European Journal for Security Research
https://doi.org/10.1007/s41125-019-00053-w

ORIGINAL ARTICLE

An Acid Test for Europeanization: Public Cyber Security Procurement in the European Union

Jukka Ruohonen[1]

Received: 22 May 2019 / Accepted: 28 September 2019

Abstract

Public procurement refers to processes through which national, regional, and local public authorities, state-owned enterprises, or other related bodies governed by public law, purchase products, services, and public work. Such purchases have been a particularly important element in developing the Internal Market of the European Union (EU). Given recent procurement reforms in the EU, including the 2009 reform on defense procurement, this paper examines public cyber security procurement in Europe. Two questions are examined: (1) whether cyber security procurement differs from public procurement in general, and (2) whether there are any noteworthy signs of Europeanization in terms of cyber security procurement. According to the empirical results, cyber security procurement tends to differ from general public procurement. In particular, competition obstacles are visible in terms of bids for cyber security procurement tenders. This result is accompanied with a visible lack of Europeanization, although the same observation generalizes to public procurement in the EU generally. With these results and the accompanying discussion, the paper contributes to the recent lively discussion about European security and its relation to marketization.

Keywords Security industry · Defense industry · Marketization · Tendering · Public–private partnerships · Dual-use technologies · EU · PPP · CSDP

The initial idea about using public procurement data in the cyber security domain is gratefully acknowledged to Riccardo Coluccini and his presentation at the 34th Chaos Communication Congress (34C3) held in Leipzig.

✉ Jukka Ruohonen
juanruo@utu.fi

[1] Department of Future Technologies, University of Turku, Turku, Finland

Published online: 05 October 2019

1 Introduction

Public procurement has been a continuing economic and political issue in Europe during the past 20 or 30 years. There have been also many large reforms for the regulation of public procurement. The public procurement directives were reformed first in 2004 and then again 2014, but particularly noteworthy was the 2009 introduction of a directive for defense procurement—the first supranational legislation in the defense and security domains. Given this background, this paper examines two research questions:

- Question Q_1: Does public procurement of cyber security technologies and services differ from general public procurement in the European Union?
- Question Q_2: Does public cyber security procurement in European Union show any forceful and visible signs of Europeanization?

In addition to the answers provided to these two questions, the paper contributes to the recent blossoming literature on the slow evolution of European security and its relation to marketization (Britz 2010; Calcara 2017; Fiott 2017b; Strikwerda 2017). Much of the existing research is about traditional security and defense, however. The present paper is the first one to examine the topic from a perspective of cyber security. The same applies to procurement research. Even though there is an excellent and extensive literature base on European public procurement (Gelderman et al. 2010; Powell-Turner et al. 2016; Mehrbod and Grilo 2018, among others), thus far, no previous work has been done to examine public cyber security procurement in the EU. What is more, there is precious little empirical social science research on cyber security. While some attempts have been made for improving the situation (Valeriano and Maness 2018), none of the existing empirical state-centric studies on cyber security are convincing. The reason relates partially to the unsolvable problem about reliable and valid data, and partially to the nature of the Internet as a fundamentally non-Westphalian system. However, the present work demonstrates that many relevant cyber security questions can be addressed with traditional means for empirical social science research. Political economy is political economy also in cyber security.

Also the relevance of the paper's topic is easy to justify. Public procurement belongs to the very core of the Internal Market of the European Union. For about four decades, procurement has also been a fundamental policy instrument for establishing the European defense industry and a common European security policy with it. Obviously, many of the security issues faced by Europe have fundamentally changed in the meanwhile. The ongoing digitalization of European societies has made them also more vulnerable. Although cyber crime continues to be an issue, particularly important have been the offensive cyber operations carried out by states against other states. Such operations have made cyber security a matter of national security, and differentiated the concept from more traditional terms such as information security (von Solms and van Niekerk 2013; Zajko 2018). Cyber threats have also required the adoption of risk-based approaches to

public administration (Massacci et al. 2016; OECD 2017). Whether it is procurement or exports, security considerations have become increasingly important for both producers and consumers (Fiott 2017a; Kepe et al. 2018; Trimintzios et al. 2017). A good recent example would be the Russia-based Kaspersky Lab whose products were phased out in 2017 from governmental use in the USA and elsewhere due to concerns about the supplier for national security (Abramova and Garanina 2018). Another example would be the 2019 debate on the deployment of Huawei's 5G technologies in Europe and elsewhere. While both examples may be as much about geopolitics as these may be about cyber security, these are still noteworthy for justifying the relevance of Q_1.

With respect to Question Q_2, it should be further emphasized that cyber security is among the prime examples about so-called public–private partnerships (PPPs), which have recently become an important alternative for traditional procurement practices (Christou 2016; Healey 2017; Hodge and Greve 2017). Therefore, implicitly, an answer to Q_2 is important also for evaluating the potential role played by PPPs in Europeanization. As will be further discussed, these partnerships represent a new type of EU-level public administration that goes far beyond the traditional questions about marketization and Europeanization. When the EU and its member states have attempted to simultaneously tackle new threats and industry competitiveness, they have also entered into another fundamental realm represented by concepts such as democracy and basic rights.

The remainder of the paper proceeds in a straightforward manner. The opening Sect. 2 outlines the background, discussing the paper's theoretical framing as well as the relevant public procurement legislation in the EU. Three hypotheses are also presented for motivating the two research questions. The subsequent Sect. 3 presents the empirical evaluation of the hypotheses presented and the two questions asked. The final Sect. 4 discusses the answers reached.

2 Background

2.1 Theoretical Framing

There are many theoretical continua for framing the current European security landscape. The nexus between external and internal security is one of these. Many of the security threats Europe is facing neither respect the geopolitical boundaries of nation states and the EU nor fit clearly into institutional boundaries. The blurring of boundaries between external and internal security has mixed also the traditional institutional security arrangements and their boundaries. Law enforcement and administrative authorities have long had to consider also external security challenges, while at the same time, internal security issues have become increasingly important for military, defense, foreign policy, diplomacy, and other institutions traditionally responsible for external security (Burgess 2009). While terrorism is a good example, cyber security is arguably a better one; like the Internet, cyber security does not respect borders.

The development of coherent supranational policies and institutions that merge external and internal security has long been an explicit goal in the EU. This broad strategy applies also to cyber security. Although a thorough discussion about recent cyber security developments in the EU is beyond the scope of the present work, a concise but reasonable summary from the literature is that there has been a certain degree of convergence on one hand, and a continuing lack of coherence on the other (Carrapico and Barrinha 2017; Christou 2016; Pawlak 2019; Ruohonen et al. 2016). This summary generalizes to the post-war history of European security in general (Eriksson and Rhinard 2009; Howorth 2019). External, internal, convergence, and coherence are decent theoretical concepts for analyzing the institutional, policy, coordination, and governance developments of the EU's cyber security strategies. But by no means, these are the only available theoretical concepts.

In this paper, cyber security is explicitly framed with two continua: public–private and civilian–military. These can be defined as theoretical abstractions that represent themselves through two truncated continuous variables. In other words, cyber security is not a dichotomous concept. The term truncation is used to emphasize that none of the endpoints (civilian, military, public, and private) can be fully reached theoretically. The civilian side is present even when cyber security is understood as a military concept—as is typical in the cyber warfare, cyber defense, and related discourses. None of "the new threats to Europe are entirely military, nor can be addressed by entirely military means" (Burgess 2009, p. 322). Recent policy documents also emphasize the necessity to cooperate with civilian actors in order to improve the EU's defense and security capabilities (Kepe et al. 2018). What is often left unsaid are the politics of cooperation; what kind of institutions and regulations are enacted; to which areas and for whom public EU funds are allocated and under which conditions; and so forth.

By following the so-called framing theory (Drake and Donohue 1996), the political placement of cyber security toward the military or civilian endpoint, as well as toward the private or public endpoint, can be thus seen as a continuous negotiation and bargaining process. There are often legal, social, political, economic, and technical ramifications from a given placement resulting from a given bargaining process. The framing applies also to academic research. For instance, criticism has long been expressed about state-centric approaches to cyber security (van Eeten 2017), which tend to lean toward the military endpoint due to their heavy emphasis on foreign policy, international relations, and traditional security and defense. On the other hand, according to critics, research on European security has often overemphasized the supranational level at the expense of the national level (Meijer and Wyss 2018; see also Howorth 2019). These two scholarly examples serve to underline that a given theoretical viewpoint implicitly or explicitly affects the corresponding framing of the European cyber security landscape. From a political economy viewpoint, framing done on the public–private continuum is relevant for better understanding the civilian–military continuum. This framing is also an inherent part of procurement.

A brief elaboration of European security in general is required in order to frame the question about public cyber security procurement. Thus, to begin with, the EU is still a civilian project in its normative underpinnings. From this perspective, the EU's power originates from norms and values that include the

rejection of divisive nationalism and the avoidance of Europe's militaristic history (Burgess 2009; Ladi and Tsarouhas 2017). While normative power does not equate directly to civilian power, the concept is still closer to the left endpoint in the civilian–military continuum. On the side of the other endpoint, Europe's post-war power has relied on both sovereign states and the North Atlantic Treaty Organization (NATO). However, the failure to prevent the war in the former Yugoslavia brought the impetus for a common European defense policy. In this setting, convergence is often framed with the term Europeanization, which—at least in the present use—is distinct from the older concept of European integration. In essence, Europeanization is about increasing interaction between European and domestic policies (Britz 2010). After alternating periods of acceleration and gridlocks, such increasing interaction led to the first "NATO-compatible but politically autonomous European crisis management apparatus" (Mérand 2006, p. 135). The apparatus later evolved into the current Common Security and Defence Policy (CSDP) signed with the Treaty of Lisbon in 2007.

