspace defense operational capacities, including the need to establish Command and Control structures capable of effective cyberspace military operations planning and implementation (Presidency of the Council of Ministers, Italy, The Italian Cybersecurity Action Plan, 2017, p. 14).

France's 2015 National Digital Security Strategy also emphasized autonomous strategic thinking, security of critical networks, privacy, awareness raising, and the importance of cyberspace for the economy. In 2017, France established a Cyber Command, Commandement de la cyberdéfense – COMCYBER, and adopted a Cyber Defence Policy in 2019 based on six pillars: prevent, anticipate, protect, detect, react, and attribute (Ministère des Armées, Politique ministérielle de lutte informatique

défensive, 2019, pp. 4–5). Cyber defence capabilities have been created in the Finnish Defence Forces, including cyber-attack capabilities (The Security Committee, Finland, Implementation Programme for Finland's Cyber Security Strategy for 2017–20, p.13) and the National Cyber Security Strategy of the Czech Republic for the Period 2015 to 2020 is clear: the "state defence forces must have the capability to effectively respond to threats coming from cyberspace and proactively participate in the elimination thereof (National Security Authority, National Cyber Security Centre, 2015, p. 14). Hence one of the aims is to increase national capacities for active cyber defence and cyber-attack countermeasures (p. 18), as well as to train experts specialized in questions of active counter-measures in cyber security and cyber defence, and in offensive approaches to cyber security in general. The Lithuanian National Cyber Security Strategy also sets as an objective the development of cyber defence capabilities, stating that, "in case of failure to ensure effective deterrence, the Lithuanian Armed Forces would defend the Republic of Lithuania by using military cyber security measures acting autonomously and in cooperation with allies" (Ministry of National Defence, Republic of Lithuania, 2018, p. 8).

Cyber commands were also established in Estonia in 2018 and in Hungary in 2019, yet the Estonian Cybersecurity Strategy 2019–22, unlike others, expressly points to Europe's limited technological autonomy (computer and network hardware is produced largely in Asia, and operating systems, software and services come mainly from the U.S.), which forces the EU into a passive position, limited to responding to security flaws and focusing on risk prevention (Ministry of Economic Affairs and Communications, Republic of Estonia, 2018, pp. 21–22).

Member states' Cybersecurity policies address both military and civilian dimensions of protecting the information society, however these areas are highly interdependent. While in general states are actively militarizing cyberspace, the civilian population is impacted significantly, because attacks like WannaCry and NotPetya were/ are indiscriminate in nature and not confined to military, intelligence or other governmental targets (Griffith, 2018, p. 11). The defence posture of all EU Member States relies on increasing security and resilience-building, dissuasion of adversaries by establishing norms, some also emphasize denial-based deterrence and security (for example by adopting the 'no-legacy' principle and advocating strengthening strategic autonomy, in particular the European cyber industry). However, many EU Member States also deploy classical deterrence strategies aiming to establish credible threats.

Transnational Actors in the Private Sector

In the private sector the number of players is enormous, however we can try to make a distinction between two groups of enterprises: the ones that operate in one of the priority areas, which already fall under EU regulatory frameworks (telecom, financial services, essential service providers and digital services operators in the

