BASC WORKING PAPER SERIES

THE EUROPEAN UNION'S CYBER INDUSTRIAL POLICY

Paul Timmers

Working Paper 2018-04

BERKELEY APEC STUDY CENTER
552 Barrows Hall
University of California
Berkeley, California 94720-1950
September 2018

This paper is part of a project "Comparative Industrial Policy in the Cyber Security Industry: Policies, Drivers, and International Implications," organized by Vinod K. Aggarwal and Andrew Reddie of the Berkeley APEC Study Center and funded by the Center for Long-Term Cybersecurity at the University of California, Berkeley. The author would like to express his gratitude to UC Berkeley's Center for Long-Term Cybersecurity, Institute for East Asian Studies, Berkeley APEC Study Center and UC San Diego's Institute on Global Conflict and Cooperation for supporting the workshop series. The author would also like to thank Vinod Aggarwal, Michael Adams, and Andrew Reddie for comments on previous drafts of the manuscript.

BASC working papers are circulated for discussion and comment. They have not been peer-reviewed.

The European Union’s Cyber Industrial Policy
Paul Timmers
BASC Working Paper No. 2018-04

Abstract

Since 2013, EU cybersecurity policy has quickly developed, with many implications of an industrial policy nature, even if there is no fully articulated EU cybersecurity industrial policy. In parallel, the private sector has organized itself to better respond to cybersecurity challenges, influence policy making, and benefit from the rapidly growing cybersecurity market. EU policy-makers, within a mandate constrained by national security which is the remit of its Member States, have sought to make the EU Single Market, internal security, and external relations coherently address the rapidly evolving and uncertain world of cybersecurity. To do this, they use policy tools ranging from defining common political visions to written law. The EU model for political and practical cooperation of a large number of countries on shared public, economic, and security objective, serves as an example of wider international cooperation, providing insight on positioning cybersecurity industrial policy in a wider policy context, defining governance for related policy development, and suggesting an international agenda.

Paul Timmers[1]
European Union Commission
Paul.timmers@politics.ox.ac.uk

[1] Paul Timmers is the Former Director of the European Commission for Digital Society, Trust & Cybersecurity and visiting research fellow University of Oxford. He holds a Ph.D in theoretical physics from the University of Nijmegen, an MBA from Warwick Business School, has been an EU research fellow at UNC Chapel Hill, USA and completed executive education in cybersecurity at Harvard. Opinions expressed by the author should not be taken to be representing the views of the European Commission or the University of Oxford.

Introduction

In 2015, the European cybersecurity market represented about 25% of the world market (which at that time was estimated at 70 B€, with the U.S. market comprising about 40% of this). Average annual growth of the European cybersecurity market is estimated at 6% while the world market is growing at over 8% annually. About 60% of the European Union (EU) market is in the UK, Germany, and France. The European Cybersecurity Organisation (ECSO) distinguishes between high-grade cybersecurity (served by a small number of companies originating from the defense industry); mid-grade (dealing with critical infrastructures and public authorities with many European small and medium-sized companies); and low-grade (general public, B2C; being largely dependent on non-European companies). There are an estimated 600 SMEs active in the field, the large majority of them with a turnover rate below 5 M€ and with less than 50 employees (ECSO 2016).

In terms of cybersecurity readiness, the 2017 ITU Global Cybersecurity Index (ITU 2017) indicates that Europe, as well as the EU, averages high scores across all five categories of cybersecurity (legal measures, technical measures, organizational measures, capacity building, and cooperation). This is an exception in comparison to other geographic regions. The US, however, still scores higher than the EU on all categories (see Figure 1).