However, the Europeanization of defense has been more about marketization than European security itself. While the liberalization of the European defense industry largely occurred already in the 1980s (Hartley et al. 2008), the drive toward the EU-level started in the 1990s and continued throughout the 2000s. The developments were pushed forward particularly by France and the French military establishment, which is understandable because historically France was less tightly integrated into the NATO compared to Germany and the United Kingdom (Mérand 2006; Rieker 2006). Here, integration refers particularly to the defense industry, and, indeed, also France's later pro-active strategy has partially originated from the needs of its national defense industry (Calcara 2017; Fiott 2017a). In this sense, the EU-level was a facilitating medium for the establishment of European defense industry relations, while the marketization itself was largely driven by national interests. It is possible to interpret this historical background by stating that marketization was in fact a precondition for the slow but still visible Europeanization of security and defense (Britz 2010). This precondition is suitable also for approaching the potential Europeanization through public cyber security procurement. In terms of framing on the public–private continuum, the corresponding Premise P_1 for Q_2 is illustrated in Fig. 1.

Defense procurement has been a fundamental puzzle in the European marketization trend. Although EU-wide public procurement continues to face substantial problems in all economic sectors (Gelderman et al. 2010; OECD 2017), it is the civilian side on which procurement has been more prevalent. That said, it must be stressed that also defense procurement has been widespread in Europe, albeit often under different joint ventures and their monopolistic arrangements (Hartley et al. 2008). Even when keeping in mind the recent demands from the USA for the European NATO member states to increase their defense spending, the illustration in Fig. 2 is thus sufficient for pointing out the substantial amount of money already involved in the defense and security procurement in the EU member states. The EU-NATO conundrum, Brexit, and new threats and geopolitical concerns have also pushed the CSDP forward in recent years. Particularly noteworthy was the 2017 establishment of the so-called Permanent Structured

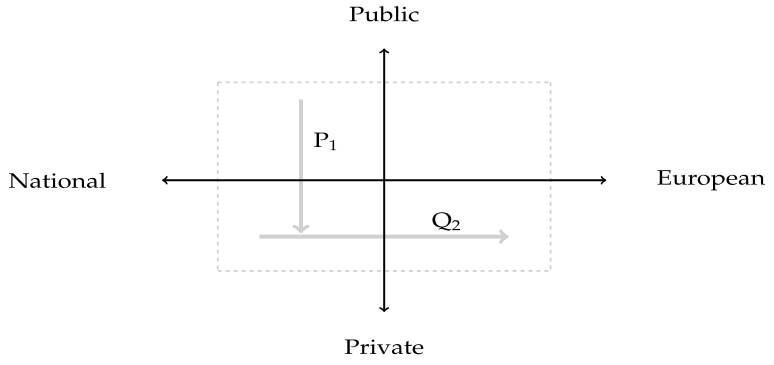

Fig. 1 A premise for the Europeanization of (cyber) security procurement

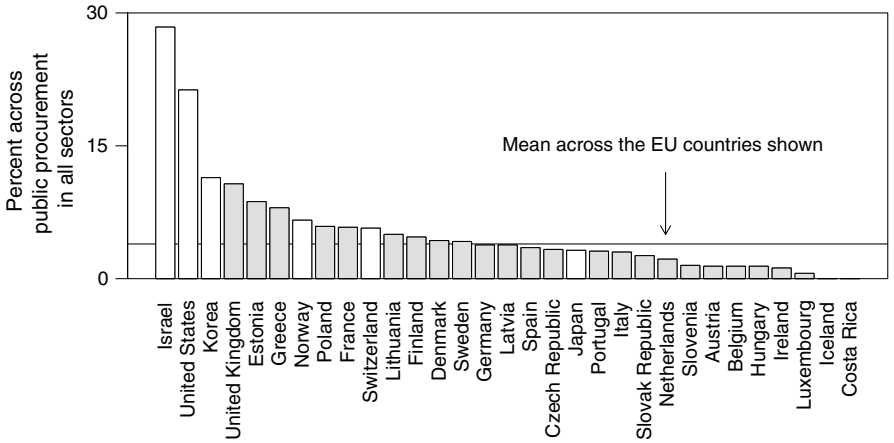

Fig. 2 Relative share of public procurement in the defense sector in selected countries in 2015 [based on OECD (2017), Table 9.2, p. 173]

Cooperation (PESCO) framework and the European Defence Fund (EDF). In general, the rationale behind these was to incentivize cooperation, reduce duplication, foster innovation, level the field for smaller companies, improve interoperability, and rationalize procurement practices. As always with the CSDP, the actual impact of PESCO/EDF upon European security and defense is under a debate. Although many observers have expressed skepticism (Howorth 2019; Meijer and Wyss 2018; Nováky 2018), the political impact upon defense procurement has already been visible. In particular and somewhat paradoxically, in 2019, the USA expressed a concern that the new framework would increase protectionism within the EU's defense industry—despite the demand to increase defense spending and the great defense trade imbalance in favor of the USA (Fiott 2019). To some extent, rather analogous political and economic controversies have been seen in the cyber security domain.

On the surface, also seemingly similar market-driven Europeanization has occurred in the cyber security domain. To a certain degree, there has been a split between military approaches to European cyber security, which are exercised largely through the NATO like in defense and conventional security (Robinson and Slack 2019), and civilian cyber security exercised through separate institutions and policies (Ruohonen et al. 2016). There are also efforts to marry the CSDP with cyber security (Trimintzios et al. 2017). When scratching the surface, however, this interpretation is incorrect; the European cyber security landscape cannot be strictly equated to the European defense and traditional security. While there are several reasons for this claim, the role of the private sector is especially important for the present purposes. As a part of the information and communication technology (ICT) sector, the relatively new cyber security industry has never been characterized by state-owned enterprises or related close ties to the public sector. In contrast to the defense industry, the cyber security industry has also long operated in more or less open international markets.

The dominant role of the private sector is also reflected in the EU's cyber security regulations and strategies. If cyber crime, terrorism, privacy, and some related policy domains are excluded, the union's current rationale seems to indeed largely center on the idea that the EU institutions and national public authorities provide loose oversight, while the actual day-to-day cyber security is left for the private sector (Christou 2016, pp. 121–131). This rationale reflects the EU's traditional soft power; the goal has been to empower the private sector through dialogue and partnerships (Carrapico and Farrand 2017). While the CSDP has always carried its own peculiar European flavor (Howorth 2019), it should be emphasized that this cyber security rationale is hardly unique to Europe. In other words, information sharing, private sector partnerships, and related policy goals for cyber security are commonly shared among public authorities in Europe and elsewhere (Healey 2017; Kuerbis and Badiei 2017). These strategies are important also for the framing of cyber security procurement. With respect to ICT, the public sector has traditionally been more of a consumer than a strategic actor using procurement as a policy instrument for specific goals. This consumer-like role marks another difference to traditional security and defense within which strategic leeway has always been used widely. It would also allow to expect a negative answer to Q_1. To counter this expectation, it is necessary to consider the framing on the civilian–military continuum.

Although cyber security continues to be primarily a civilian matter, there has been a visible propel toward the military endpoint in recent years. Before continuing any further, however, it should be emphasized that the framing of cyber security as a military affair is coupled with a fair share of politics and exaggerations; cyber security is hardly an "existential challenge for national security," as claimed by some observers (Pawlak 2019, p. 174). "Remarkably little has changed in the past decade, with one important exception: offensive operations by nation states" (van Eeten 2017, p. 430). This offensive side is important already because investments to cyber security have partially and paradoxically increased also cyber insecurity. Also the recent international efforts to regulate the offensive side of cyber (in)security through multilateral venues have faced problems (Ruohonen and Kimppa 2019; Stevens 2017). The same could be said about traditional multilateral venues in general;

actual day-to-day cyber security governance continues to occur through different non-hierarchical, non-state, or market-based forms of hybrid governance (Kuerbis and Badiei 2017). These points restate the criticism about state-centric approaches to cyber security. However, what is often overlooked in this criticism is the political economy of cyber security; states and their supranational unions do have a great influence on cyber security already through their power to redistribute economic resources.

The increased cyber insecurity partially caused by states themselves allow to reverse the expected answer to Q_1. In other words, it seems sensible to assume that public authorities use scrutiny when purchasing cyber security technologies and services due to the increased supply-side risks and other related threats.

A final important point is that the political economy viewpoint adopted and the observable political framing toward the military endpoint reveal also parallels to the CSDP and the European defense industry. Many cyber security technologies are inherently also dual-use technologies; they are primarily civilian in their nature, but they can be also used to enhance military capabilities.[1] A parallel to traditional security and defense is therefore apparent: the dual-use concept was important already during the 1980s liberalization—and like today, it was seen as a crucial vehicle for fostering research and development (R&D) and improving cost-efficiency (van Scherpenberg 1997). The concept was also a significant element in the 1990s efforts to establish a common European defense market (Calcara 2017). This time-honored trend has continued to the 2010s. Indeed, numerous recent policy documents in the EU explicitly stress that integration should be improved for R&D programmes that have a dual-use dimension (Kepe et al. 2018; Trimintzios et al. 2017). These programmes cover cyber security. It is also important to underline that the EU-funded (cyber) security programmes are administrated primarily through PPPs. Therefore, it seems sensible to expect a negative answer to Question Q_2. If there has been Europeanization through marketization in the cyber security domain, it can be expected that public procurement has not been the primary policy instrument for the increasing interaction between the member states and their cyber security industries. A brief look at the procurement regulations in the EU can be used to formalize the discussed prior expectations for the two questions examined.

