Chapter Ten

Towards a 'Cyber Maastricht': Two Steps Forward, One Step Back

Agnes Kasper & Vlad Alex Vernygora

Abstract

This chapter evaluates the EU's cybersecurity policy from four perspectives – neofunctionalism, liberal intergovernmentalism, post-functionalism, and the imperial paradigm. A search for a theory-based framework is performed to ensure that the analysis in this chapter is completed within a set of boundaries, and does not stray into speculation about the EU's prospective strategic steps. Using this contribution's findings and elaborations, a proposal on the policy-associated model is made. Having observed the empirical data, while analytically reflecting on actuality, it can be argued that a 'Cyber Maastricht' is long overdue.

Introduction

Cybersecurity is an invisible, collective and ubiquitous challenge in our modern life, as we have computerised most of the main human functions suited to contemporary lifestyles. Computers are used to distribute natural resources, feelings, and state functions, and, within our communities, we have begun to set some rules for these processes. The current EU cybersecurity policy is a result of several developments, and considering this chapter's title, there is a certain degree of positivity associated with this process. However, it is still unclear how this development is being strategised and where it might lead the EU to. Regardless of any ideological or historical connotations, one can assess the step-by-step developments when the process takes place within a framework. In the context of cybersecurity, it appears that different forces are pulling and pushing the actual development and the complexity of the domain can lead us to contradictory logics, while we are searching for explanations. Arguably, a framework can be 'crafted' for the EU by political science, and this contribution will be relying on several multi-disciplinary approaches to clarify the issues.

Retrospectively, if we focus too much on the revolutionary prediction that "Cyberwar is coming!" (Arquilla and Ronfeldt, 1993) and the no less revolutionary "Cyber war will not take place" (Rid, 2012), it is likely that a number of important events, which occurred between these Cassandrical statements, will ensure that those statements will not be forgotten. For example, in 2007, the Republic of Estonia

became a "subject of a new form of 'cyber violence'", when it experienced a large-scale denial of service (Haataja, 2017, p. 160). Those cyber events were a side-story for many, who found themselves living through an unexpected 'explosion' of political tensions, which demonstrated how an entire country can easily be brought to the brink of collapse if it is dependent on information and communication technologies for its vital functions.

In 2010, a cyber 'worm' called 'Stuxnet' affected over 60,000 computers in several countries (from Iran to the United States, from Germany to Australia), interlinking a simple USB stick with centrifuges containing uranium-235 (Farwell and Rohozinski, 2011, pp. 23–24). Indeed, theoretically, in order to make a destructive difference, no tanks and artillery are needed. Although this scenario remains popular for science fiction movies, rather than the history books – right now technological developments may have brought us close to these scenarios and for a geo-strategically 'herbivorous' entity as the EU, such a situation should be of special concern. In scholarly terms, it has arguably become one of the main catalysts for the grand-debate on what the EU is and in what framework the EU acts.

The roots of the EU lie in the historic rivalry between France and Germany, and the recognition that peace can be maintained through intense collaboration in the field of political economy. In the early 1950s, coal and steel were the basis of a country's power, given the industries' role in war-waging, and hence the 1951 Treaty of Paris concentrated on the prevention of future security threats by pooling resources, establishing common oversight mechanisms, and a common market for products and resources in these areas. The mid-twentieth century economic collaboration was seen as a means to prevent war – a paramount security threat. Today, the EU has turned into an entity that is unmatched elsewhere in scope and depth of integration, and this process took place in the context of lasting peace. This provides a platform for theories of positive integration, which acknowledges that security threats led to economic interdependencies. However, most of these integration theories seem to ignore the changed and modern security interdependencies. As Börzel and Risse (2018) argue, economic interdependencies are not always able to explain the reasons for (or lack of) regional integration: in economically interdependent North America or Northeast Asia, supranational institutions are scarce, and the Economic Community of West African States (ECOWAS), is empowered to intervene militarily in its member states without their consent, although trade levels between ECOWAS members remain low.

Historically, the EU's legal and policy measures in the field of cybersecurity have been motivated by the need to create and complete the European Single Market, whose dynamics have been mostly explicable by the spillover effect (Kasper and Antonov, 2019). The EU's new Cybersecurity Strategy sets out a plan to improve cyber resilience, deterrence and defence, and creates a horizontal policy overlapping and intertwined with several other EU policy areas. Such a complex issue as this is naturally 'plagued' by conflicting interests and controversies; in particular, that the implications go way

beyond economic aspects and the Single Market associated needs. A distinct problem has been the difficulty in collecting, sharing, and operationalizing cybersecurity information among actors (sometimes, it is referred to as cyber threat intelligence or CTI, be it in the private or public sectors). Nothing illustrates this point better than the legislative history of the Directive on security of network and information systems (Directive (EU) 2016/1148, NIS Directive), where the Commission's original proposal was changed to exclude the public sector, while calls for more actionable information sharing with the private sector were ignored at the EU legislative level. Cooperation and integration in this field deserve special attention, since at the core of resource pooling, oversight and regulation of the market, we are dealing with data and information – which, probably, are also the main resources for waging cyber and hybrid wars, because, arguably, they are the twenty-first century equivalent of coal and steel.

It is likely that the EU may be losing its way in the process of reflective, unsystematic, and inertial application of its very own and predominantly spillover-based integrative elements of cooperation and entering into a set of objectively new relationships, which necessarily require a different framework, an issue-specific system, a revision of all major theories of positive integration, and an explicitly determined range of policy clusters to confront it. In other words, cybersecurity is more complex than it is currently represented by existing EU processes, and more express links should be drawn between the market-oriented, security and defence fields. Cybersecurity, whether it is considered as a process or a point of arrival, makes it nonpareil for 'shining' at the EU's highest echelons of discussion, because "(a) stable system defines the behaviour of the collective as a whole" (Lotman, 2013, p. 62).

Hence, an enquiry on a strengthened theoretical framework should be performed, investigating the fit between EU cybersecurity policy and integration theories, to detect where the borderlines of the relationship should be, so that a proper policy framework can be provided within its boundaries. To achieve this end, a proposal based on a schematic three pillar-based model is made here. We do not adopt any particular theory to explain the EU's policy on cybersecurity, but we do engage in a path-finding mission to find correlations. Indeed, we leave it for future research to dwell on the details.

Methodologically, this material extensively employs a pluralistic range of classic and cross-boundary qualitative techniques, elicited from discourse analysis, process tracing and normative content analysis. As Neumann (2008, p. 62) argues, discourse analysis not only "seeks to capture the inevitable cultural changes in representations of reality", but a particular discourse in itself "maintains a degree of regularity in social relations (...), produc(ing) preconditions for action". It is not worrying that the reason for an action cannot be fully determined by analysing a discourse that is corresponding to it – instead, process tracing is required in such cases. Characteristically for this classic qualitative tool, it can assist in providing a number of theoretical alternatives, because the in-depth checking procedure

(on what factor is linked to which) can encourage research to consider different theoretical frameworks. Indeed, the further the EU drifts away from the theoretical paradigms of the 1950s, the more stagnating its integrative framework is becoming. In the highly complicated case of cybersecurity, this contribution suggests that, by necessity, EU policy requires a solid theoretical fit (or, at least, the EU is in askance of a useful theory) built on a neo-functional, intergovernmental, and post-functional analytical instrumentarium, whilst keeping in mind an imperial paradigm as a means to explain the EU's organisational nature more precisely.