meaning of NIS Directive, etc.); and the ones that fall under generic policy areas (personal data protection, information society services, IT product manufacturers, as well as cybersecurity companies and specialized associations, etc.). Transnational forums often bring together private actors, and allow for governmental and non-governmental experts to exchange information and experiences, and building mutual trust, which is known as the multi-stakeholder approach. Such forums include the Forum of Incident Response and Security Teams (FIRST), the Internet Engineering Task Force (IETF), the Institute of Electrical and Electronics Engineers (IEEE), the Internet Corporation for Assigned Names and Numbers (ICANN), the International Cyber Security Protection Alliance (ICSPA) and the Financial Services – Information Sharing and Analysis Centre (FS-ISAC). However, these forums mainly focus on narrow and technical issues, and only few (such as the Global Commission on the Stability of Cyberspace) aim to connect the various cyberspace communities and engage with broader policy questions. One should not lose sight of the user-consumer and citizen level, which may be represented by specific lobby and rights protection organizations (for example, BEUC, the European Consumer Organisation, has been vocal about cybersecurity, but privacy advocacy groups also take influential action, such as the one which culminated in the Schrems judgement (CJEU, C-362/14) which declared the 'Safe Harbo(u)r' agreement between the EU and U.S. to be invalid). In the preparations for the EU's first cybersecurity law, the NIS Directive, the private sector stakeholders participating in the consultations included individual electronic communications service and network providers; Internet service providers, and industry associations; suppliers of hardware and software components for electronic communications networks and services, and industry associations; providers of products of services for network and information security; and representatives from the banking and financial sectors, as well as from the energy sector.

Despite the existence of the consumer and privacy lobby, it should be clear that digital manufacturers and producers are constrained by their context and profit-oriented shareholders, and as long as security is considered by the markets as a luxury side-service, there are few incentives to consider implementing costly principles, such as security by design, notwithstanding that the private sector is in charge of over 80% of cyberspace. Indeed, the common industry practice is to give preference to product functionality and user-friendly design, while security considerations are secondary and fixes are issued (if at all) when flaws are discovered during use. In principle the market seems to accept the release of insecure products.[28] For the boardroom, security appears to work well when nothing happens, hence

28 Software updates and patches are issued by producers for fixing different 'bugs' or flaws, which are discovered from time to time. Such security flaws can be misused for malicious purposes. 'Security by design' approach advocates that producers should focus more on security (e.g. security testing, fixing the found flaws) prior to release, which would likely eliminate significant part of the security issues.

additional resources are hard to get for departments responsible if nothing happens. However, apart from security diligence, the imposition of security levels in sectoral and generic contexts is being generated by the EU, and by at least some awareness on all sides, including supply-chain participants.[29] Yet, the EU legislation still focuses only on some of the most significant market players, which are likely to have the resources to invest in their security or have already been doing so. The EU plans to address concerns and challenges faced by SMEs, as well as best practice in the public sectors and e-governance services, although these still remain a long-term challenge. Stakeholders showed support for the EU's plans of ensuring a high level of network and information security, and indeed the overwhelming majority looked up to the governments and the EU to take steps in this regard, pointing out that users were unaware of cyber threats (European Commission NIS Directive proposal, COM/2013/048 final). The EU is facing a puzzling double-headed question on how to present 'cybersecurity' as a marketable product, and how to create more demand for high-level security by users on an organizational and national level. While the benefits of privatization of governance and integration of private actors into the political process can be shown (e.g. increased transparency and accountability), it is also a source of several problems, in particular when it comes to issues of national security and defence. Nevertheless, the intellectual capital of the industry has been exploited by ENISA, where the proposed regulatory standards and norms often originate from the private sector (Dunn Cavelty, 2018, p. 314).

Salience and attitudes to cybersecurity in national political debates

When it comes to the Member States' and effects of the governments' constituencies on the cybersecurity policies of the EU, one can also take as a point of departure the emphasis on digitization by national political parties which can help explain aspects of the current EU cybersecurity policy. According to König and Wenzelburger (2018), the salience of digitization in party manifestos have reached the highest level in Germany, Austria and Italy, and recently increased yet remains relatively modest in the UK and France. Digitization generally does not appear to be a priority issue in Ireland, Spain and Portugal. Once the priority of digitization as a policy at the national level is determined, one may reasonably expect that cybersecurity issues (where digitization is a core precondition) could also gain salience within this broader context. Therefore, there is a likelihood that those Member States' governments would be under stronger national pressure to act, particularly in countries where digitization is more politicized, although there are also a number of other policy issues that may act as catalysts for cybersecurity-salient national policies (for instance,

29 NIS Directive.

personal data protection debates related to data retention regulations, surveillance scandals, and election 'hackings').