2.2 Procurement Regulations

The history of public procurement directives in the European Union traces all the way back to the 1970s. While the early directives were largely ignored in practice, intense regulatory work started in the mid 1980s and resulted in Directive 2004/18/EC under which all potential but willing suppliers must be invited to tender (Gelderman et al. 2010). This directive was further replaced in 2014 with a package of new directives. In practice, already the 2004 directive covered large portions of public

[1] See Regulation 428/2009 and the amending Regulation 2018/1922.

work, supply, and service contracts, irrespective of an economic sector. Yet, defense contracts were excluded.

The famous Article 346 of the Treaty for the Functioning of the European Union (TFEU) has been at the heart of the crux about defense procurement.[2] According to this article, the member states are not obliged to disclose any information they consider contrary to their essential security interests. This article has long provided the fundamental legal basis for shielding the European defense and security industries from competition with different protectionist measures (Markowski and Wylie 2007; Strikwerda 2017). From a regulatory perspective, the conceptual vagueness of Article 346 has been a large part of the problem. As there is no commonly agreed definition on what constitutes essential security interests, the member states have used the exemption provided liberally (Powell-Turner et al. 2016). In particular, large defense contracts and acquisitions were therefore often pushed to outside of the Internal Market. For instance, in the early 2000s, about four-fifths of the total value of defense equipment procurement in the EU was exempted through the article (Hartley et al. 2008). To overcome these long-standing market imperfections, Directives 2009/43/EC and 2009/81/EC were introduced and enforced for further increasing the liberalization of the European defense industry.

In particular, the intensely debated Directive 2009/81/EC on defense procurement has supposedly made it more difficult to use traditional means for national favoritism and bilateral counter-trade agreements. While it has been suspected that the use of Article 346 may indeed be increasingly difficult nowadays (Fevolden and Tvetbråten 2016; Kennedy-Loest and Pourbaix 2010; Strikwerda 2017), there are numerous visible traits that warrant skepticism about the true extent of liberalization. For instance, the defense procurement directive carries an explicit protectionist trait in that large bids originating from outside of the EU can be rejected (Ladi and Tsarouhas 2017). Empirical observations also point out that participation from outside of the union has remained limited for public procurement in general (Pîrvu and Bâldan 2014). A further point is that 2009/81/EC excludes government-to-government contracts for military equipment, as well as cases whereby public procurement occurs through international organizations, including NATO in particular (Fiott 2017b). Finally, the defense procurement directive also explicitly allows the use of the TFEU's Article 346. Anything and everything related to essential security interests are thus still potentially exempted.

This brief regulatory background can be used to state three explicit hypotheses for the two Questions Q_1 and Q_2. These hypotheses are analytically illustrated in Fig. 3. The first Hypothesis H_1 states that cyber security procurement is closer to the defense procurement directives, and therefore differs from public procurement in general (Q_1). The Hypothesis H_2 assumes that Europeanization has occurred for procurement in general, whereas H_3 states the opposite for cyber security procurement due to the positive answer expected for $H_1 \mapsto Q_1$.

[2] The same article was formerly known as Article 296 of the Treaty establishing the European Community (TEC).

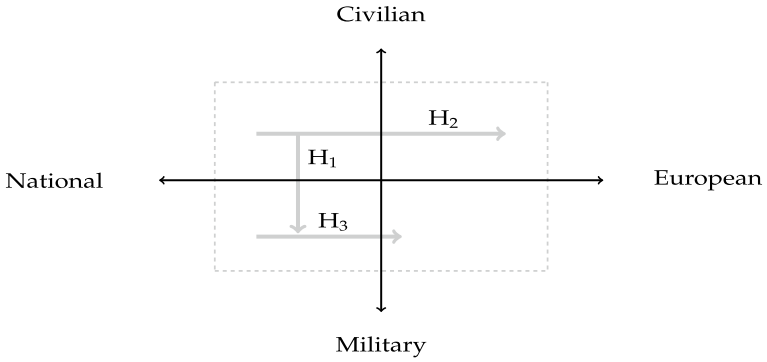

Fig. 3 Three hypotheses for cyber security procurement

However, the hypothesized framing toward the defense procurement directives (H_1) is not entirely straightforward. If cyber security is framed toward the military endpoint instead of the civilian one, also 2009/81/EC should apply together with its exemptions. These exemptions would support also H_3. If the focus is on the civilian endpoint, the direction points toward the more encompassing directives. Given that procurement has been much more widespread on the civilian side (OECD 2017), this framing might allow to expect Europeanization for both cyber security procurement and procurement in general; H_2 would be supported and H_3 would be rejected. This reasoning is not without theoretical and legal caveats, however. The procurement of non-sensitive and non-military items is mainly covered by Directive 2004/18/EC and its successor 2014/24/EU, which, interestingly, are both also subject to Article 346 and its exemptions (Powell-Turner et al. 2016).[3] Therefore, even for essential civilian cyber security technologies and services, it is possible that these exemptions are used because some (civilian) cyber security technologies and services are as sensitive as those covered in the defense Directive 2009/81/EC. For instance, a procurement of a supervisory control and data acquisition (SCADA) system for a nuclear power plant may well-justify the use of Article 346, while purchasing a similar system in some other sector may not.

Additional complexity is added by Directive 2014/23/EU on concession contracts and Directive 2014/25/EU on procurement in water, energy, transport, and postal services sectors.[4] In particular, the transport and energy sectors have long been seen by most European governments as essential parts of the so-called critical infrastructure that should be protected from cyber threats. Innovations such as smart grid systems have further increased the importance of cyber security in these areas (Massacci et al. 2016). Unfortunately, like most definitions in the cyber security domain, the concept of critical infrastructure is open-ended and rather vague. The vagueness applies also to Directive 2008/114/EC that attempted to clarify the

[3] See Article 15 in Directive 2014/24/EU.

[4] Directive 2014/25/EU replaced the earlier Directive 2004/17/EC.

legal definition for critical infrastructure in the EU jurisdiction (EC 2019; Harašta 2018). Like most procurement controversies in the EU, the interpretation details are best left to be resolved in future court cases—and, indeed, questions related to Article 346 and critical infrastructure provide a particularly vexing case for the EU's Court of Justice. In addition to such potential legal issues, the concept is important theoretically. Due to the privatization and deregulation from the 1980s onward, the European critical infrastructures are largely owned and operated by the private sector. Also the expertise to protect these from cyber threats continues to be located primarily in the private sector. This critical role of the private sector for protecting the European critical infrastructures has also strengthened the civilian side in the EU's policy frameworks for cyber security (Carrapico and Farrand 2017). While bringing the military side to the policy mixture has caused its own set of problems, another problem set is located in the public–private continuum. In other words, critical infrastructure and related concepts have necessitated new forms of coordination and collaboration between the public and private sectors.

It is therefore necessary to point out an important further loophole. By and large, R&D and the associated innovation-driven PPPs are largely excluded from the procurement directives.[5] In addition to the inefficiency and other problems associated with procurement through PPPs (ECA 2018), auxiliary R&D support for national companies has been a typical way for European states to protect their defense industries and enhance their military capabilities (Blom et al. 2013; Fevolden and Tvetbråten 2016). The point about R&D is particularly important because cyber security is largely about research and development. Furthermore, it is precisely R&D and PPPs through which EU funds have been allocated for different (cyber) security projects, including those that were present in the large-scale FP7 program and those that are present in the ongoing Horizon 2020 program (Martins and Küsters 2019; Statewatch 2017). These funding schemes have brought new policy complexities due to the sensitive linkage between the civilian nature of most EU-funded cyber security projects and the traditional defense R&D, including the funding and collaboration through NATO's programs (Fiott 2017b; Robinson and Slack 2019). Given that concerns about the Horizon 2020 program's relation to dual-use technologies and associated ethical issues have been reported also in media (Campbell 2019), the new funding opportunities through the PESCO/EDF framework may also help at sharpening the required policy boundaries for civilian and military cyber security R&D.

Regarding the forthcoming empirical analysis, R&D and PPPs are important to emphasize because these further strengthen P_1 in Fig. 1 and H_3 in Fig. 3. In other words, the partnerships have brought a new policy instrument for fostering the long-standing marketization trend, whereas the regulatory framework for traditional public procurement still contains plenty of explicit exemptions and implicit loopholes that presumably undermine Europeanization through this particular policy instrument. As will be elaborated, different security considerations are also spelled out in

[5] See Article 13 in Directive 2009/81/EC, Article 16 in Directive 2004/18/EC, and Article 14 in Directive 2014/24/EU for the exemptions regarding R&D.

the procurement directives, whereas such explicit considerations are largely missing for PPPs. These strengthen also the basis for H_1.

3 Empirical Insights

3.1 Data

The data analyzed is based on the Tenders Electronic Daily (TED) database (EU 2018). This database archives all procurement notices in the European Union, regardless whether these are voluntary announcements or mandatory reports. Following previous research on selecting domain-specific subsets (Nielsen and Hansen 2001), cyber security procurement was probed by using the so-called Common Procurement Vocabulary (CPV) identifiers.[6] The particular identifiers used are enumerated in Table 1. These can be grouped into four broad categories: software security, electronic military systems, anti-virus solutions, and surveillance systems. Therefore, both endpoints are covered in the civilian–military continuum. Although the coverage is hardly perfect, these four categories should provide a reasonable probe into the typical cyber security technologies and services purchased by European public sector authorities. Sampling of cases from the TED database is also constrained by many practical issues. Five such issues are worth briefly discussing.