Finally, on a further methodological note, the EU has an inbuilt normative characteristic. Norms are thus very important in this empirical investigation to observe the relevant processes and find interlinkages between them. By determining the right set of normative material and contextualising the data, it is possible to analytically "account for the nuances and complexities that are part of any political phenomenon" (Hermann, 2008, p. 160). For the context and stakeholders' attitudes, we will also refer back to the previous chapter in this book – 'EU Cybersecurity Governance – Stakeholders and Normative Intentions towards Integration' – which outlined the rise and current features, as well as the institutional background of the EU's cybersecurity policy.

Searching for a proper framework

There is nothing extraordinary in searching for a framework, because an academic wishes to "place rigid boundaries around the domain of philosophical inquiry" (McCormick, 2003, p. 255). Apart from being attributed by positivists to Immanuel Kant, it has a longer history and a life within post-positivism. It is advantageous to achieve a "greater accuracy of description" (Lotman, 2013, pp. 48–49), and it goes well with this contribution since it is aiming at detecting the exclusive range of constituent clusters for EU policymaking on cybersecurity.

What is also relevant for the context is that the EU, meticulously treasuring its 'theoretical' organisational background, has consistently been a theory-driven entity in its policymaking. Through its existence, the EU has literally encouraged international scholarship to analyse its development, and in the process, this 'created' some of the major integration theories as well. There was a relatively sceptical vision of Robert Keohane (1984, p. 49) that "the Europeans" do not have the functional capacity to grow into a hegemon "in the foreseeable future", but this is questioned by actuality. A hegemon has different qualities, and the EU's distinct hegemonic stance in international trade is not a matter for serious academic disputes.

Practically and usually, a particular EU policy could receive backing from a single theoretical concept (for example, intergovernmentalism for the Common Foreign and Security Policy (CFSP). However, there are many situations when the EU aims at combining a few theories in order to establish a decent framework for a policy (e.g. regionalism, neo-regionalism, functionalism and neo-functionalism for the

European Neighbourhood Policy/ENP). The level of effectiveness in each case has been different: the EU's 'exam marks' in political economy are rather high, but when it comes to the entity's 'tests' on geo-strategy, there is still plenty of 'homework' that needs to be completed by Brussels and, to an extent, Strasbourg. On cybersecurity, as it was argued in the introductory notes of this chapter, there is a likelihood that, in order to positively benefit from the policy-focused theoretical support, the EU has to seek some assistance from among the analytical postulates of the following four concepts: neo-functionalism, intergovernmental theory, post-functionalism, and a scholarly 'treatment' of the EU as a contemporary political empire.

Neo-functionalism: a 'puzzle' of transnational interdependence and supranational capacity

Within a decade from the start of the European integration process, Ernst Haas (1958), reflecting on the project's development, offered a holistic observational concept exemplified by it. His neo-functionalism, was only semantically linked to David Mitrany's seminal contributions (1975), but it helped the EU's founders in interpreting what they were functionally doing to 'run away' faster from the past. At the end of the day, as the theory was elucidated by its competing 'cousin' (post-functionalism) much later in time, the neo-functional framework postulated "a series of mutually reinforcing processes that [would] lead to further integration" (Hooghe and Marks, 2019, p. 2). Arguably, the so-called neo-functional spillover became the EU's major, as well as almost unquestionable, methodological tool in a number of important framework-building exercises (for example, in the case of working out the euro convergence criteria). It is also true that the EU missed few opportunities to perform some kind of "distilling" (McGowan, 2007) of neo-functionalism. Further down the track, the 'spillover effect', as noted, became "almost completely detached from its puzzling fathering theory" and, like in the peculiar case of the European Neighbourhood Policy (ENP), was even applied to a geographic area, which Brussels could not operationally control (Vernygora et al., 2016, p. 14). Should neo-functionalism be employed in the context of the EU's policy on cybersecurity?

The basic underlying rationale for cybersecurity cooperation can be viewed in terms of securitised functional logics: the dependence of the EU's economy and citizens' every-day life on information and communication technologies create exposures that endanger the Digital Single Market, European democracies, freedoms and values. Bergmann and Niemann (2018) point out that sectors and issues can be interdependent to the extent that differentiation may prove extremely difficult. This is even truer in the context of cybersecurity, where the underlying technologies operate without respect for state borders and are decentralised in nature.

Functional discrepancies and links can certainly be identified in the EU's cybersecurity policy, for instance between the free movement of digital products and the need for safe and secure Internet that fosters consumer trust. In this case,

criminal law enforcement plays a significant deterrent role against cybercrimes, but it compromises consumer trust. In order to investigate offences, law enforcement agencies, more often than not, need to collect evidence from information systems outside their national borders, and they need it fast, whereas the current mechanisms for cross-border cooperation to collect evidence can be burdensome. Hence, the EU proposed the E-evidence Regulation that creates the European Preservation and Production Orders, mechanisms associated with procedures that are, presumably, easier to implement vis-a-vis private sector stakeholders. However, this has also opened a window outside the EU, since the largest actors in the EU are U.S.-based companies. The USA had also decided to address digital evidence collection, which resulted in conflicting legislations with the EU (additionally there are some legal issues and conflicts in the GDPR), while the Council of Europe (CoE) is also busy with negotiations on an additional protocol to the Cybercrime Convention, addressing questions of digital evidence.

On 5 February 2019, the European Commission proposed to start a round of international negotiations on cross-border access to electronic evidence, which is necessary to track down dangerous criminals and terrorists, and two sets of negotiating directives were issued: one for negotiations with the USA, and the other for the Second Additional Protocol to the CoE-originated Budapest Convention on Cybercrime (Joint Statement on the Launch of EU-U.S. Negotiations to Facilitate Access to Electronic Evidence, 2019). The logic that a single market issue needs to create higher levels of consumer trust for digital products, leads to functional pressures in the security and foreign relations domain, in this case the e-evidence negotiations with the USA and the CoE, which Bergmann and Niemann (2018) described as "external spillover".

Another functional discrepancy can briefly be indicated between the high-level network and information security requirements, as in the NIS Directive (European Parliament and the Council, 2016) and the need for standardisation and certification schemes. Evaluation of the security levels of networks and information systems, as well as digital services and products, to ensure conformity with EU-wide or at least harmonised cybersecurity standards, hence the Cybersecurity Act (European Parliament and the Council, 2019), confer new competences, tasks and resources on the European Network and Information Security Agency (ENISA) (which has been transformed into the EU's Cybersecurity Agency).

Functional pressures stemming from the Single Market also seem to appear in the field of security and defence, notwithstanding that some scholars deny this (Bergmann and Niemann, 2018). On the basis of the 2013 Single Market-focused Cybersecurity Strategy, the EU Cyber Defence Policy Framework was adopted in 2014 (Council of the EU, 2014) and updated in 2018 (Council of the EU, 2018a). These strategies envisage EU and NATO cooperation on cybersecurity and defence. In 2018, the EU cyber defence staff also took part in the NATO's Cyber Coalition exercise, in

Estonia (NATO News, 2018).[31] Functional pressures, linkages and interdependencies may seem to point to the neo-functional theory of integration; however, it is not able to account for a significant part of the EU's cybersecurity policy, since transnational actors remain 'toothless' when it comes to issues beyond purely private business and the Single Market.

The role of supranational institutions enjoys distinct attention of neo-functionalist theories of integration. Niemann (2016) explains that supranational institutions foster integration processes when they behave as policy entrepreneurs or when leveraging their central positions or authority to influence various actors. Hooghe and Marks add that this is a continuous process reinforced by learning, changing preferences and tactics, until the supranational actors become stronger and more autonomous (2019, pp. 2–3). After learning the lessons from international cyber incidents, and because of direct attacks, cybersecurity became one of the most salient issues in the EU's agenda (Christou, 2016, p. 1), and the European Commission has played a very significant role in promoting integrated policy development in cybersecurity.