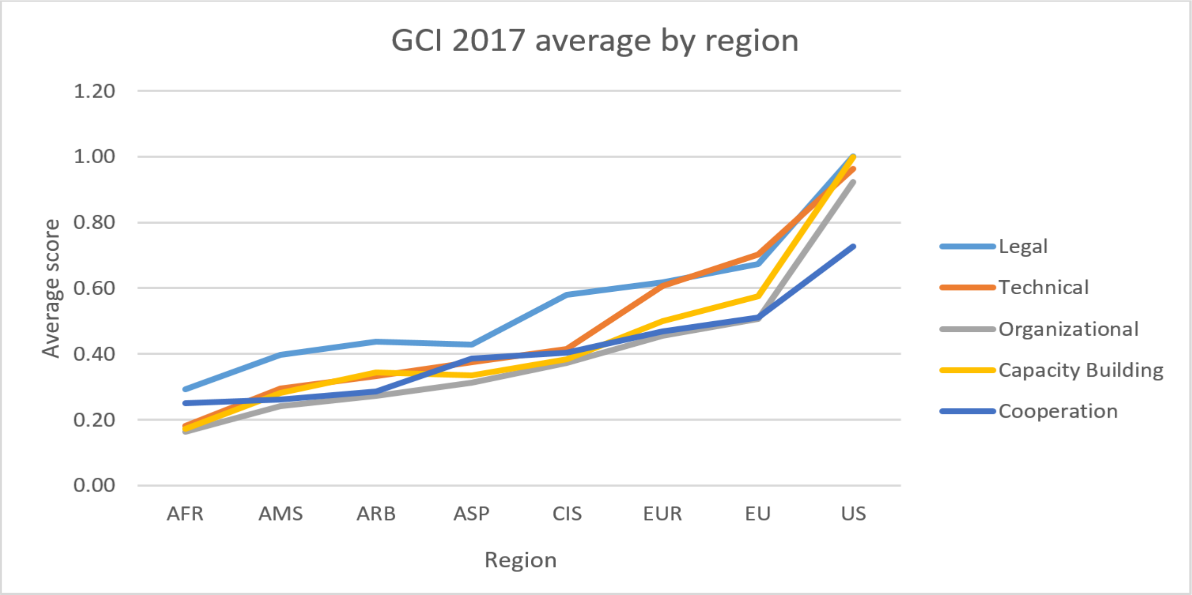


Figure 1 ITU Global Cybersecurity Index by region of the world[2]*. Top ranking countries are Singapore, US, Malaysia, Oman and Estonia, respectively.*

[2] Data courtesy Maxim Kushtuev, ITU. Region abbreviations: AFR=Africa, AMS=Americas, ARB=Arab States, ASP=Asia-Pacific, CIS=Commonwealth of Independent States, EUR=Europe, EU=European Union, US=United States of America.

The EU, as a regionally, economically, and politically cooperative entity,[3] pursues the common interests of its 28 Member States and its 500 million citizens. With regard to EU cybersecurity policy, an important area of shared economic interest is the safeguarding of the **Single Market** (i.e. the free flow of goods, services, capital and people; also called internal market). A second important area of shared interest is maintaining European security, particularly with regard to protecting against terrorism or natural disasters ('internal security'). These two strong interests are complemented by European support for being 'a stronger global actor', support demonstrated through EU policies on international diplomacy, enlargement, development cooperation, defense, and trade (European Commission 2014).

Potential and actual disruption of the Single Market is a serious concern. The 2017 WannaCry and NotPetya attacks caused a great deal of real disruption for numerous actors including the disruption of international logistics. Beyond direct disruption, there is also a concern about the risk of an erosion of trust in the Single Market which could hamper trade. Moreover, a well-functioning Single Market is seen as a great opportunity for growth and competitiveness for the European cybersecurity industry. Thanks to the EU's strong formal mandate for the Single Market, such issues can be addressed by EU cybersecurity policy. For example, the aforementioned 2017 cyber-attacks triggered multilateral cooperation at the EU level, as defined by the EU's Network and Information Security Directive, thus resulting in a specific instance of the implementation of EU cybersecurity policy.

Dealing with cyber-incidents in the Single Market is of ever greater importance in EU sectoral policies for industries such as finance, transport, and energy. For example, end-to-end continuity of energy supply ('energy security') requires reliable interconnection of electricity lines between countries across Europe and an ability to handle cyber-attacks.

The second area of EU-level interests and concerns, **internal security**, mostly focuses on continent-wide terrorism and cybercrime. Action is justified at the European level given the free flow of people in Europe, common external borders (at least in the Schengen area) and the open nature of the internet. Over the years, internal security policy has been increasingly strengthened as a pillar of European cooperation. Important specific challenges include the use of encryption by criminals or terrorists—an issue on which countries are not fully aligned—, the exchange of

[3] The EU is supported in policy-making and implementation by a number of bodies of which the most important ones referred to here are the European Commission (EC), the Council of Ministers ('Council'), and the European Parliament (EP). Also mentioned here is the European External Action Service. The EU's legal basis is provided by the Treaty on the European Union TEU and the Treaty on the Functioning of the European Union TFEU (European Union 2016c). The EC has the mandate to propose legislation. EP and Council then negotiate and agree such laws with mediation by the EC. EU law includes Directives that require transposition into national law in each EU Member State or directly applicable Regulations or Decisions. A country which does not live up to the transposition or implementation of EU law can be taken to the European Court of Justice by the EC.

information for judicial cooperation, penalizing cybercrime, and action on content-related challenges such as hate speech and fake news.