First, some categories had to be excluded due to a too broad coverage. For instance, the CPVs for security services (such as 79700000-1 and 79710000-4) are too broad for cyber security, containing physical guarding, patrolling, and related services. Second, it should be stressed that most entries in the TED database are accompanied with multiple CPV codes. If a public authority purchased a large information system, which crossed the EU-level reporting thresholds and contained security-specific software development (as captured by the 72212730-5 identifier), it is included in the sampling irrespective of the primary application domain of the system. Incorrect allocation of CPV identifiers is also a possibility in such scenarios (Varney 2011). Third, it remains unclear how accurate the reported monetary amounts are. As currency conversions would be further required for an EU-level analysis, all monetary aspects were bypassed in the sampling; the dataset analyzed covers both small and large public purchases.[7] Fourth, it can be remarked that the natural language descriptions are delivered in the TED database in multiple European languages with incomplete translations. This delivery largely prevents the use of more sophisticated sampling solutions proposed in the literature (Alvarez-Rodríguez et al. 2014; Mehrbod and Grilo 2018). Last, the sampling was restricted to a period between January 2011 and July 2018 during which the data were retrieved.

[6] These are specified in the Commission's Regulation 213/2008.

[7] The EU-level reporting thresholds do not vary much between the directives. Article 8 in Directive 2009/81/EC specifies a little over four hundred thousand euros for supply and service contracts and roughly about five million euros for works contracts. These amounts are comparable in magnitude to those specified in Articles 7 and 4 in Directives 2004/18/EC and 2014/24/EU, respectively.

Table 1 CPV codes for the cyber security sample

Code	Description
48730000-4	Security software package
48731000-1	File security software package
48732000-8	Data security software package
66131000-7	Security brokerage services
72212730-5	Security software development services
72212731-2	File security software development services
72212732-9	Data security software development services
35700000-1	Military electronic systems
50660000-9	Repair and maintenance services of military electronic systems
72231000-3	Development of software for military applications
73436000-7	Test and evaluation of military electronic systems
48761000-0	Anti-virus software package
72212760-4	Virus protection software development services
72212761-1	Anti-virus software development services
32235000-9	Closed-circuit surveillance system
32323500-8	Video surveillance system
32441100-7	Telemetry surveillance system
35720000-7	Intelligence, surveillance, target acquisition and reconnaissance

This restriction is a practical necessity for robust parsing of the raw data because the abstract data structures used in the TED database are not consistent across full historical records; a consistent format is provided only from 2011 onward.

The last points warrant a further comment. The period observed is also the period during which implementations of the large 2014 procurement restructuring occurred in the European Union. (The national implementation deadline for the restructuring was in 2016.) In addition to the interpretation problems with respect to cyber security, the restructuring complicates the empirical analysis because also historical regulations are covered. By implication, the period prevents intervention-style (cf. Siponen and Baskerville 2018) policy analysis regarding the empirical effects of some particular directives upon public procurement.

Instead of a longitudinal comparative setup, Question Q_1 is therefore approached by comparing the cyber security procurement to a random sample covering five percent of all entries in the TED database during the period observed. As there were about 3.5 million entries in the database for this time interval, the random sampling amounted to about 170 thousand procurement cases. Further data manipulation was required because many of these cases dealt with different procurement notices, including the worldwide submission of tendering calls to the TED database. To exclude such cases, the cyber security and random samples were both restricted to actual contract awards, contract award notices, and voluntary *ex ante* transparency notices about contracts sent by public authorities in the EU member states.

On the one hand, this restriction reduced the sample sizes considerably: only 1207 and 29,234 cases are included in the cyber security and random samples observed, respectively. On the other hand, this restriction provides a much sharper picture to the cyber security procurement in the EU because only contracts dealing with actual monetary transactions are covered.

For seeking an answer to $\{H_2, H_3\} \mapsto Q_2$, the two samples were further manipulated by making two additional subsamples that include only contracts for which details were available for both the contracting public authorities and the contracted companies. Given these two subsamples, three (social) networks were constructed based on these contracting bodies as well as their geographic locations in terms of countries and towns. All three network types constructed are directed and weighted. For instance, if a French public authority located in Marseilles would have made two contracts with a company located in Paris, an edge with a weight of two would be placed from Marseilles to Paris in the town-based network. In the country-based network, this placement would amount to a corresponding weighted edge from France back to France. But if a public authority located in Copenhagen would have made a single contract with the same company located in Paris, there would be an edge with a weight of one from Copenhagen to Paris in the town-based network, a similar edge from Denmark to France in the country network, and an edge in the network based on the actual contracting bodies. The edge weights specified are also cumulative: if another Danish public authority would have further contracted a French company, the edge weight would increase to two in the country-based network, and so forth. As has been elaborated previously (Mérand et al. 2010), this relational network abstraction provides a powerful technique for observing the extent of Europeanization. The underlying hypothesis is simple: the traditional bastions of national security and their use of Article 346 should manifest themselves through a visible lack of cross-border European cyber security procurement contracts. Before examining this Hypothesis H_3 and Question Q_2 more generally, an answer is sought to $H_1 \mapsto Q_1$ with a few descriptive statistics on the contractual and structural characteristics of the public procurement contracts observed.

3.2 Contractual Characteristics

The procurement systems in most European countries span the whole range of public administration, from the central government and other national institutions to regional administration and local public authorities. To increase efficiency, transparency, and accountability, many governments have recently centralized the administration of public procurement to common national institutions. This worldwide centralization trend applies particularly to contracting activities and information systems, whereas the implementation details are often still left to decentralized public sector units (Keränen 2017; Meehan et al. 2016). In a similar vein, focus at the EU-level has been on the so-called e-procurement systems, which are believed to improve efficiency and transparency, foster innovation, and level the playing field for small- and medium-sized companies (Khorana et al. 2015; Obwegeser and Müller 2018; Varney 2011). Regardless of the administration and technical systems, public

Table 2 Authority and contract award types (% across a given sample)

	Cyber security	Random sample
Authority types		
EU institution	0.1	< 0.1
National institution	24.4	13.9
Regional or local institution	32.8	34.8
Others, undefined, not applicable, etc.	42.7	51.3
Contract award types		
Lowest price	32.6	39.3
The most economic tender	58.5	51.9
Undefined, not applicable, etc.	8.9	8.8

procurement regulations in the EU apply practically to all organizational units covered by public law.[8] This broad coverage offers a good way to start the dissemination of the empirical results.

Thus, the first panel in Table 2 shows a re-coded breakdown according to the type of the contracting public authorities. There are a couple of points worth making from the numbers shown. The first point is that the random sample aligns rather well with national datasets regarding the relatively small share of contracts made by ministries and other central government units (Gori et al. 2017). Most of the procurement contracts are made by public units operating at regional and local levels. The second point is that cyber security seems to indicate a small exception from this overall conclusion. While the sample covers many contracts made by local authorities (such as video surveillance systems purchased by local law enforcement units), it seems that cyber security contracting tends to be located on higher levels of public administration than contracting in general. If the focus would be extended to defense contracts and traditional national security aspects, the effect would be presumably even stronger.

The type of a contracting authority makes no difference on how a contract is awarded. The EU regulations specify that contracts can be awarded by two main criteria: according to the so-called "most economically advantageous tender" (MEAT) and the lowest price.[9] As shown in the second panel in Table 2, the latter has been slightly more common for the public procurement of cyber security technologies, services, and works. A possible explanation relates to the many exemptions available with the MEAT criterion. Even though both criteria should ensure compliance with respect to transparency, indiscrimination, equal treatment, and related ideals, the MEAT criterion allows specifying many factors other than price for the contract

[8] See Article 1(9) in Directive 2004/18/EC, as referenced also in Article 1 of Directive 2009/81/EC. Article 2 in the new Directive 2014/24/EU is much more explicit, but the fundamental message remains the same.

[9] While Article 53 in Directive 2004/18/EC mentions the lowest price criterion explicitly, Article 67 in the new Directive 2014/24/EU leans generally toward the MEAT criterion.

awards. These cover everything from cost-effectiveness, running costs, quality, and technical merit to environmental considerations and even aesthetic factors.

Thus, the room for maneuvering is generally wide. The wiggle room is even wider for defense and security contracts (Masson et al. 2015; Kennedy-Loest and Pourbaix 2010). In particular, the EU regulations allow numerous exemptions in terms of the security of information and security of supply.[10] Together these cover requirements regarding the confidentiality of potentially classified information, certifications, export controls, technical specifications, and generally the technical competency of whole supply chains.[11] The details are largely specified in national laws. For instance, the EU-level harmonization is limited for the treatment of classified information (Gleeson and Walde 2016). The same applies with respect to the details for evaluating the security and trustworthiness of suppliers. National laws may also strengthen the indirect oversight role of central governments in the cyber security domain. After all, security clearances and other evaluations are done by organizations operating at national levels.

Be that as it may, the share of lowest price tendering is large enough in both samples to also warrant the commonplace concern about schedule and budget overruns typically associated with this particular way of awarding contracts (Regan et al. 2011). In this regard, cyber security technologies do not mark an exception from ICT in general. Given that procurement of these technologies is particularly difficult with respect to requirements, the exemptions provided can be seen also in positive light (Moe et al. 2017). Barriers for competition would be the obvious drawback. A lack of competition in European cyber security procurement becomes also evident by taking a look at a few key structural characteristics of the contracts observed.

3.3 Structural Characteristics

A few important observations can be made about the structural characteristics of the procurement contracts sampled. The four plots presented in Fig. 4 provide a succinct basis for the observations. The first plot shows a (complementary) empirical cumulative distribution function (ECDF) for the number of CPV categories used in the contracts. The rationale behind the plot is similar to that sometimes used in patenting research; a patent classified into many categories may denote a particularly innovative or encompassing technology (Ayres 1994; van der Pol and Rameshkoumar 2017). Given the boundary spanning nature of cyber security, many of the contracts in this domain could be expected to span also many CPV categories. According to

[10] See Article 47 in Directive 2009/81/EC, which is more encompassing than Article 53 in Directive 2004/18/EC. Definition 31 in Directive 2004/18/EC and Definition 42 in Directive 2014/24/EU allow to also use flexible arrangements for complex projects, including those related to transport infrastructure and large computer networks. Qualitative observations and theoretical arguments (Keränen 2017; Meehan et al. 2016; Moe et al. 2017) also bespeak for such arrangements particularly with respect to software projects.