However, the cross-jurisdictional nature of problem areas put supranational institutions in a position where their impetus for greater cooperation and integration encounters significant resistance based on Westphalian principles. One of the most intricate issues involves cybersecurity information collection and sharing, which cuts across policy levels. During the 2012 stakeholder consultations in preparation of the NIS Directive, 87.5% of respondents indicated that public administrations should be subject to security requirements. In particular, 93.5% considered that public administrations should report security breaches (besides banking and financial sector, transport, health, energy and internet services). While this signified a call for Member States' accountability and was backed by the EU institutions such as the European Data Protection Supervisor, the European Parliament, and the European Economic and Social Committee, the Council of the EU was not ready for a new grand design that impinges upon the heart of the Member States' sovereignty. The Economic and Social Committee (2014) had stated that the NIS Directive should take the form of a regulation, which would leave little discretion in Member States' hands. The proposal's provisions would have led to the setting up of a cooperation network and secure information-exchange system between the Member States, the Commission and ENISA, and provide for coordinated response according to the EU's NIS Cooperation Plan. It would have imposed security requirements of public administrations, but these were toned down to the minimum by the Council which meant that only some core private actors in cyberspace (essential services operators, cloud services, e-marketplaces and search engines) were affected and breach notification frameworks were set up. The focus remained one-sided, imposing

31 See more in NATO (2018) *NATO and the European Union work together to tackle growing cyber threats*. Available at: https://www.nato.int/cps/en/natohq/news_161570.htm?selectedLocale=en

mandatory controls on information flows between the private and public sectors and leaving cooperation between Member States at the voluntary level. The Council's formal message was (Council of the EU, 2013):

> Many Member states have been in favour of more flexibility, limiting the adoption of binding rules at EU level to critical and basic requirements, to be supplemented by optional measures. Other delegations on the contrary, considered that only legally binding measures could guarantee the network security throughout the EU.

Additionally, competences and resources are still lacking at the supranational level, since implementation of the cybersecurity policy and operational capacity lies with the Member States, as the "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" (European Commission, 2017).

The EU's capacities are being strengthened, and the establishment of the EU's Cybersecurity Agency endowed with financial, human and some operational resources testifies to this ongoing process, but in politically more sensitive areas the competence of supranational institutions is called into question by the Member States while they are engaging in a "common reflection process" with DAPIX experts [Working Party on Information Exchange and Data Protection (DAPIX)] on data retention (Council of the EU, 2018b). This behavior amounts to ignoring the highest courts' repeated rulings against blanket data retention legislation. This is not to say that neo-functionalist 'episodes' do not take place in the EU and cyberspace. A number of EU institutions have been active and accumulating significant expertise in cybersecurity, including the Commission, ENISA, European Defence Agency, etc, which on their own or by leveraging functional inefficiencies, budgetary powers or institutional gaps, can lead to a strengthening of their role, which could eventually lead to deeper integration of the EU (Kasper and Mölder, 2019, forthcoming).

With reference to the explanation by Hooghe and Marks (2019, p. 3) of the neo-functionalist views that "integration is the outcome of cooperation and competition among societal actors", one can find little evidence to support a claim that stakeholders other than the Member States steer the deepening European integration in the cybersecurity domain. Since 2016, the EU has positioned itself on a trajectory towards strategic autonomy, including that in cyberspace. The 2017-revised EU cybersecurity strategy, and, in particular, the 2018 update of the EU Cyber Defence Policy Framework, emphasise the growing linkages between cybersecurity and cyber defence, yet the Member States' hesitation about the EU as a (cyber) security community is still manifested in the volunteer nature of information sharing mechanisms (apart from the breach notifications obligations imposed on private sector players), signifying

their readiness to work to create a 'cyber steel and coal community', which is still a long way from a 'Cyber Maastricht'.

(Still) Liberal Intergovernmentalism: Member States, their preferences and bargaining power

In a way, Liberal Intergovernmentalism could hardly be outlined using a more straightforward route than the one chosen by Andrew Moravcsik. Being presumably driven by a justified desire to reshuffle the postulates of intergovernmentalism and to see how much out of the Westphalian paradigm would be considered practically applicable in the present situation, Moravcsik (1998, p. 4) linked the positive effectiveness of European integration with "economic interests, relative power, (and) credible commitments" of the Member States as long as they continue to subscribe to a liberal outlook. In other words, as Schimmelfennig (2015, p. 178) extensively explained much later, the process of integration "results from three steps that translate the incentives created by international interdependence into collective institutional outcomes: the domestic formation of national preferences, intergovernmental bargaining to substantive agreements and the creation of institutions to secure these agreements". Another summary of this iconic concept is supplied by its 'competitors' – Hooghe and Marks (2019, p. 4) – who noted that "(l)iberal intergovernmentalism conceives institutional outcomes as functional responses to cooperation problems (...,) anticipat(ing) that states will delegate or pool just enough authority to ensure that national governments will find it in their interest to comply with the deal". Once again, the obvious assumption here is that the EU Member States remain effectively liberal in general, and positively liberal towards the EU's 'togetherness' when such an exercise needs to be performed. Arguing, bargaining, and being not fully satisfied are distinguishing features of the liberal intergovernmentalism-based framework. Undermining, humiliating, and questioning the EU as an objectively reliable provider of multi-dimensional opportunities cannot be considered natural for liberal intergovernmentalism in the process of seeking solutions. The latter statement is still in full agreement with Schimmelfennig's argument that this theory of integration "offers no specific propositions to account for the crisis as such" (2015, p. 178).

Since 2007, when Estonia realised that its dependence on information and communication technologies leads to new vulnerabilities and exposes its society to existential threats operating through cyberspace, it has become a global heavyweight in cybersecurity with several innovations implemented in the technological, legal and political domains, and deservedly can be referred to as an avant-garde experimental bunny after introducing innovations like e-residency (Särav, Kerikmäe, and Kasper, 2017). Inspired by Estonia's success and after examining other top scorers in cybersecurity indexes, several observations can be made, and which will provide an overall discussion in this chapter.

According to the ITU's Global Cybersecurity Index, Estonia achieved peak scores in legal and technical commitments, occupying the fifth position after the UK, the USA, France and Lithuania (ITU, 2018, p. 18). Although cooperation commitments generally remain low, Lithuania, Estonia, the UK, Spain and France take the lead in the EU, while the EU as a whole is far more committed to cooperation than other regions of the world (ITU, 2018, p. 49). According to the National Cyber Security Index administered by the Estonian E-Governance Academy, which measures the preparedness of states to prevent cyber threats and manage incidents, the Czech Republic, Estonia, Spain, Lithuania and France are the global leaders, with Germany and the UK following them. However, the digital development levels of these countries do not seem to provide a simple plausible explanation for scoring high in cybersecurity. The curious cases of Estonia, Lithuania, and the Czech Republic – where the digital development scores are modest – imply that factors other than economic ones may have significant impacts on governments' plans.

Since the end of 1990s, the EU has been engaged in fighting 'classical' cybercrimes and it has adopted positions on the negotiations on the CoE Convention on Cybercrime. As one of the early attempts to raise the complex issue of cybersecurity to the EU level, the Spanish Presidency proposed in 2001 the establishment of an EU Research and Technological Alert Center (Council of the EU, 2001). Although the proposal referred to 'cybercrime', its reasoning was based on concerns raised from national security threats following the 9/11 terrorist attacks. The Spanish proposal was somewhat misinformed about the lack of initiatives. The Stockholm European Council of 23–24 March 2001 concluded that "the Council together with the Commission will develop a comprehensive strategy on security of electronic networks including practical implementing action" (European Council, 2001). A few months earlier, the Commission had also referred to the growing national security concerns and difficulties in providing security due to liberalization, convergence and globalization (Commission of the European Communities, 2001). Indeed, in the aftermath of the 9/11 attacks, the Council was quick to turn its attention to address terrorist threats and critical infrastructure protection, which included information and communication technology and the internet (Commission of the European Communities, 2004).