The third broad area for EU-level action is the **external dimension**, which ranges from trade policy to export controls, to development cooperation where cybersecurity capacity-building can be included, to international diplomacy. Not only is this a wide and diverse area of work where both the European Commission and the European External Action Service have a role to play with and next to the Member States, it is also an area where the EU *de facto* competence continues to develop, namely in handling migration.

Trade policy is also of particular interest, as the EU has a unique mandate on this. That is, only the EU may negotiate trade deals, not individual member states. Therefore, if cybersecurity became a point of contention in trade negotiations, the EU dimension of cybersecurity policy would be significantly strengthened.

Finally, while the EU can be viewed as a successful model of international cooperation, notably the achievement of the Single Market, the EU model also has its challenges. Brexit is a case in point. Thus, the EU, as a governing body, has to constantly evolve and innovate. Cybersecurity represents a challenge to established EU governance. The analysis of struggles, failures and successes in the EU may provide useful insights for dealing with cybersecurity internationally. To perform this analysis, I use the theoretical framework developed for this special issue by Aggarwal and Reddie (2018).

2. Market Failures

Regarding market failures, two viewpoints can be considered: the political perspective regarding cooperation at the EU-level rather than at the level of individual Member States; and the economic perspective which addresses the issues with the functioning of the market of cybersecurity across the EU. The focus is on EU-level market failures, rather than those that may hold in a country individually such as lack of cyber-awareness.

2.1 Political

From a political perspective, 'market failures' include prioritizing national security or national interests, formalizing limits to the EU mandate to act in cybersecurity matters, and presenting an incomplete common vision, policy, and leadership. While **national security** restrictions are less prominent in European countries in comparison to states such as China or the USA, individual state restrictions can still play a role when territory comes into play such as for physical critical infrastructures. This distinction contributes to a differentiated approach in EU law (the Network and Information Security Directive) between physical and digital critical infrastructures with regard to incident information sharing and common approaches.

Formal limits in the **EU-level mandate** stem from the EU Treaties. Article 4(2) of the TEU notes that the EU shall respect 'essential State functions, including […] maintaining law and order and safeguarding national security. In particular, national security remains the sole responsibility of each Member State. Consequently, EU legislation and policy often has a national security exemption clause.

Except where EU law prevails by the EU Treaties over domestic law, national cybersecurity policy is a Member State matter, though it can possibly be influenced by cooperation within subgroups of Member States or by alignment with EU-level soft policy.

Still, EU-level legislative action on cybersecurity with industrial implications is possible notably since the EU has a strong mandate on the areas of the Single Market and trans-European networks (Art 114 and Art 172 TFEU) as well as in justice and police cooperation to deal with serious crime with cross-border dimension (Art 83(1) TFEU). Furthermore, the possibility for legislative action exists in sectoral legal bases such as for energy (Art 194 TFEU) and transport (Art 90) as well as for administrative cooperation in justice and security (Art 74 TFEU). Always, EU law must pass tests of subsidiarity and proportionality to prevent undue centralization and overregulation.

Smaller coalitions of Member States, often involving Germany and France, also team up to influence EU cybersecurity policy. This happens both formally[4] and informally.
Finally, the inability to present a complete **common vision**, policy, and leadership is both a consequence of the limited mandate and of fragmentation and lack of past political prioritization (e.g. the EU does not have a unique cybersecurity coordinator at European level).

2.2 Economic

From an economic perspective, "market failures" specific to the EU include internal market fragmentation, institutional dependency, inadequate capital markets and financing, market consolidation barriers, and inadequacies in governance.

Fragmentation means that the Single Market is not as smooth as it could be, manifesting itself for example in overlapping standards and nationally diverse security requirements. The European Network and Security Agency (ENISA) reported an overlap in standards and a risk of duplication in certification schemes due to the work done by security agencies in France,

[4] An example is the input of France, Germany, Italy and Spain for the 28 Sept 2017 Digital Summit, https://archiv.bundesregierung.de/Content/EN/Reiseberichte/2017_en/2017-09-28-tallinn-digitalgipfel_en.html.