[11] See Articles 22 and 23 in Directive 2009/81/EC.

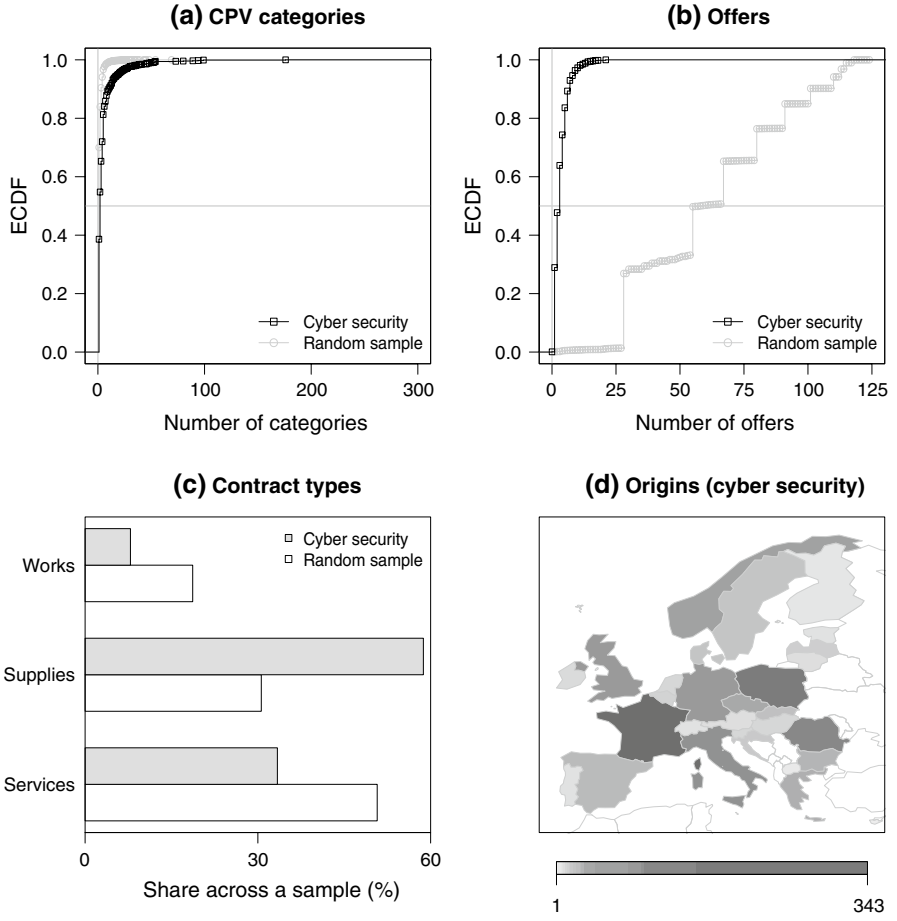

Fig. 4 Descriptive statistics

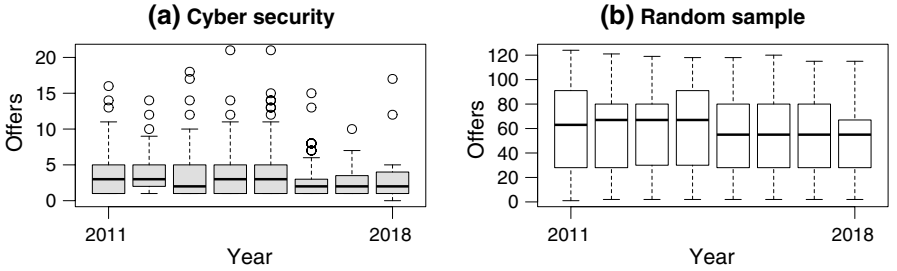

Fig. 5 Number of offers in annual subsets

Table 3 Network characteristics

	Cyber security	Random sample
Network density (unweighted)		
Countries	0.0534	0.0612
Towns	0.0011	0.0002
Contracting bodies	0.0006	< 0.0001
Share of weighted self-loop edges (%)		
Countries	94.56	94.32
Towns	20.96	15.41
Contracting bodies	0.00	0.03

the results, this reasoning does not hold ground, however. No notable visual difference exists between the two samples.

In contrast, the second plot shows a substantial difference between the two samples with respect to the number of offers received for the procurement contracts. The median number of offers (which is represented by the value 0.5 on the *y*-axis) is 59 in the random sample and as low as three in the cyber security sample. About 29% of the cyber security contracts have received just one offer. This number is comparable to those reported for defense procurement (Masson et al. 2015). As can be further concluded from Fig. 5, the situation has not improved during the period observed. These observations are somewhat alarming.

In fact, procurement contracts with a single bidder or a few bidders are often interpreted as signs about competition imperfections—or even as red flags for the potential presence of outright corruption (Fazekas et al. 2016; Flynn 2018). Although the data does not allow to go beyond speculation, a possible explanation may again relate to the MEAT criterion and related flexible arrangements: the availability of lax exemptions may allow the contracting public authorities to specify overly strict requirements that only a single predefined contractor is able to fulfill.[12] In addition to such unreasonable requirements, the usual concerns apply with respect to splitting contracts into smaller pieces in order to avoid crossing the EU-level thresholds, manipulating assessment criteria, using accelerated procedures, allowing late submissions, and sending early notifications to specific national, regional, or local suppliers (Gelderman et al. 2010; Graycar 2019; Obermann and Kostal 2003; Nielsen and Hansen 2001). Whatever the actual reasons may be, the results presented are enough to conclude that competition does not seem to be working at an optimal level in the EU with respect to public cyber security procurement.

The third plot in Fig. 4 shows a basic categorization according to the content type of the contracts. The random sample is in line with previous observations; service

[12] The flexible arrangements allow to also explicitly limit the number of suitable candidates invited to tendering; see Article 38(3) in Directive 2009/81/EC and Article 44(3) in 2004/18/EC. While Articles 28, 29, 30, and 31 in the new Directive 2014/24/EU have clarified these exemptions related to the flexible arrangements, *ex ante* limiting the number of candidates is still allowed.

Table 4 Weighted degree correlations

	Cyber security	Random sample
With self-loops		
Countries	0.996	0.998
Towns	0.545	0.813
Contracting bodies	− 0.172	− 0.084
Without self-loops		
Countries	− 0.019	0.416
Towns	− 0.028	0.651
Contracting bodies	− 0.172	− 0.084

contracts have been more common than contracts for supplies, which, in turn, have been more common than works contracts (Pîrvu and Bâldan 2014). There are also differences between the two samples; contracts for supplies cover nearly 60% of all contracts in the cyber security sample. The reason may relate to the sampling strategy; many of the categories in Table 1 cover hardware as well as software. The weight of supplies would be presumably even more pronounced in traditional defense contracts that cover military equipment from weapons and munitions to fighter aircraft.

Finally, the fourth plot in Fig. 4 illustrates the geographic locations of the countries from which the contract data was filed to the TED database. While these locations may not correspond with the locations of the contracting public authorities or the contracted bodies, the illustration hints that particularly French public authorities have been active in cyber security procurement. A little surprisingly, procurement contracting has been common also in countries such as Poland and Romania. These hints provide a good motivation to proceed into a more detailed analysis of the relational characteristics of the contracts observed.

3.4 Relational Characteristics

All networks constructed are extremely sparse. As given in the first panel in Table 3, the ratio of unweighted edges to all possible unweighted edges is very low in all six networks. The unweighted network density is even lower in the town-based network and the network constructed from the contracting bodies. This observation is logical in the sense that there are much more European towns and contracting bodies than member states in the EU. In any case, public cyber security procurement contracts do not mark an exception from the sparsity.

The technical explanation for the sparsity is simple; the amount of so-called self-loop edges and disconnected nodes is large in all networks. Here, a self-loop refers to an edge from a node back to the same node; a public authority located in one country made a procurement contract with a company in the same country, for instance. By accounting for the edge weights, a simple computation reveals that about 95% of all contracts in the cyber security sample were made nationally. While only a few national public authorities have contracted companies abroad through cyber security

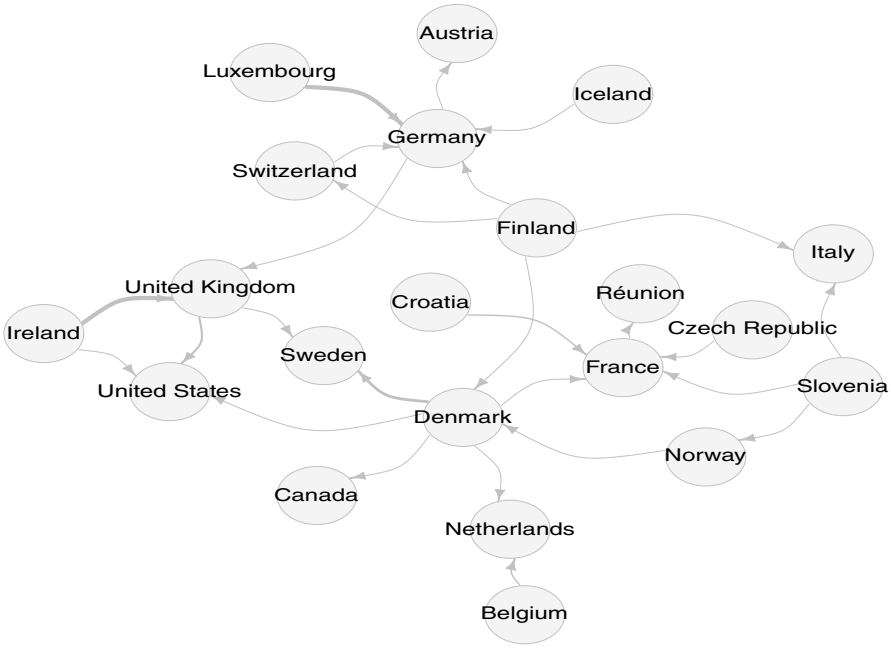

Fig. 6 A pruned country network for cyber security procurement contracts (self-loops and disconnected nodes removed; the widths of edges approximate edge weights)

procurement, the sample observation holds with respect to the random sample. The second panel in Table 3 indicates that an analogous effect is much less pronounced in the town-based network. This observation hints particularly about intra-state regional cyber security clusters. Furthermore, an analogous effect is absent in the network for the actual contracting bodies, which is expected because a self-loop in this network implies that a public authority made a procurement contract with itself.