While the Commission has examined the available electronic communication infrastructures and their robustness in 2007 in high detail, cybersecurity remained an 'exotic' topic for the Member States. Three overlapping sets of EU policies were pursued in parallel. One was on cybercrime, which could be traced back to the need to deal with organised and high-tech crime – predominantly motivated by economic gain. The other concerned critical information infrastructure protection, which can be linked to the recognition of terrorist threats – assumed to be motivated by ideology. The third was on strengthening the information society to complete the Single Market, hence economic considerations.

After the large-scale cyberattacks against Estonia in 2007, the terminological construct of critical information infrastructure protection started featuring in the Council's agenda with increasing frequency, and, between 27 and 28 April 2009, Tallinn hosted a ministerial conference, stressing the importance of cybersecurity based on its own painful experience. The Member States' ostrich-like policies were about to change, following security threats close to home, and after realising the possibilities that cyberspace could be used for political purposes, following the 2008 cyberattacks against Lithuania and Georgia.

Preferences shifted towards establishing common policies, common mechanisms and coordination. The interdependencies between policy areas, the evolving and growing threat landscape, and the complexity of cybersecurity left Member States with no real alternatives but to merge the separate policies into a single comprehensive one at EU level. While 12 Member States decided to ratify the CoE Convention on Cybercrime after 2007[32], the 18-month trio-presidency programme of the Council led by the Polish, Danish and Cypriot Presidencies, in 2011 already raised cybersecurity issues going beyond cybercrime (Council of the EU, 2011).

In 2012, the Friends of the Presidency Group on Cyber Issues was established as a cross-cutting forum for coordination and cooperation and exchange of information encompassing various fields of expertise. In a December 2012 meeting of the group on Cyber Issues, the Netherlands reported yet another real cyberattack[33], and emphasised the need for cross-border cooperation. In the meantime, Estonia announced its next Cyber Security Conference, which was organised in Brussels.

In the context of the 18-month trio-residency programme of the Council for the period 1 January 2013 to 30 June 2014, the Irish, Lithuanian and Greek Presidencies, clearly referred to cybersecurity as one of the global challenges faced by the EU (Council of the EU, 2012). The first EU Cybersecurity Strategy was adopted in 2013, but the Member States resisted significant deepening of integration in several politically sensitive areas. The Member States' approach to comprehensive cybersecurity was tailored to the needs of sovereign states and was followed by the adoption of an outline for European Cyber Diplomacy Engagement. The Members States regularly discussed cyber defence questions, and the Council adopted the EU Cyber Defence Policy Framework at the end of 2014 (Council of the EU, 2014a). While the Member States' approach to information sharing and their readiness to express their positions publicly on cybersecurity is still cautious, the high interest in clarifying the normative frameworks became evident in The Hague Process, when over 50 countries participated in the Tallinn Manual 2.0 consultations on how international

32 Those were Austria, Belgium, the Czech Republic, Germany, Greece, Italy, Luxembourg, Malta, Poland, Portugal, Slovakia, Spain, and the UK.

33 The Netherlands have previously experienced the Diginotar incident, although there are no indications that this particular case was discussed at the meeting.

law could apply to cyber operations – although, state input in the Manual remains confidential (Asser Institute, 2016).

The subsequent Italian, Latvian, and Luxembourgish trio Presidencies also strongly emphasised comprehensive cybersecurity, and laid out an ambitious agenda prioritising internal and external actions (Council of the EU, 2014b). For the period between 1 January 2016 and 30 June 2017, the Dutch, Slovak and Maltese Presidencies aimed to have a comprehensive and integrated approach to cybersecurity, and kept the focus thereon, although their programme was more pragmatic, and increased secrecy in the Council's work on cyber issues became evident (Council of the EU, 2015). The Friends of the Presidency Group on Cyber Issues, drawing on the "claimed to be state-sponsored hack of the Ukrainian power grid" prepared a non-paper suggesting a joint response to coercive cyber operations, namely the development of the cyber diplomacy toolbox under the Common Foreign and Security Policy and the Common Security and Defence Policy (Council of the EU, 2016). The strategic environment also led to a new impetus in EU-NATO partnership, and the Joint Declaration in Warsaw on 8 July 2016 included cybersecurity and defence as an area where cooperation should be enhanced. In 2016, the Horizontal Working Party on Cyber Issues was established, replacing the Friends of Presidency Group, while the world learned about the DNC hack and Russian interference in U.S. elections (arguably, both cases sent clear signs about the vulnerabilities of national elections).

The Estonian, Bulgarian and Austrian Presidencies prioritized cybersecurity policy as an integral part of a genuine Security Union (Council of the EU, 2017), and Estonia laid out a very strong digital agenda building on its 2007 experience of large-scale cyberattacks and the EU's cybersecurity package was rolled out on 13 September 2017. This updated the EU's cybersecurity strategy, and included proposals for institutional changes in terms of establishing the EU Cybersecurity Agency, integrating cybersecurity into existing EU-level crisis management frameworks, and adopting the Cybersecurity Diplomacy Toolbox. In 2017, the Czech Republic also discovered that for many years Russia and China had penetrated its Foreign Ministry's information systems (Czech security service says Russia behind cyber attacks on ministry, Reuters, 2018).

Current focus in the Council appears to centre on the implementation of the Cyber Diplomacy Toolbox, the detailed discussion of questions related to attribution, cyber restrictive measures, preparation for the upcoming discussions in the United Nations (UN) on cyber issues in the context of international security, as well as cybersecurity capabilities and capacity building.

Having pointed out some key turning points, the authors note that despite the Commission's thorough analyses and reasoning about interdependencies and security threats, the impetus to develop policies came from the Member States governments, prompted by their realisation of the political threats posed by cyberattacks. Since the EU is not a federal state, the arguments for sovereign autonomy of the Member

States overwhelmed the functional arguments for deepening integration, which is an underlying need for small states in an interconnected world. Ambitious Commission proposals were toned down and reformulated, under the Council's leadership, in a manner that better corresponds to the Member States' readiness to cooperate and share in potentially sensitive areas of cybersecurity.

Post-functionalism: channeling a political conflict towards a common good

A post-functionalist theory of European integration, has an empirically stable base as a point of departure: a) it has the possibility to detect how "domestic patterns of conflict across the [EU] constrain the course of European integration"; b) "no one has succeeded in reducing the debate to rational economic interest"; and c) since national communities are demanding more self-rule, "the preference for self-rule is almost always inconsistent with the functional demand for regional authority" (Hooghe and Marks, 2008, p. 2). However, where does the initial push for action come from? The theory refers to the prime role that a political conflict "makes all the difference, and [...] engages communal identities" (Hooghe and Marks, 2008, p. 2).

In the context of classical functionalism and apart from "common material needs" (Mitrany, 1975, p. 145), in principle an integrative task, "can be narrow or comprehensive in scope" (Smith, 2004, p. 22). In addition, "an action to stop the process or to go backwards is a function-performing exercise" as well (Vernygora et. al., 2016, p. 15). At the same time, this post-functionalist view on where a desirably effective functionality can 'reside' within the framework of European integration claimes that there could be a need to "probe beyond the economic preferences of interest groups" (Hooghe and Marks, 2008, p. 5). Is it not what cybersecurity needs to 'hear'?