A brief examination of political party manifestos prima facie confirms the saliency of cybersecurity in the countries which prioritize digitization; however, the link is not straightforward between the saliency of digitization and cybersecurity. In Germany, the CDU/CSU and SPD 2017 programmes featured clear and expansive points on cybersecurity, while the Austrian ÖVP 2015 Policy Programme briefly mentions only cybercrime, and in 2018 SPÖ refers to the 'dark side of digitization'. Among the Italian parties, M5S dedicated some attention to cybersecurity within its Programme on Security, Lega just mentioned cyber bullying, but Forza Italia and Fratelli d'Italia did not raise the issue at all. In the UK, the Conservative Party's 2017 manifesto elaborates on cybersecurity in detail, while the Labour Party's manifesto does the same but to a lesser extent. In 2017 in France, En Marche! confirmed cyber defence and cybersecurity as priorities, and the Irish Fine Gael also expressed ambitions towards innovative responses to new and emerging criminal threats. In 2019, the Spanish PP and PSOE extensively elaborated on cybersecurity issues in their electoral programmes. In 2017, the Czech ANO manifesto raised several issues on cybersecurity, while a complete silence about cybersecurity was encountered in the Hungarian Jobbik's 2018 programme, and the FIDESZ programme has not been traced.

Characteristically, those states, where the level of digitization is already high, may not have this item on their political agendas as such. For instance, in Estonia, the Estonian Center Party, instead, focuses on the depth and the quality of existing databases and services, the use of Artificial Intelligence technologies for making existing systems more user-centered, as well as how to raise the quality and security of e-governance systems. The Reform Party's programme concentrates on expanding digital services; however, it specifically raises the issue of cybersecurity in the context of hybrid threats, and also addresses cybercrime and the security of the e-state. Yet, Estonia has been a vociferous policy entrepreneur when it comes to the EU and cybersecurity. Therefore, the low salience of digitization and/or cybersecurity-related issues at national level may not always indicate low priority, but could result from the deep integration of digital policies, including cybersecurity, into other policy areas.

Countries that stress digitization usually address cybersecurity as well, but in some cases (particularly, in the case of Ireland and Spain) it appears that cybersecurity has disproportionately stronger emphasis. It may suggest that beyond the economic factors related to digitization, other factors come into play when engaging in mass politics. The most cybersecurity-conscious states who raised the issue in the public debate with a holistic approach (addressing economic, social, political, defence, international cooperation questions) are Germany, the UK, France, Spain, and, to an extent, Estonia. A second round of the Treaty of Paris (the 2018 Paris Call for Trust and Security in Cyberspace) will probably happen at some point soon (with more

legitimization this time), because distinct security concerns are prompting further integration.

A report on the costs of cybercrime suggested that a good predictor of cybercrime is the income level of a country, since wealthier companies are more likely to be targeted, while countries tolerate malicious activity as long as its cost remains at an acceptable level. However, were the cost to rise above 2% of GDP, it would prompt a strong call for action from companies and society (McAfee & Center for Strategic and International Studies, 2014). Germany, which loses 1.6% of its GDP to cybercrime, is the most severely affected country globally, which explains the saliency of cybersecurity in German politics. However, in countries like Estonia and the Czech Republic, it is more likely that a trigger event occurred which ignited awareness about cybersecurity and turned it into a political issue.[30]

Conclusions

Cybersecurity became a strategic and national security issue in the past two decades. Although it is a fluid concept, it has been raised to the highest-level agendas and the European Union cybersecurity policy developed from a single market-oriented one to a comprehensive one, tackling issues horizontally. Integration in some core problem areas; such as addressing cybercrime, critical information infrastructure protection, network and information security, and personal data protection are benchmarked by instruments like the NIS Directive, GDPR and the Cybersecurity Act. However, in the light of the entanglement between private and public, external and internal, civilian and military issues in cybersecurity, significant gaps remain in the EU's supposed-to-be-integrated policy. Incidents reported daily affect both private and public sectors. Nation states and cybercriminal groups use digital attacks hiding behind anonymizing features of cyberspace, while cybersecurity in the civilian context and cyber defence in the military context address the same threats, follow the same basic principles, and require similar measures and procedures (Powell, 2018, p. 36).