Another way to look at the sparsity is to consider correlations between weighted in-degrees and out-degrees. Depending on whether such a correlation is positive or negative, the terms assortative and disassortative mixing are often used (Newman and Park 2003; Peng 2015). In the present context, strong assortative mixing (a large positive correlation coefficient) in a country-based network implies that procurements are generally reciprocal: national public authorities tend to contract foreign companies but these are accompanied with contracts between national companies and foreign public authorities. Given the substantial amount of self-loop edges, the lower panel in Table 4 provides a more reliable insight into such reciprocal cross-border relationships. The corresponding correlation coefficients are negligible in all three networks constructed from the cyber security sample. In contrast, relatively large positive coefficients are present in the country and town networks assembled from the random sample of procurement contracts. This observation provides additional support about the differences between the European cyber security procurements and procurement contracts in general (H_1). While also cross-border contracts are rare in the cyber security domain (H_3), this lack of Europeanization seems to

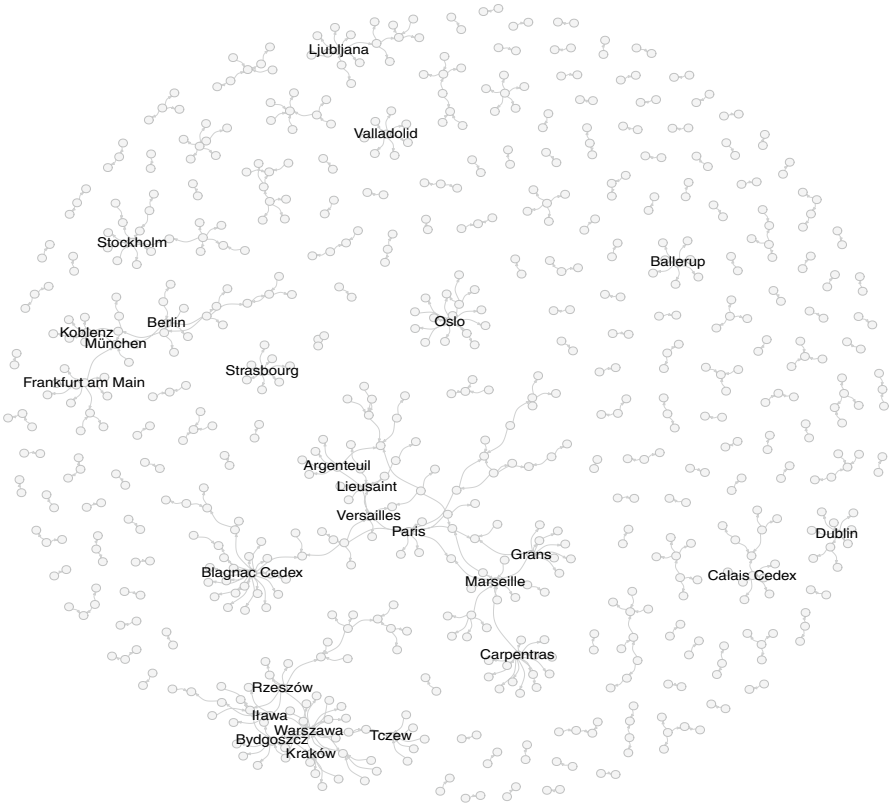

Fig. 7 A pruned town network for cyber security procurement contracts (self-loop edges and disconnected nodes removed)

apply to procurement contracts in general (*versus* H_2). Most contracts made by national public authorities are done with national companies.

Despite these observations, it is worthwhile to make a brief visual outlook to the actual networks. Thus, Fig. 6 shows the country-based network of cyber security procurement contracts with self-loops and disconnected nodes erased. While the sparsity and the lack of reciprocity are both visible, there seems to be also four distinct groups in the network. Interestingly, these clusters do not seem to correlate well with the various recent bilateral defense cooperation arrangements (cf. Keohane 2016). These are also mostly located in western parts of the continent; only Czech Republic and Slovenia represent the eastern parts.

The first group involves the traditional transatlantic link, covering Ireland, the United Kingdom, and the USA. The second is located in Central Europe with Germany in a pivotal position. Although the clustering effect is less clear in the third group, four Nordic countries are connected to each other through Denmark. Interestingly, Denmark and Finland have also the network's highest out-degrees (meaning relatively many foreign procurement contracts) but with low in-degrees. The highest

in-degrees are possessed by Germany and France, and the latter is at the center of the fourth group of countries. The national French cluster is highly visible also in the corresponding town-based network visualized in Fig. 7. For instance, there is a distinct cluster around Blagnac—where the head office of Airbus is located. This town is a few topological network hops away from Paris where companies such as Thales Group are headquartered. Even though Polish public authorities have not made cross-border cyber security procurement contracts, there is also a dense regional cluster between many towns in Poland. A similar regional cluster is present in Germany—and elsewhere in Europe. All in all, Europeanization seems limited in the cyber security domain when portrayed through public procurement; regionalization would be a much better characterization.

4 Discussion

This paper examined two research questions. The answers obtained to the questions can be summarized as follows:

- Question Q_1 asked whether cyber security procurement in the EU tends to differ from public procurement in general. As was expected (H_1), the answer is positive; there are differences. Cyber security procurement contracts are more often signed by national institutions compared to regional or local public authorities. When compared to procurement contracts in general, these more often cover supplies instead of services and public works. These tend to also emphasize the so-called MEAT criterion more often than procurement contracts in general. However, the numerical differences are not substantial. In contrast, a decisive difference exists with respect to offers received for tendering calls; public cyber security procurement contracts receive much less bids compared to procurement contracts in general. Oftentimes, there is only a single bidder or a few bidders for cyber security procurement offers.
- Question Q_2 asked whether public cyber security procurement exhibits any noteworthy signs of Europeanization. Again as was expected (H_3), the answer is negative; there are no worthwhile empirical signs of Europeanization in this domain. Unlike what was expected (H_2); however, this observation generalizes to public procurement contracts in general. Although there are some visible clusters between the member states, the amount of cross-border cyber security procurement contracts is still negligible. Instead, the results seem to point toward within-state regional cyber security clusters that are particularly active in public procurement activities.

These answers provide interesting material for a brief speculation about the policy reasons behind the empirical observations. The obvious starting point would be the 2009 defense procurement reform in the EU and its potential relation to cyber security. In particular, the visible lack of Europeanization could be perhaps brushed off with the all too familiar reference to Article 346 and its essential security interests. Together with other exemptions and loopholes, this procurement legalese would

offer a simple and traditional explanation along the lines of "judicial politics and economic patriotism" (cf. Fiott 2017a). Although the explanation may apply to a portion in the lack of cross-border procurement contracts, the explanation alone does not seem sufficient, however. Because the lack of Europeanization applies to public procurement contracts in general, the directives related to defense cannot provide a sufficient explanation. Furthermore, most procurement contracts are signed by local public authorities regardless of the economic sector. While there are clear signs about competition obstacles in terms of public cyber security procurement, these thus seem to relate mainly to national cyber security markets. This reasoning supports earlier observations about the lack of international interests regarding procurement at the local public administration level (Obermann and Kostal 2003). The absence of a sufficient amount of bidders is also familiar from existing studies (Flynn 2018; Masson et al. 2015). The same applies to the observation about regionalization (Keohane 2016). All in all, the results echo the conventional chorus about the ineffectiveness of the EU's procurement regulation and practice.

However, further empirical research is required for better understanding the results presented. In particular, it is necessary to continue the already commenced work (Masson et al. 2015) on defense procurement, which should be explicitly compared cyber security procurement. As was argued in Sect. 2.1, defense procurement is not the only relevant case for comparisons; comparing cyber security procurement to general ICT procurement would be equally worthwhile. After all, throughout Europe, the ICT sector is famous for its (often deliberately) dysfunctional procurement contracts with the public sector. As was briefly noted in Sect. 3.3, some of the results presented may thus explain themselves through traditional procurement issues, including even the possibility of corruption. Furthermore, there is precious little previous work on the cyber security industry—let alone on the European cyber security industry in particular. What is generally known is that the market is mainly dominated by large companies from the USA (Kuerbis and Badiei 2017). Like with defense and traditional security (Kepe et al. 2018), the R&D efforts of these companies presumably surpass the efforts of their European competitors by a large margin. These points and the negative answer to Q_2 thus warrant further research regarding the effectiveness of the EU's procurement practices for improving industry competitiveness, including leveling the field for small- and medium-sized cyber security companies. With respect to general security PPPs, there exists some evidence that large European defense contractors (including Thales Group, Selex, Airbus, and Indra) have received the majority of R&D funding granted for the private sector (Statewatch 2017). Such findings are encouraging neither for smaller companies nor for smaller member states. This point is fundamental not only for the European cyber security industry but also for the CSDP.