While post-functionalist literature on EU cybersecurity is almost non-existent, it could be possible that functionality resides with interest groups – since cyberspace is predominantly owned and operated by the private sector. However, one should consider those factors that characterise cyberspace – particularly, the compression of time and space in this context, which challenges not only the worldviews, but the core elements of the current international order based on territoriality. In addition, technical challenges and the lack of a common vocabulary in the technical and non-technical fields do not favour political institutions in identifying common domestic constraints to integration, which could be formulated into a joint agenda by the relevant actors. Scholars who write on cyber power refer to the passive role of non-state actors who recognize the need of their 'intellectual capital', while stressing that the "state is the political entity that needs to learn how to optimize its cyber power" (Dunn Cavelty, 2019, p. 307).

The fragmentation and diverse interests in cybersecurity make it almost impossible to create a community (besides the ones headed by national governments or another

central institution) on cybersecurity. Cybersecurity does not (yet?) typically feature on national political parties' agendas, while interests intertwined with cybersecurity cannot be reduced purely to economic or political ones given their complexities. Policies on cybersecurity feature military, diplomatic, intelligence, economic, legal, ethical and social considerations. Cyberattacks are not immediately apparent to communities, and tend to be discovered months after their commencement. Unless they lead to consequences, which affect the physical world in a palpable manner, it cannot be confidently assumed that societal processes on their own will lead to comprehensive cybersecurity policies. People are unlikely to perceive a 'common material need' to have such policies.

Cyberspace is not a homogenous community, but a conglomerate resembling a loose open source community without a central point, sharing overlapping principles and agreements at the technological level. While some participants can be mature enough to ride on established frameworks, the rest move with the flow; trusting a central coordinating authority to show what is to be done next. Those who behave in this way often find their ideas suppressed by overriding political considerations, and naturally in such an environment only the strongest and most persistent, usually large private actors can pursue impactful initiatives. Joint private initiatives to engage with policy-makers have been reported in the USA (see, for example, Breland, 2018), and significant similar efforts by think tanks have become evident, such as the Global Commission on the Stability of Cyberspace, but the situation in the EU remains considerably more fragmented given the different levels of development of the Member States' cybersecurity policies. Controversially, Dunn Cavelty (2018) claims that the ENISA's (EU Agency for Cybersecurity) main reason for proposing standards and norms to the industry, was to ensure as little influence from governments as possible. However, do we expect (trans)national actors and industry to consider various potential national security implications to the full, and then choose the policy option that may be the best solution for European society, even at the expense of losses to shareholders?

In the meantime, while the responsibility for cybersecurity is pushed down to the national levels, little politicisation at the domestic levels can be detected (see Chapter six by Kasper in this book). Decision-making rarely takes place in the arena of mass politics and steps towards integration have not been linked to identity issues or to cultural divides that polarise societies. Hence, it appears that in its current form, the post-functional theory of European integration cannot provide a definitive explanation of all the realities of cybersecurity policy in the EU.

A contemporary empire on a mission to engage its periphery?

These days, as Zielonka noted, "(i)n the field of diplomacy it is virtually impossible to conclude any global negotiations without the consent of (the United States, the EU, Russia, and China)" (2012, p. 509), while also arguing that these important actors

"'look, talk and walk' like empires" (2012, p. 502). Arguably, this imperial paradigm is academically useful, has no negative connotation, and can be employed in different analytical exercises. The point is that the EU tends to claim its "technocratic or institutional superiority", making the essence of the entity's civilising mission to be bound around exporting 'good' governance (Zielonka, 2012, pp. 515 and 511). Remarkably, it goes very well with one of the major priorities of the 2013 EU Cybersecurity Strategy, which proposed focusing on establishing "a coherent international cyberspace policy for the EU and promote EU values" (European Commission, 2013). It can be noted that one of the operational objectives of this priority may be based around an idea to engage the EU's periphery into the process.

The race for domination in cyberspace has long begun and recently it has found concrete form in the UN-framed discussion on cybersecurity. While U.S. dominance of cyberspace, in technological terms, remains unquestioned (not unchallenged though), in other 'soft' areas a clear competition has become manifest. When, in 1998 the Russian Federation proposed a draft UN resolution on cybersecurity, it was not taken seriously. However, it ignited a process in which the developments in this field were noted by the so-called UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE). The work of the UN GGE went mostly unnoticed and was fruitless until 2013, when the experts finally made a breakthrough: international law applies to states' cyber operations (Kaljurand, 2016, p. 112). While this conclusion may now seem like a no-brainer, the UN GGE never managed to answer the question as to how international law applies (Henriksen, 2019).

A competition for the 'legal' dominance of cyberspace officially commenced in late 2018, when both a new open-ended working group and a new GGE was approved by the UN. The proposal to set up an open-ended working group was sponsored by Russia, while the proposal for the GGE was backed by the U.S. and like-minded states, including the EU Member States. Many states in the UN are still undecided about their approach to cybersecurity, participating in both or none of these groups, hence these recent developments clearly signify a major contest between two fundamentally different ideologies on how cyberspace should be governed/ruled. It is no surprise that the Council and the EU Member States are preparing for these meetings, nevertheless it also straightens out illusions that the EU is limited to economic cooperation, since the EU seems to be embarking on a global 'civilizing mission', at least in as far as online human rights are concerned, while at the same time prioritizing capacity building in cybersecurity.

The EU has been engaging in bilateral cyber-partnerships with key countries, such as the U.S. (perhaps the most comprehensive relationship), Canada, Japan, Brazil (on cybercrime and research) and some other 'strategic partners', amongst them India and the Republic of Korea, are seen as the most promising. Bilateral cooperation with Russia and China is less straightforward, since these countries are perceived as the main source of major cyberattacks and cyberespionage in the EU – although

confidence-building initiatives have been reported mainly in the fight against cybercrime and cyberterrorism (Renard, 2018, pp. 328–330).

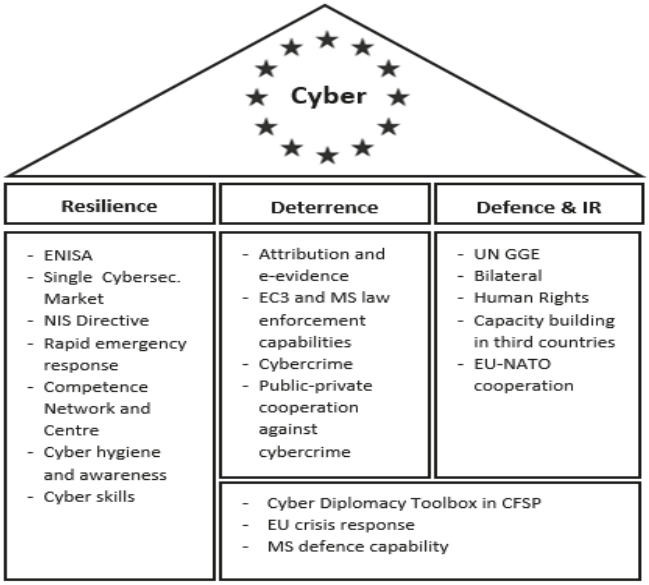
The three 'Cyber Pillars' of the EU

In the past five years, the ENISA reported that each year cybercriminals remained the most active threat agent group in cyberspace. In 2018 they were responsible for over 80% of incidents, affecting approximately 0.8% of GDP (ENISA, 2019, p. 119). Over 60% of email traffic contained malicious content, and email was involved in 90% of the cyber-attacks. In second place came the 'insiders' threat agent group with 25% of breaches, attributed to insiders in corporate environments. That same year, states as threat agent group came in third place. ENISA observed attempts to increase the impact of cyberattacks (particularly, in critical infrastructures). ENISA (2019, 117–118) also pointed out that "[i]t is assumed that traditional state sponsored threat agents are currently repositioning themselves in the changing geopolitical space". The discovery of vulnerabilities continues to increase and advanced threat actors "are making progress in using the supply chain to achieve their objectives". The EU is facing numerous challenges at different levels, but the most significant is clearly cybercrime, impacting the economy. However, threats originating from states, and the use of the internet by terrorists, as well as the manipulation of social media cannot be underestimated either. Links between cybersecurity and hybrid threats are also highlighted by the Joint Communication on Countering Hybrid Threats (European Commission, 2016b) and media reports using terms such as 'social media warfare' (The Telegraph, 2019). These trends call for national resilience-building and cooperation in law enforcement, as well as deeper trust and cooperation between allies such as that between the U.S., the EU and NATO.