Germany, and the UK (ENISA 2016b). Gaps in standards such as for managed security services may hinder the free flow of services across the EU. Security requirements can also vary between providers of similar communications services such as telecom operators and OTTs. This, in turn, can create pressure for regulatory intervention to level the playing field[5]. Lack of clarity about harmonized compliance has led to calls for EU-level certification and labelling. According to 38% of respondents to a 2016 EC public consultation, current ICT security certification schemes do not adequately support the needs of European industry (European Commission 2016a)[6].

Fragmentation leads to smaller markets, less economies of scale, and thereby smaller companies, making home-grown industry less competitive as pointed out by the European Cybersecurity Industry Leaders group (ECIL 2016)[7]. In a field where expertise is often scarce, fragmentation reduces the re-use of and access to such expertise. Moreover, since cybersecurity is categorized as a low-trust field, brand and reputation are incredibly important, two characteristics which are difficult to develop for a small local company competing against large global players.

At the high-grade end of the market, suppliers have traditionally had a close relationship to military and government buyers. The downside of this is a degree of **national institutional dependency,** or perhaps even lock-in[8]. As observed in (European Commission 2016a): "Historically, industrial development in this area has been stimulated by governmental procurement and some highly innovative European companies in this sector are still largely dependent on this in their home country. A side effect of this situation is limited willingness for cross-border procurement, which is a barrier to the development of a common cybersecurity market."

Another market challenge in Europe is the relative **lack of well-developed capital markets** and complementary industries with large (ICT) companies which could be interested in acquiring cyber companies and thus help consolidation. There is not enough capital available for scaling-up. According to one study, only 25% of European cybersecurity companies that are viable at a small scale manage to move into later-stage funding (and only few into IPO), further reinforcing why companies stay relatively small. In a 2016 consultation, "75% of respondents stated they did not feel they had sufficient access to financial resources to finance cybersecurity projects and initiatives" (European Commission 2016a). Industry leaders in ECIL also reported a lack of supporting financial and fiscal environment (though the taxation measures they proposed are likely not an EU competence).

[5] In telecommunications (see also proposal for a European Communications Code, Sept 2016) and in privacy in electronic communications (see also proposal for an ePrivacy Regulation, Jan 2017).

[6] See also the proposal for an ICT Security Certification Regulation, Sept 2017 <…>.

[7] The European Cybersecurity Industry Leaders group consists of Thales, Atos, Airbus Group, BBVA, BMW, Cybernetica, Deutsche Telekom, Ericsson, F-Secure, and Infineon.

[8] Similar as for the security market, as observed in (European Commission 2012c).

In addition, ECIL industry leaders pointed to other **barriers to market consolidation (**i.e. the possibility to scale-up rapidly through M&A): they hypothesize that under current European merger rules, an emphasis is too heavily placed on company turnover with not enough emphasis being placed on market developments and global industrial dimensions.

Moreover, there is a perceived threat of FDI and foreign M&A in the open EU economy. Indeed, globally the most active acquirers are large ICT and cybersecurity companies (which are mostly from the U.S.) and the top-10 largest exits from 2012-2017 were all U.S. companies (CBInsights 2017). The European Commission in-house policy advisory department (EPSC) considers the situation a risk to economic competitiveness but also an economic risk to resilience due to dependency on external technologies (EPSC 2017). Related to this is the risk of outflow of European talent and know-how. This on-going debate in Europe about 'digital sovereignty' is one of the drivers for a proposal made in in September 2017 to establish EU-level FDI scrutiny (see below).

With regard to inadequacies in **governance,** a whole range of gaps can be identified regarding industry cooperation, demand-supply dialogue, synergies between civilian and defence cybersecurity markets, pooling of expertise, organization for certification, and ecosystems of smaller companies - larger companies, universities – industry, academia-industry-education-government. EPSC made a plea for 'ramping up institutional collaboration' through initiatives like the European Cybersecurity Coordination Platform. (EPSC 2017) observes that while "some initiatives across a few member states aim to bring together the competencies and industrial players in this area, potentially helping European companies to join forces and expand across a number of European countries, the gap is still considerable: the industry is nowhere near some more structured segments of the ICT industry, such as micro-electronics, where well-established regional clusters of excellence and ecosystems can be identified, leveraging academia, industrial, institutional and customers/users capacities, and enabling this industry to compete on a global scale."[9]

2.3 Interplay of Political and Economic Factors

Obviously 'market failures' are interrelated, thus suggesting a combined soft and hard intervention logic for industrial policy: a central role for common political vision together with binding measures notably Single Market based – where EU-level mandate and economic focus is strong - complemented by internal security measures and with a strong linkage to international policy. Indeed, this is largely the logic which the EU has moved towards since 2013.