In addition, further research should merge the two analytical continua used for the theoretical framing with other relevant dimensions of European cyber security. The nexus between external and internal security is one of these dimensions. If the procurement-specific Hypothesis H_1 in Fig. 3 is refined into a Prediction $\widehat{H}_1$ that the drivel toward the military endpoint continues, a possible analytical scenario is presented in Fig. 8. The shown Premise P_2 represents a fundamental transformation; institutions responsible for external security would explicitly become responsible

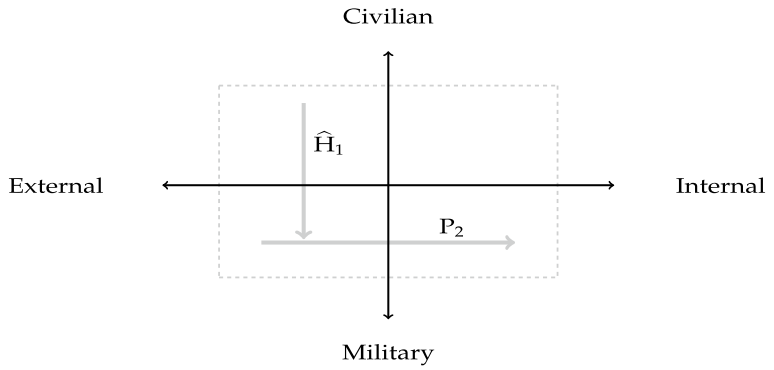

Fig. 8 A scenario for European cyber security

also for internal security in the EU. Despite the far-reaching consequences, the premise appears in recent policy documents; "armed forces are likely to become more involved in supporting the resilience of a country's civilian security sector and society as a whole" (Kepe et al. 2018, p. 15). The scenario offers many interesting avenues for research.

One avenue unfolds to the always fundamental relation between security and surveillance, privacy, and basic rights. As is acknowledged in the related EU policy documents, raising "awareness about information security proves difficult in many cases, in which the public perceives security as intrusive surveillance and an unwanted intrusion into personal rights and liberties" (Trimintzios et al. 2017, p. 27). To cast aside the peculiar wording about information security, which does not deal with surveillance—or even works against it (Zajko 2018), it should be stressed that the question is not merely about perceptions. Although several examples would be immediately available, border control is a classical case for approaching the external–internal continuum (Burgess 2009; Eriksson and Rhinard 2009). Thus, consider the recently enacted Regulation 2019/817, which further strengthens the sharing of biometric and other information for external border control throughout the EU. If P_2 realizes, a potential risk scenario would be that the associated biometric databases will be used also for internal purposes, such as reckless facial recognition within the member states. Another topic that warrants further research is the apparent duplication between the military and civilian approaches to European cyber security. This topic covers also the R&D programmes funded and coordinated by the EU. For instance, there is an ongoing PESCO project for incident response and information sharing about cyber threats. These are already well-established activities on the civilian side, including the private sector (Zrahia 2018). That said, the military and private sector approaches have one thing in common; they are mostly non-transparent.

Accountability and transparency are essential properties in the new era of artificial intelligence, big data, and digitalization. Not only are these properties necessary for algorithms used in the name of security and public policy, but these are increasingly seen also as crucial for sustaining the very foundations of democratic political systems (Zweig et al. 2018). Following this reasoning, the basic Premise P_1 from

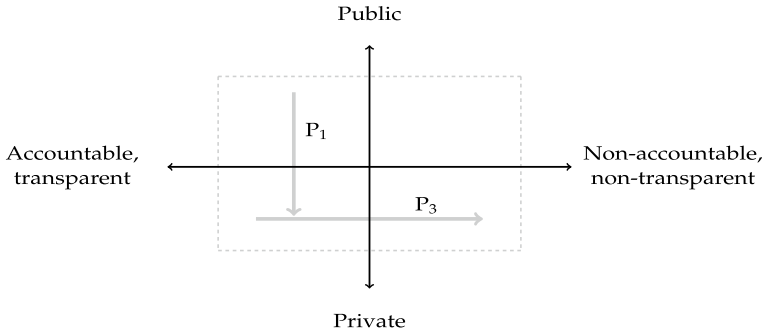

Fig. 9 Another scenario for European cyber security

Fig. 1 is used also with a new Premise P_3 in order to demonstrate another scenario illustrated in Fig. 9. To some extent, P_3 has already realized in the European Union through PPPs and related arrangements. These provide another prolific path for further research. The various security PPPs in the EU—whether those funded through PESCO/EDF or those present in the Horizon 2020 program—may also unveil novel forms of Europeanization.

Much effort has been devoted in the EU for improving practical procurement via e-procurement systems and other administrative improvements, but at the same time, paradoxically, particularly the security-related programmes have been explicitly moved to the non-transparent and non-accountable endpoint. The results are not necessarily flattering; balancing public interests (cyber security) with profits (private sector) has resulted in many inefficient and ill-defined forms of coordination (Carrapico and Barrinha 2017). Despite the long-standing problems with public procurement, these partnerships and their arrangements are most of all less transparent and less accountable compared to traditional public procurement. Legal accountability is largely lacking, and political accountability even more so. Even financial accountability has raised questions among the EU's own institutions (ECA 2018). Furthermore, little if any hard evidence has been presented regarding the economic improvements for the European cyber security industry—sans the benefits (or subventions) for the large defense contractors who appear to be reaping much of the money from the EU's security PPPs. The often used counterargument to this commonly expressed criticism has culminated to risk-taking, innovation, and related aspects (Hodge and Greve 2017), which, however, offer only a poor justification when the fundamental question is about the security of Europe and its people.

As is made explicit in Fig. 9, P_1 is a precondition for P_3 in this scenario. By implication, recent research has often started from the fundamental transformations that have shaped public administration in recent decades. For instance, some authors have used the term corporatization instead of marketization: "*markets* entail *private* actors producing, buying and selling *commodities*", but corporatization includes also private actors who "secure physical and human assets and property values and raise funds for their organizations to accomplish these goals and not *necessarily* for profit" (Lippert and Walby 2018, p. 196). Even though traditional procurement

continues to be a fundamental element for defense and traditional security, this alternative term seems appropriate for European cyber security. In other words, marketization may have outlived its usefulness as a theoretical concept for describing new forms of security and their relation to Europeanization. The term corporatization captures also well the increased agenda-setting power of private sector for framing the European (cyber) security landscape (cf. Statewatch 2017). If corporatization describes the strategy, the result could be described with the concept of hybrid governance. Besides the lack of transparency and the lack of accountability, hybrid governance for security PPPs has been characterized with two additional attributes: market belief and political risk aversion (Martins and Küsters 2019). All four attributes are difficult in a political union of sovereign states. Especially in case $\widehat{H}_1$, P_2, and P_3 together realize to their full potential in the future, there will be far-reaching consequences for Europeans and their civil societies. These consequences may undermine the political legitimacy of the CSDP and the whole European Union.

Acknowledgements Open access funding provided by University of Turku (UTU) including Turku University Central Hospital.

References

Abramova A, Garanina O (2018) Russian MNEs under sanctions: challenges for upgrading in GVCs (cases of energy and IT industries). J East West Bus 24(4):371–391

Alvarez-Rodríguez JM, Labra-Gayo JE, Rodríguez-González A, De Pablos PO (2014) Empowering the access to public procurement opportunities by means of linking controlled vocabularies. a case study of product scheme classifications in the European e-procurement sector. Comput Hum Behav 30:674–688

Ayres RU (1994) Towards a non-linear dynamics of technological progress. J Econ Beh Organ 24(1):35–69

Blom M, Castellacci F, Fevolden AM (2013) The trade-off between innovation and defense industrial policy: a simulation model analysis of the Norwegian defense industry. Technol Forecast Soc Change 80(8):1579–1592

Britz M (2010) The role of marketization in the Europeanization of defense industry policy. Bull Sci Technol Soc 30(3):176–184

Burgess JP (2009) There is no European security, only European securities. Cooperation Confl 44(3):309–328

Calcara A (2017) State-defence industry relations in the European context: French and UK interactions with the European Defence Agency. Eur Secur 26(4):527–551

Campbell Z (2019) Swarms of drones, piloted by artificial intelligence, may soon patrol europe's borders, the intercept. Available online in May 2019: https://theintercept.com/2019/05/11/drones-artificial-intelligence-europe-roborder/

Carrapico H, Barrinha A (2017) The EU as a coherent (cyber)security actor? J Common Mark Stud 55(6):1254–1272

Carrapico H, Farrand B (2017) 'Dialogue, partnership and empowerment for network and information security': the changing role of the private sector from objects of regulation to regulation shapers. Crime Law Soc Change 67(3):245–263