Hostile or malicious activity passes through several jurisdictions and leverages assets in private hands: for example, botnets use networks and compromised computers, servers and IoT devices (i.e. a smart watch, smartphone, smart lightbulb, or any internet-connected device) to attack a target system. Similar techniques can be used by cybercriminals, terrorist groups, as well as states. Such hostile actors easily hide behind anonymity-enabling and/or plausible deniability features of cyberspace. In countering such ambiguous attackers, measures need to be applied in several areas including underlying technologies, business practices, and market dynamics. There is also a need to develop security standards covering critical infrastructure or consumer devices, rules for responsible disclosure of vulnerabilities, patching and updating of software, regulatory frameworks to address liability issues and the elaboration of the 'duty of care' principle. It also requires building cyber threat intelligence capabilities, or controlling the foreign acquisition of critical cyber technologies. In short, it calls for a broader view where the lines between the internal and external policies, between market-oriented, criminal and defence policies are blurred.

A nouvelle model of cooperation has to be created by/for the EU to realise its objectives in cybersecurity. Historically, the EU has been shaped by schematic grand-scale structural pillars. This approach can once again be used to clarify the EU's vision and strengthen its actions on cybersecurity. A 'Cyber Maastricht' model could be constructed, based on the following three pillars: Resilience, Deterrence, and Defence & International Relations/IR (see Figure 1 for details). The model's structural elements are not new, and what is more important is the place, the nature of the elements, and the interrelations between the proposed pillars as foundations for new governance institutions.

FIGURE 1: A 'CYBER MAASTRICHT' MODEL



Source: Authors

A gargantuan element of the world's political economy, the EU needs to be capable of recovering as fast as possible after a prospective cyberattack. Moreover, given the tightness of intra-entity cooperation, a resilient EU means a great deal more than a resilient Member State taken separately from the EU, immaterial as to whether such a state is big or small. However, such a pillar structure finds plenty of operational space within a post-functional framework.

While cyber resilience-building in the EU is often justified by the need to complete the single market, one needs to look beyond economic considerations and realise the informational interdependence of actors, which is very visible, as for example in the vulnerability of disclosure mechanisms (or the lack of them). Security information,

just like cyber-tools, tends to have a dual use. Interdependence is multi-dimensional, and leads to the necessity of appropriate institutions and mechanisms for sharing information among private players, between private and public sector, and between states. However, current solutions include one-way or voluntary information flows, in which bridges to other pillars are difficult to build. Resilience is also linked to technological factors, such as the presence or absence of a high number of errors/bugs/flaws in products, which leads to fewer public concerns and also calls for interaction with other pillars to decrease vulnerabilities. This also fits the concept of deterrence by denial as opposed to deterrence by punishment (Burton, 2018, p. 9). Thus, the resilience pillar's aim is to increase both private and public sectors' accountability for technologies to absorb malicious cyber activities and incidents, as well as transparency among actors to the maximum possible level.

If a 'Cyber Maastricht' can establish a normative re-conceptualisation of the EU as a deterrence provider, it can lead to a significant change with regards to the EU's geo-strategic role. The dominant legislative side of this pillar can, in principle, be supported by the theoretical platform of liberal intergovernmentalism. A range of serious 'credible commitments' can be worked out, for example, on 'attribution and e-evidence', which are also relevant in the context of the third pillar where they are guided by the strict constraints of criminal legal frameworks rather than political ones. Whereas national governments as gatekeepers to protect the interest of societies are privileged actors in the second and the third pillars, their losses in authority by means of surrendering competences to EU is compensated by gains in legitimacy and problem-solving capabilities. As reluctant or incapable as Member States have been to resolve conflicts between law enforcement needs and fundamental human rights regarding the data retention regime, functional pressures – arising from the trans-border nature of data flows and cyberattacks, and the fact that cyberspace is over 80% in the hands of the private sector – provide strong and credible commitments to cooperation because it has become an existential need.

On cyber deterrence, some commentators do not accept the relevance of this concept due to the credibility of the threat of punishment (Arquilla and Ronfeldt, 1996, p. 94) and attribution problems (Clark and Landau, 2010). On the other hand, Rid and Buchanan (2015, p. 7) argue that attribution is "what states make of it", and not a binary relationship. Just as criminal law theory accepts that absolute obedience to the law cannot be guaranteed, the 2017 EU strategy accepts that no ICT product, system or service can be guaranteed to be '100 %' secure and not all cyberattacks can be prevented. Therefore, the goal should not be that of achieving absolute deterrence and unrealistically seeking to prevent all cyberattacks from occurring, but to maintain an effective deterrence posture by strong messages and responses aimed against offenders and thus force aggressors to recalculate their intentions. In short, focus on prevention (Tor, 2017, pp. 94–95). The measures taken in this area by the EU range from technical to legal and political ones; from encouraging the uptake of IPv6(Intern Protocol version 6 (IPv6) is the communications protocol (IP)

that provides an identification and location system for computers on networks and routes traffic across the internet.)

to stepping up the law enforcement and political response, to cooperation with the financial sector and building the cyber defence capabilities of the EU Member States.

A 'Cyber Maastricht', with its Defence & IR pillar, can lead the EU to a breakthrough by becoming more relevant geo-strategically. Cybersecurity is not an isolated policy, but in the context of today's security challenges, a shift to new platforms enabled by current technologies. In the light of setbacks in integration due to Brexit and the mixed messages received from the U.S. on its defence outlook for Europe, a militarized cyberspace is certainly a good reason to aim for as part of the EU's strategic autonomy and security union. An integral part of this militarised cyberspace relies on the EU's cybersecurity efforts. However, as cyber defence is part of the EU's broader cybersecurity policy, it remains unclear how it fits into the concept of "strategic autonomy" (European Commission, 2016a) and defence union – whether or not strategic autonomy includes EU level operational capabilities, and if yes, what kind, and whether or not strategic autonomy means 'independence' for the underlying industry. Although currently there are initiatives to boost operational capabilities of the member states and foster cyber defence innovation in the EU (for example in the framework of PESCO and the European Defence Fund), these actions are more aimed at coordination leaving the EU with the role of an advisory, or at best a coordinator in some areas related to budget and high-level crisis response. While BREXIT may open some doors for deeper integration in cyber defence, some might be perceiving a potentially growing strategic autonomy of the EU and a defence union as undesirable, and damaging to U.S. defence/industrial interests (Fiott, 2018, p. 7). Others advocate executive powers to the EU institutions in cyber defence and the establishment of a Cyber Defence Agency (Griffith, 2018).