[9] In September 2017 forms of enhanced EU cooperation were proposed: Blueprint for handling large-scale cyber-attacks and Competence Network, addressed elsewhere in this paper.

Political and economic factors can weaken or strengthen Single Market cybersecurity industrial policy measures. Likely, the increased need for cooperation on internal security matters such combating terrorism and crime is strengthening a common vision on cybersecurity (though unbreakable encryption is a more divisive issue). Renewed attention to the external dimension of cyber-security such as coordinated EU-level involvement in international cyber-dialogues also reinforces this common vision, despite debate on such things like freedom of speech in cyberspace or dealing with the situation of 'unpeace', a level of conflict below war but above peaceful competition between states (Kello 2017). A stronger common vision increases the willingness to let the EU act and strengthens the effectiveness of EU mandates and allows for more collaborative governance. This in turn, makes Single Market measures more effective and reduces national lock-in.

3. Inventory of Measures

While there is no EU cybersecurity *industrial policy* as such, there is a set of measures with an industrial policy dimension that originates from another objective: Single Market, internal security, external dimension. Below we first give a brief overview of the history of cybersecurity policy development to make clear that there has been a shift in thinking from national orientation towards joint action and common vision in the last decennium. Next the most important measures from an industrial policy point of view are highlighted and put in a classification. Finally, these measures are related to general digital and data protection policy.

3.1 History

From the early 1990's until 2012, several cybersecurity policy measures had already been put into effect. Amongst the most significant early initiatives was mutual recognition of certification through cooperation of a limited number of European countries since 1992 in the SOG-IS group; combating cybercrime through a 2005 Decision on Attacks against Information Systems (European Union 2005)[10] and establishment of the Europol Cybercrime Centre EC3 in 2012); and strengthening cyber-resilience capability in the Member States through the establishment in 2004 of the EU Network and Information Security Agency ENISA. However, all these measures had never before been combined into one integrated framework.

2013, however, marked the launch of the first fully-fledged EU Cybersecurity Strategy by the European Commission and the European External Action Service (EC and EEAS 2013)[11] . The 2013 Strategy presented a comprehensive and integrated vision. Firstly, it addressed

[10] Superseded in 2013 by an eponymous Directive.

[11] The Strategy is a joint EC and EEAS Communication. A Communication is a non-binding policy document usually from the European Commission (sometimes jointly from the Commission and the External Action Service EEAS) often followed-up by Council Conclusions and a European Parliament Opinion.

cybersecurity policy from several perspectives (resilience & market/industrial, cybercrime, cyber defense & international cyberspace). Secondly, it outlined relations between these perspectives. The 2013 Strategy was a high-level and political document rather than a detailed and binding action plan.

As part of the EU Cybersecurity Strategy, an important cyber-resilience law was proposed – the Network and Information Security (NIS) Directive. Council and EP concluded their negotiation on this law in 2016. The NIS Directive is to come stepwise in force in the Member States until mid-2018, i.e. five years after its initial proposal.

Internationally, the EU was a relative latecomer in coming forward with a cybersecurity strategy. The EU could thus build upon the work of several EU Member States, the USA and other countries to come forward with an up-to-date and leading-edge approach. In 2012-2013 it was already well-recognized that cybersecurity merited a dedicated policy, which has ever more become a 'Chef-Sache' due to the rise and seriousness of cyber incidents.
It was also understood that economic, crime, and international issues should not be dealt with in isolation. Departments in EC and EEAS worked closely together in defining the Strategy, supported by joined-up political leadership of the European Commissioners for Digital Policy, Justice & Home Affairs, and the EU High Representative for External Affairs.