Christou G (2016) Cybersecurity in the European Union: resilience and adaptability in governance and policy. Palgrave Macmillan, New York
Drake LE, Donohue WA (1996) Communicative framing theory in conflict resolution. Commun Res 32(3):297–322
EC (2019) Evaluation of Council Directive 2008/114 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, SWD (2019) 310 final, European Commission (EC). Available online in August 2019: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20190723_swd-2019-310-commission-staff-working-document_en.pdf
ECA (2018) Public private partnerships in the EU: widespread shortcomings and limited benefits, European Court of Auditors (ECA). Available online in May 2019 https://www.eca.europa.eu/Lists/ECADocuments/SR18_09/SR_PPP_EN.pdf
Eriksson J, Rhinard M (2009) The internal–external security nexus. Cooperation Confl 44(3):243–267
EU (2018) Tenders electronic daily (TED)—public procurement notices from the EU and beyond. Available online in July 2018 https://data.europa.eu/euodp/en/data/dataset/ted-1
Fazekas M, Tóth IJ, King LP (2016) An objective corruption risk index using public procurement data. Eur J Crim Policy Res 22(3):369–397
Fevolden AM, Tvetbråten K (2016) Defence industrial policy—a sound security strategy or an economic fallacy? Def Stud 16(2):176–192
Fiott D (2019) The poison pill: EU defence on US Terms? European Union Institute for Security Studies (ISS), Brief/7. Available online in August 2019 https://www.iss.europa.eu/sites/default/files/EUISSFiles/7
Fiott D (2017a) Patriotism, preferences and serendipity: understanding the adoption of the defence transfers directive. J Common Mark Stud 55(5):1045–1061
Fiott D (2017b) The EU, NATO and the European defence market: Do institutional responses to defence globalisation matter? Eur Secur 26(3):398–414
Flynn A (2018) Measuring procurement performance in Europe. J Public Procure 18(1):2–13
Gelderman K, Ghijsen P, Schoonen J (2010) Explaining non-compliance with European Union procurement directives: a multidisciplinary perspective. J Common Mark Stud 48(2):243–264
Gleeson N, Walde I (2016) Placing the state in the cloud: issues of data governance and public procurement. Comput Law Secur Rev 32(5):683–695
Gori GF, Lattarulo P, Mariani M (2017) Understanding the procurement performance of local governments: a duration analysis of public works. Environ Plan C Polit Space 35(5):809–827
Graycar A (2019) Mapping corruption in procurement. J Financ Crime 26(1):162–178
Harašta J (2018) Legally critical: defining critical infrastructure in an interconnected world. Int J Crit Infrastruct Prot 21:47–56
Hartley K, Bellais R, Hébert J (2008) The evolution and future of European defence firms. In: Fontanel J, Chatterji M (eds) War, peace and security. Bingley, Emerald, pp 83–104
Healey J (2017) Who's in control: balance in cyber's public–private sector partnerships. Georget J Int Aff 18(3):120–130
Hodge GA, Greve C (2017) On public–private partnership performance: a contemporary review. Public Works Manag Policy 22(1):55–78
Howorth J (2019) Differentiation in security and defence policy. Comp Eur Polit 17(2):261–277
Kennedy-Loest C, Pourbaix N (2010) The new EU defence procurement directive. ERA Forum 11(3):399–410
Keohane D (2016) The renationalization of European defense cooperation. In: Thränert O, Zapfe M (eds) Strategic trends 2016: key developments in global affairs. Center for security studies, ETH Zurich, Zurich, pp 9–28. Available online in August 2019 http://www.css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/ST2016.pdf
Kepe M, Black J, Melling J, Plumridge J (2018) Exploring Europe's capability requirements for 2035 and beyond: insights from the 2018 update of the long-term strand of the capability development plan, RAND Europe, prepared for the European Defence Agency (EDA). Available online in August 2019 https://www.eda.europa.eu/docs/default-source/brochures/cdp-brochure---exploring-europe-s-capability-requirements-for-2035-and-beyond.pdf
Keränen O (2017) Roles for developing public–private partnerships in centralized public procurement. Ind Mark Manag 62:199–210
Khorana S, Ferguson-Boucher K, Kerr WA (2015) Governance issues in the EU's e-procurement framework. J Common Mark Stud 53(2):292–310

Kuerbis B, Badiei F (2017) Mapping the cybersecurity institution landscape. Digit Policy Regul Gov 19(6):466–492
Ladi S, Tsarouhas D (2017) International diffusion of regulatory governance: EU actorness in public procurement. Regul Gov 11(4):388–403
Lippert RK, Walby K (2018) Corporatizing security through champions, condos and credentials. Aust N Z J Criminol 52(2):193–212
Markowski S, Wylie R (2007) The emergence of European defence and defence industry policies. Secur Chall 3(2):31–51
Martins BO, Küsters C (2019) Hidden security: EU public research funds and the development of European drones. J Common Mark Stud 57(2):278–297
Massacci F, Ruprai R, Collinson M, Williams J (2016) Economic impacts of rules-versus-risk-based cybersecurity regulations for critical infrastructure providers. IEEE Secur Priv 14(3):32–43
Masson H, Martin K, Quéau Y, Seniora J (2015) The impact of the 'defence package' directives on European defence, European Parliament Think Tank. Available online in July 2019 http://www.europarl.europa.eu/RegData/etudes/STUD/2015/549044/EXPO_STU(2015)549044_EN.pdf
Meehan J, Ludbrook MN, Mason CJ (2016) Collaborative public procurement: institutional explanations of legitimised resistance. J Purch Supply Manag 22(3):160–170
Mehrbod A, Grilo A (2018) Tender calls search using a procurement product named entity recogniser. Adv Eng Inform 36:216–228
Meijer H, Wyss M (2018) Upside down: reframing European defence studies. Cooper Confl 54(3):378–406
Mérand F (2006) Social representations in the European security and defence policy. Cooper Confl 41(2):131–152
Mérand F, Hoffman SC, Irondelle B (2010) Governance and state power: a network analysis of European security. J Common Mark Stud 49(1):121–147
Moe CE, Newman M, Sein MK (2017) The public procurement of information systems: dialectics in requirements specification. Eur J Inf Syst 26(2):143–163
Newman MEJ, Park J (2003) Why social networks are different from other types of networks? Phys Rev E 58(3):036122
Nielsen JU, Hansen LG (2001) The EU public procurement regime-does it work? Intereconomics 36(5):255–263
Nováky N (2018) The EU's permanent structured cooperation in defence: keeping sleeping beauty from snoozing. Eur View 17(1):97–104
Obermann G, Kostal T (2003) Public procurement at the local level in Austria: the economic consequences of compulsory competitive tendering for public services. Ann Public Cooper Econ 74(1):139–162
Obwegeser N, Müller SD (2018) Innovation and public procurement: terminology, concepts, and applications. Technovation 74–75:1–17
OECD (2017) Government at a glance 2017. OECD Publishing, Paris
Pawlak P (2019) The EU's role in shaping the cyber regime complex. Eur Foreign Aff Rev 24(2):167–186
Peng T (2015) Assortative mixing, preferential attachment, and triadic closure: a longitudinal study of tie-generative mechanisms in journal citation networks. J Inform 9(2):250–262
Pîrvu D, Bâldan C (2014) Access to the EU public procurement market: Are there disparities based on the origin of economic operators? J Econ Issues 47(3):765–780
Powell-Turner J, Antill PD, Fisher RE (2016) The United Kingdom Ministry of Defence and the European Union's electrical and electronic equipment directives. Resour Policy 49:422–432
Regan M, Smith J, Love P (2011) Infrastructure procurement: learning from private–public partnership experiences 'down under'. Environ Plan C Govern Policy 29(2):363–378
Rieker P (2006) From common defence to comprehensive security: Towards the europeanization of French foreign and security policy? Secur Dialogue 37(4):509–528
Robinson N, Slack C (2019) Co-operation: a key to NATO's cyberspace endeavour. Eur Foreign Aff Rev 24(2):154–166
Ruohonen J, Kimppa KK (2019) Updating the Wassenaar debate once again: surveillance, intrusion software, and ambiguity. J Inf Technol Polit 16(2):169–186
Ruohonen J, Hyrynsalmi S, Leppänen V (2016) An outlook on the institutional evolution of the European Union cyber security apparatus. Govern Inf Q 33(4):746–756
Siponen M, Baskerville R (2018) Intervention effect rates as a path to research relevance: information systems security example. J Assoc Inf Syst 19(4):247–265

Statewatch (2017) Market Forces: the development of the EU security-industrial complex. Available online in April 2019 https://statewatch.org/analyses/marketforces.pdf
Stevens T (2017) Cyberweapons: an emerging global governance architecture. Palgrave Commmun 3:1–6
Strikwerda J (2017) Sovereignty at stake? The European Commission's proposal for a defence and security procurement directive. Eur Secur 26(1):19–36
Trimintzios P, Chatzichristos G, Portesi S, Drogkaris P, Palkmets L, Liveri D, Dufkova A (2017) Cybersecurity in the EU Common Security and Defence Policy (CSDP): challenges and risks for the EU. European Parliamentary Research Service (EPRS). Available online in May 2019 http://www.europarl.europa.eu/RegData/etudes/STUD/2017/603175/EPRS_STU(2017)603175_EN.pdf
Valeriano B, Maness RC (2018) How we stopped worrying about cyber doom and started collecting data. Polit Gov 6(2):49–60
van der Pol J, Rameshkoumar J (2017) The co-evolution of knowledge and collaboration networks: the role of the technology life-cycle. Scientometrics 114(1):307–323
van Eeten M (2017) Patching security governance: an empirical view of emergent governance mechanisms. Digit Policy Regul Gov 19(6):429–448
van Scherpenberg J (1997) Transatlantic competition and european defence industries: a new look at the trade–defence linkage. Int Aff 73(1):99–122
Varney M (2011) E-procurement–current law and future challenges. ERA Forum 12(2):185–204
von Solms R, van Niekerk J (2013) From information security to cyber security. Comput Secur 38:97–102
Zajko M (2018) Security against surveillance: IT security as resistance to pervasive surveillance. Surveill Soc 16(1):39–52
Zrahia A (2018) Threat intelligence sharing between cybersecurity vendors: network, dyadic, and agent views. J Cybersecur 4(1):1–16
Zweig KA, Wenzelburger G, Krafft TD (2018) On chances and risks of security related algorithmic decision making systems. Eur J Secur Res 3(2):181–203