Indirectly tilting toward the imperial paradigm, the EU will enhance its cooperation on cybersecurity with the like-minded NATO, and it will have more chances to cooperate with the UN, particularly with the UN GGE, while solidifying 'Capacity Building' mechanisms in the neighbourhood. It will do the same, wherever its 'civilising mission' (e.g. promoting 'Human Rights') leads it to. Defence is not Resilience, but, together with Deterrence, it has a durable common basis, constructed out of the 'Member States Defence Capabilities', the 'EU Crisis Response', and 'Cyber Diplomacy Toolkit in the CFSP'. Once again, in order to build this 'pedestal' for the two pillars, some 'raw material' will need to be supplied by liberal intergovernmentalism, but this is a routine issue, which should start by finding a common definition of EU cybersecurity, clarifying the content for clusters for its overall policy, identifying exogenous and endogenous influencing factors and taking stock of available resources in a systematic manner. In short, should the EU consider converting the model of a 'Cyber Maastricht' into reality, it just needs to make an effort. Time is, unfortunately, running out.

Conclusion

This paper engaged in a comprehensive search for a relevant theoretical concept (or a right mixture of several theories) that best explain integration processes in the EU's cybersecurity governance. We examined both internal and external domains – since the line between these is blurred in cyberspace – with the application of toolboxes provided by neofunctionalism, intergovernmentalism, post-functionalism and the imperial paradigm. The discussion led this research towards creating a schematic model that essentially represents a scholarly call on the necessity for the EU to formulate a 'Cyber Maastricht'. Characteristically for the proposed pillar-based model, it requires almost no 'assistance' from the neo-functional spillover, which has previously helped the EU to realise achievements in the field of political economy, but has not been so effective in the sphere of geo-strategy. Instead, a far more sophisticated combination of integration-driven theories will be needed, and this fact in itself depicts a positive sign for the EU to remain relevant, creative and flexible in its policymaking. This is especially important when it comes to addressing the issue of cybercrime and cyber defence – the alternative, a cumbersome policy on cybersecurity, can quickly push the EU into mediocrity.

References

Arquilla, J, and Ronfeldt, D. (1996) The Advent of Net War. Santa Monica, California: RAND Corporation. Available at: https://www.rand.org/pubs/monograph_reports/MR789.html

Asser Institute (2016) The Tallinn Manual 2.0 and The Hague Process: From Cyber Warfare to Peacetime Regime. Available at: https://www.asser.nl/media/2878/report-on-the-tallinn-manual-20-and-the-hague-process-3-feb-2016.pdf (Accessed: 14 May 2019).

Börzel, T.A. and Risse, T. (2018) 'A Litmus Test for European Integration Theories: Explaining Crises and Comparing Regionalisms', KFG Working Paper No. 85. Available at: https://www.polsoz.fu-berlin.de/en/v/transformeurope/publications/working_paper/wp/wp85/index.html

Bergmann, J. and Niemann, A. (2018) 'From Neo-Functional Peace to a Logic of Spillover in EU External Policy: a Response to Visoka and Doyle', Journal of Common Market Studies, 56 (2), pp. 420–438. Available at: https://internationale.politik.uni-mainz.de/files/2018/11/JCMS_12608_e_%C3%9Cberarbeitung-Sch%C3%B6nbach_AN.pdf

Breland, A. (2018), 'Tech and telecom lobbying groups announce joint cybersecurity initiative', The Hill, 23 February. Available at: https://thehill.com/policy/technology/375287-lobbying-groups-for-tech-and-telecom-announce-joint-cybersecurity

Burton, J. (2018) 'Cyber Deterrence: A Comprehensive Approach?', CCDCOE. Available at: https://ccdcoe.org/uploads/2018/10/BURTON_Cyber_Deterrence_paper_April2018.pdf (Accessed: 14 May 2019).

Christou, G. (2016) Cybersecurity in the European Union – Resilience and Adaptability in Governance Policy,, UK: Palgrave MacMillan.

Clark, D., D., Landau, S., (2010), 'Untangling Attribution', in Proceedings of a workshop on deterring cyberattacks: informing strategies and developing options for U.S. Policy. Washington, DC: The National Academies Press, pp. 25–40. Available at: https://doi.org/10.17226/12997

Commission of the European Communities (2001), Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Network and Information Security: Proposal for a European Policy Approach. Com (2001) 298 Final. Brussels, 6 June. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52001DC0298&from=EN

Commission of the European Communities (2004) COMMUNICATION FROM THE COMMISSION TO THE COUNCIL AND THE EUROPEAN PARLIAMENT – Critical Infrastructure Protection in the fight against terrorism, COM (2004) 702 final of 20.10.2004. Available at: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2004:0702:FIN:EN:PDF

Council of the EU (2001) Proposal of the incoming Spanish Presidency and Europol's initiative for the establishment of a monitoring centre on cyber crime at Europol, Document Nr. 15456/01 of 18 December 2001, Available at: https://data.consilium.europa.eu/doc/document/ST-15456–2001-INIT/en/pdf

Council of the EU (2011), 18 month programme of the Council (1 July 2011–31 December 2012), Document Nr. 11447/11 of 17 June 2011. Available at: https://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2011447%202011%20INIT

Council of the EU (2012), 18 month programme of the Council (1 January 2013–30 June 2014), Nr 17426/12 of 7 December 2012. Available at: https://data.consilium.europa.eu/doc/document/ST-17426–2012-INIT/en/pdf

Council of the EU (2013), Communiqué de presse 3243e session du Conseil Transports, télécommunications et énergie Luxembourg, les 6, 7 et 10 juin 2013, Document Nr. 10457/1/13 REV 1. https://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2010457%202013%20REV%201

Council of the EU (2014a), Outcome of proceedings of the Council 17–18 November. Document Nr. 15585/14. Brussels 18 November. https://fdocuments.in/document/eu-cyber-defence-policy-framework.html

Council of the EU (2014b), 18 month programme of the Council (1 July 2014–31 December 2015, Document Nr. 10948/1/14 REV1 of 17 June 2014. Available at: https://data.consilium.europa.eu/doc/document/ST-10948–2014-REV-1/en/pdf

Council of the EU (2015), Taking forward the Strategic Agenda – 18 month programme of the Council (1 January 2016–30 June 2017), Document Nr. 15258/15 of 11 December 2015. Available at: https://data.consilium.europa.eu/doc/document/ST-15258–2015-INIT/en/pdf

Council of the European Union (2016) Non-paper: Developing a joint EU diplomatic response against coercive cyber operations, Document Nr. 5797/2/16 REV 2 of 16 February 2016. Available at: http://data.consilium.europa.eu/doc/document/ST-5797–2016-REV-2/en/pdf

Council of the EU (2017), Taking Forward the Strategic Agenda of the Council, 18 month programme of the Council, 1 July 2017 to 31 December 2018. Document Nr. 9934/17 of2 June 2017. Available at: https://data.consilium.europa.eu/doc/document/ST-9934–2017-INIT/en/pdf

Council of the EU (2018a), EU Cyber Defence Policy Framework (2018 update). Document Nr. 14413/18 of19 November 2018. Available at: https://data.consilium.europa.eu/doc/document/ST-14413–2018-INIT/en/pdf

Council of the EU (2018b), Data retention: State of Play. Document Nr. 14319/18 of 23 November 2018. Available at: https://data.consilium.europa.eu/doc/document/ST-14319–2018-INIT/en/pdf

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, M. (2018) 'Europe's cyber-power', European Politics and Society, 19(3), pp. 304–320. doi: 10.1080/23745118.2018.1430718.

European Economic and Social Committee (2014) Opinion, 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) 48 final, CESE2013/1414, 22 May 2014.

European Commission, (2006) Commission staff working document – Annex to the Communication from the Commission to the Council, the European Parliament, the European Economic and Social committee and the Committee of the Regions A strategy for a Secure Information Society – "Dialogue, partnership and empowerment" {COM (2006) 251 final} – Impact assessment /* SEC/2006/0656 */, 31 May.