Although EU institutions involved with cybersecurity are numerous and many exert significant influence on the integration process in the cyber domain, constraints inherent in the EU's lack of competences, the lack of clarity about its exact role, and resistance by Member States lessen the perspectives for integrated and EU-wide preventive policy. While both the EU and Member States focus on the reduction of vulnerabilities, both technological and human, with their other hands

30 In 2007, large-scale cyberattack mainly originating from Russia against critical Estonian targets demonstrated the potential to bring to its knees a country dependent on information and communication technologies. Heightened concern about cybersecurity in the Czech Republic is preceded by the discovery of years of Russian and Chinese presence throughout the Ministry of Foreign Affairs' information systems.

many Member States establish offensive cyber capabilities fitted to exploit the same vulnerabilities. Granted that defence issues mainly fall outside the competences of the EU, but such an approach makes cybersecurity governance in the EU even more fragmented and unsystematic. In addition, despite the dependence of the EU on external technology providers, the need for autonomy in cyber industrial terms, as well as the need for stronger public sector commitments (e.g. information sharing, high security standards for public sector information systems) cyber security is still under discussion in the EU when in fact it should have passed to action. Transnational private actors use their comparative technological advantage to exert influence on the EU's cybersecurity policy, they typically do not address cybersecurity comprehensively. Constituencies of the Member States' governments remain unengaged with cybersecurity policies, since the issue, as such, rarely enters the arena of mass politics.

References

Bigo, D., Boulet, G., Bowden, C., Carrera, S., Jeandesboz, J., and Scherrer, A. (2012) Fighting cybercrime and protecting privacy in the cloud. Brussels: European Parliament. Available at:http://www.europarl.europa.eu/RegData/etudes/etudes/join/2012/462509/IPOL-LIBE_ET%282012%29462509_EN.pdf (Accessed: 14 May 2019).

Börzel, T.A. (2016) 'Theories of Cooperation, Integration, and Governance', in Börzel, T.A. and Risse, T. (eds) The Oxford Handbook of Comparative Regionalism. Oxford: Oxford University Press, pp. 41–63.

Börzel, T.A. and Risse, T. (2018) A Litmus Test for European Integration Theories: Explaining Crises and Comparing Regionalisms, KFG Working Paper No. 85. Berlin: Freie Universität Berlin.

Christou, G. (2019) 'The collective securitisation of cyberspace in the European Union', West European Politics, 42(2), pp. 278–301. doi: 10.1080/01402382.2018.1510195.

Commission Communication, 'Network and Information Security: Proposal for A European Policy Approach' COM (2001) 298 final of 6.6.2001.

Commission Communication COM (2009) 149 final, 'Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience'

Council (2008) Report on the Implementation of the European Security Strategy – Providing Security in a Changing World – on the implementation of the European Security Strategy 11.12.2008. S407/08.

Council of Europe, Convention on Cybercrime, ETS No. 185, Budapest 23.11.2001.

Council of the European Union, Council Conclusions on malicious cyber activities – conclusions, 7925/18, Brussels 16 April 2018. Available at: http://data.consilium.europa.eu/doc/document/ST-7925–2018-INIT/en/pdf

Court of Justice of the European Union, Judgment of the Court – 8 April 2014 Digital Rights Ireland, Joined cases C-293/12, C-594/12.

Court of Justice of the European Union, Judgment of the Court (Grand Chamber) of 21 December 2016, Tele2 Sverige AB v Post-och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others, Joined Cases C-203/15 and C-698/15.

Court of Justice, Judgment of the Court (Grand Chamber) of 6 October 2015 Maximillian Schrems v Data Protection Commissioner, Case C-362/14.

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

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.

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 (NIS Directive).

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.