European Commission, (2013) Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace – JOIN (2013) 1 final – 7 February 2013. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52013JC0001

European Commission, (2016a) Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy, June. Available at: http://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf

European Commission (2016b), Joint Communication to the European Parliament and the Council – Joint on countering hybrid threats, a European Union response. JOIN(2016) 18 final of 6.4.2016. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016JC0018&from=en

European Commission (2017), Joint Communication to the European Parliament and the Council (2017), Resilience, Deterrence and Defence: Building strong cybersecurity for the EU. JOIN/2017/0450 final. Document 52017JC0450, Eur-Lex, https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A52017JC0450

European Council (2001), Conclusions of the Presidency. Stockholm 23–24 March. https://www.consilium.europa.eu/media/20994/stockholm-european-council-presidency-conclusions.pdf

European Network and Information Security Agency (2019), ENISA Threat Landscape Report 2018). Available at: https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscap

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

European Parliament and the Council (2019) Regulation (EU) 2019/881 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)

Farwell, J.P and Rohozinski, R. (2011) 'Stuxnet and the Future of Cyber War', Survival, 53(1), pp. 23–40. doi: 10.1080/00396338.2011.555586.

Fiott, D (2018) 'Strategic autonomy: towards 'European sovereignty' in defense?', EUISS Brief, November, 2018. Available at: https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief%2012__Strategic%20Autonomy.pdf.

Griffith, M.K. (2018) 'Strengthening the EU's Cyber Defense Capabilities', Center for European Policy Studies (CEPS), Brussels. Available at: https://www.ceps.eu/wp-content/uploads/2018/11/CEPS_TFR%20on%20Cyber%20Defense_1.pdf. (Accessed: 30 June 2019).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.

Haas, E.B. (1958) The Uniting of Europe: Political, Social and Economic Forces 1950–57. 2nd ed. Stanford: Stanford University Press.

Henriksen, A. (2019) 'The end of the road for the UN GGE process: the future regulation of cyberspace', Journal of Cybersecurity, 5 (1). Available at: https://doi.org/10.1093/cybsec/tyy009 (Accessed: 14 May 2019).

Hermann, M.G. (2008) 'Content Analysis', in Klotz, A. and Prakash, D. (eds) Qualitative methods in international relations: a pluralist guide. Palgrave Macmillan, pp. 151–167.

Hooghe, L. and Marks, G. (2008) 'A Postfunctionalist Theory of European Integration: From Permissive Consensus to Constraining Dissensus', British Journal of Political Science, 39, pp. 1–23 (first published online 27 October 2008), DOI: 10.1017/S0007123408000409

Hooghe, L. and Marks, G. (2019) 'Grand theories of European integration in the twenty-first century', Journal of European Public Policy, 26:8, pp. 1113–33, DOI: 10.1080/13501763.2019.1569711.

ITU Global Cybersecurity Index 2018. Available at: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx (Accessed: 14 May 2019).

Joint Statement on the Launch of EU-U.S. Negotiations to Facilitate Access to Electronic Evidence (2019), EVIDENCE2e-CODEX. Available at: https://evidence2e-codex.eu/a/joint-statement-access-to-electronic-evidence

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.

Kasper, A. and Mölder, H. (2019) 'The EU's Common Security and Defense Policy in facing new security challenges and its impact on cyber defense', in Troitino, D. and Kerikmäe, T. (eds)' The EU in the 21st Century – Challenges and Opportunities for the European Integration Process'. Springer. (Forthcoming)

Kaljurand, M. (2016) 'United Nations Group of Governmental Experts: the Estonian Perspective', in Osula, A.M. and Rõigas, H. (eds) International Cyber Norms: Legal, Policy & Industry Perspectives. Tallinn: NATO CCD COE Publications, Tallinn. Available at: https://ccdcoe.org/library/publications/international-cyber-norms-legal-policy-industry-perspectives/.

Keohane, R. O. (1984) After hegemony: cooperation and discord in the world political economy. NJ: Princeton University Press.

Lotman, J. (2013) The unpredictable workings of culture. Tallinn: Tallinn University Press.

McCormick, M. (2003) 'Questions about functionalism in Kant's philosophy of mind: lessons for cognitive science', Journal of Experimental & Theoretical Artificial Intelligence, 15(2), pp. 255–266. doi: 10.1080/0952813021000055180.

McGowan, L. (2007) 'Theorising European integration: revisiting neofunctionalism and testing its suitability for explaining the development of EC competition policy', European Integration Online Papers. Available at: http://eiop.or.at/eiop/pdf/2007–003.pdf. (Accessed: 1 May 2019).

Mitrany, D. (1975) 'Nationality and nationalism (1938 and early 1950s)', in Taylor, P. (ed.), The functional theory of politics. Bristol, London School of Economics and Political Science: Martin Robertson & Company, pp. 137–145.

Moravcsik, A. (1998) The Choice for Europe. Social Purpose and State Power from Messina to Maastricht. Ithaca, NY: Cornell University Press.

NATO news (2018) NATO and the European Union work together to tackle growing cyber threats. Available at: https://www.nato.int/cps/en/natohq/news_161570.htm?selectedLocale=en (Accessed: 14 May 2019).

Neumann, I.B. (2008). 'Discourse Analysis', in Klotz, A. and Prakash, D. (eds) Qualitative methods in international relations: a pluralist guide. Palgrave Macmillan, pp. 61–77.

Niemann, A. 2016, 'Neofunctionalism and EU External Security Cooperation', in Rhinard, M. and Bossong, R. (eds) Theorising Internal Security Cooperation in the European Union, Oxford University Press, pp. 129–152.

The Telegraph (2019) British Army to engage in social media warfare as new cyber division unveiled'. Available at: https://www.telegraph.co.uk/news/2019/07/31/british-army-engage-social-media-warfare-senior-soldier-announces/ (Accessed: 1 August 2019)

Rid, T. and Buchanan, B. (2015) 'Attributing Cyber Attacks', Journal of Strategic Studies 38(1–2), pp. 4–37.

Renard, T. (2018) 'EU cyber partnerships: assessing the EU strategic partnerships with third countries in the cyber domain', European Politics and Society, 19(3), pp. 321–337. doi: 10.1080/23745118.2018.1430720

Reuters (2018) Czech security service says Russia behind cyber attacks on ministry. Available at: https://www.reuters.com/article/us-czech-security-russia/czech-security-service-says-russia-behind-cyber-attacks-on-ministry-idUSKBN1O21BN (Accessed: 14 May 2019).

Särav, S., Kerikmäe, T., and Kasper, A., 'Az e-polgárság mint a virtuális migráció eszköze Észtországban', Információs Társadalom, XVI. (2016) 2, pp. 8–31. Available at:.http://dx.doi.org/10.22503/inftars.XVI.2016.2.1.

Schimmelfennig, F. (2015) 'Liberal intergovernmentalism and the euro area crisis', Journal of European Public Policy, 22(2), pp. 177–195. doi:10.1080/13501763.2014.994020.

Smith, M.E. (2004) Europe's Foreign and Security Policy. The institutionalisation of cooperation. Cambridge: Cambridge University Press.

Tor, U. (2017) 'Cumulative Deterrence' as a New Paradigm for Cyber Deterrence', Journal of Strategic Studies, 40 (1–2), pp. 92–117. doi: 10.1080/01402390.2015.1115975.

Vernygora, V., Troitiño, D.R, Västra, S. (2016) 'The Eastern Partnership Programme: is pragmatic regional functionalism working for a contemporary political empire?', in Kerikmäe, T. and Chochia, A. (eds) Political and legal perspectives of the EU Eastern Partnership Policy. Springer International Publishing, pp. 7–22.

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