Dunn Cavelty, M. (2012) 'Cyber-Security', in Collins, A. (ed.) Contemporary security studies. Oxford University Press. Available at: https://ssrn.com/abstract=2055122

Dunn Cavelty, Myriam (2018) 'Europe's cyber-power', European Politics and Society, 19(3), pp. 304–320.

European Commission, (2013) Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace – JOIN (2013) 1 final, – 7 February.

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

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

European Network and Information Security Agency – ENISA, (2012) National Cyber Security Strategies – Setting the course for national efforts to strengthen security in cyberspace.Available at: https://www.enisa.europa.eu/publications/cyber-security-strategies-paper (Accessed: 15 May 2019).

Gobierno de España (2019) National Cybersecurity Strategy, M-16844–2019.

Melissa K. Griffith, et al. (2018) Strenghtening the EU's Cyber Defence Capabilities – Report of a CEPS Task Force. Centre for European Policy Studies.

Haataja, S. (2017) 'The 2007 cyber attacks against Estonia and international law on the use of force: an informational approach', Law, Innovation and Technology, 9(2), pp. 159–189. doi: 10.1080/17579961.2017.1377914.

High Level Group on Information Society (1994) Bangemann Report. Europe and the Global Information Society: Recommendations to the European Council.

Ivan, Paul (2019) 'Responding to cyberattacks: Prospects for the EU Cyber Diplomacy Toolbox', Europe in the World Programme. 18 March. European Policy Centre. https://www.epc.eu/documents/uploads/pub_9081_responding_cyberattacks.pdf?doc_id=2120

Kaska, K., Beckvard, H., Minárik, T., (2019) Huawei, 5G and China as a Security Threat. Tallinn: NATO CCDCoE Publications. Available at: https://ccdcoe.org/uploads/2019/03/CCDCOE-Huawei-2019–03-28-FINAL.pdf

Kasper, A., and Antonov, A. (2019) Towards Conceptualizing EU Cybersecurity Law, ZEI Discussion Paper C 253 / 2019. Bonn, Germany: Center for European Integration Studies, Universität Bonn.

König, P.D. and Wenzelburger, G. (2018) 'Why parties take u

p digitization in their manifestos: an empirical analysis of eight Western European economies', Journal of European Public Policy. doi: 10.1080/13501763.2018.1544268.

Ministère des Armées, Politique ministérielle de lutte informatique défensive, 2019.

Ministry of Economic Affairs and Communications, Republic of Estonia, (2018) Cybersecurity Strategy 2019–22.

Ministry of National Defence, Republic of Lithuania, (2018) National Cyber Security Strategy, Approved by Resolution No. 818 of the Government of the Republic of Lithuania of 13 August 2018.

McAfee & Center for Strategic and International Studies, (2014) Net Losses: Estimating the Global Cost of Cybercrime. Available at: https://www.csis.org/analysis/net-losses-estimating-global-cost-cybercrime (Accessed: 14 May 2019).

National Security Authority, National Cyber Security Centre, (2015) National Cyber Security Strategy of the Czech Republic for the Period from 2015 to 2020.

Powell, Neil (2018) 'Military concept for cyber defence in CSDP', in Rehrl, Jochen (ed.) Handbook on Cybersecurity, The Common Security and Defence Policy of the European Union. Federal Ministry of Defence of the Republic of Austria.

Presidency of the Council of Ministers, Italy, (2017) The Italian Cybersecurity Action Plan.

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).

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).

The Federal Government of Germany (2016), White Paper on German Security Policy and the Future of the Bundeswehr.

The Security Committee, Finland, Implementation Programme for Finland's Cyber Security Strategy for 2017–20.

Vandeput, Steven, Minister of Defence (2016), The Strategic Vision for Defence, Belgian Ministry of Defence, nr D-2017/9376/1.

Zielonka, J. (2012) 'Empires and the modern international system', Geopolitics, 17 (3), pp. 502–525. doi: 10.1080/14650045.2011.595440.