The Strategy built upon existing policy measures such as on cybercrime, data retention, investment in research & innovation, standardization, investment in knowledge repositories and capacity building (the ENISA and Europol agencies), international cooperation, and stakeholder cooperation. The international dimension of the Strategy included stepped-up cyberspace dialogues and cooperation of the EU with international partners such as the USA, China, Japan and India as well as with NATO.

Since 2013, a range of measures have put further details into the framework of the Strategy. Most relevant from an industrial policy perspective is the 2016 policy on 'Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry' (the '2016 Strengthening Communication'). This policy presented plans to further reduce internal market fragmentation, explore certification and labelling, nurture industrial capabilities, step-up research & innovation, and improve handling of major cyber incidents.

This 2016 policy presented a combined demand - supply perspective, stating that 'Europe needs high-quality, affordable and interoperable cybersecurity products and solutions. However, the supply of ICT security products and services within the single market remains very fragmented geographically. On the one hand, this makes it difficult for European companies to compete on the national, European and global level; on the other, it reduces the choice of viable and usable cybersecurity technologies that citizens and enterprises have access to.

It argued that much of procurement is still national and that economies of scale are lacking for companies to compete within Europe and globally, exacerbated by lack of standards, interoperability and certification. Finally, the document observes that ‘The limited perspectives of growth for cybersecurity companies within the single market result in a multitude of mergers and acquisitions by non-European investors.’ This was the first time the issue of foreign-driven M&A was raised at EU-level following national level concerns.

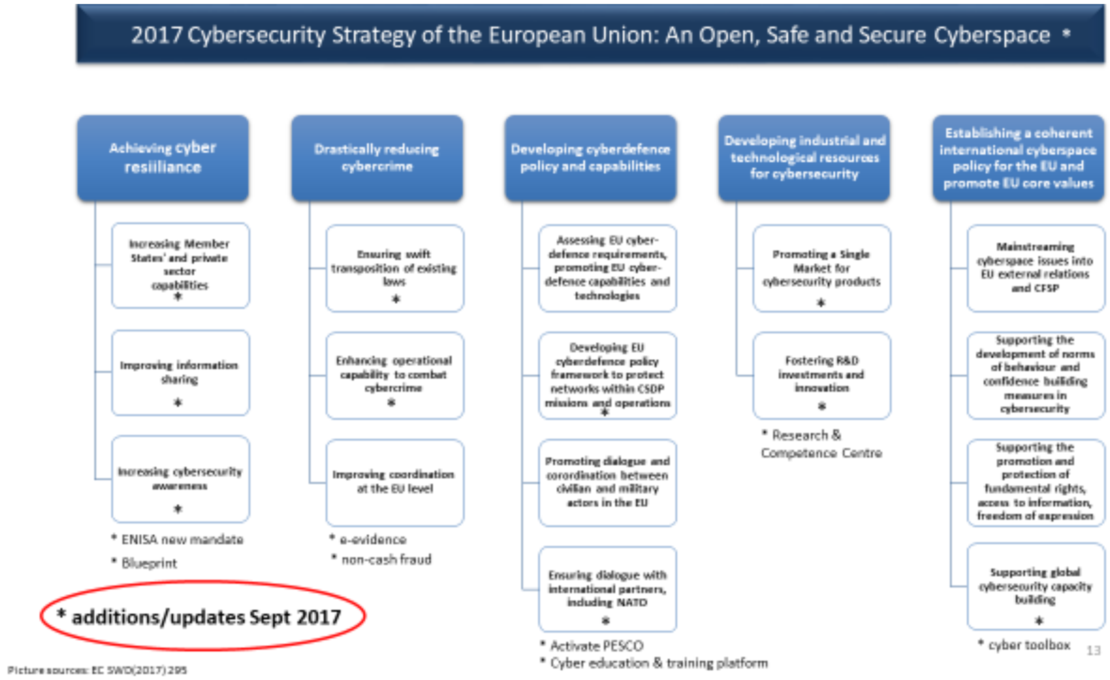
The 2016 Strengthening Communication provided the policy anchor for a private-public partnership to increase strategic steer and greater leverage of EU R&I funding. The PPP contract is between the EC and ECSO, a newly established cybersecurity industry organization.

September 2017 marked a major update to the EU Cybersecurity Strategy (EC and EEAS 2017). While maintaining the coherence of the 2013 Strategy, all pillars were strengthened with specific measures in order to achieve ‘a shift for the EU from a reactive to a proactive approach to protecting European prosperity, society and values, as well as fundamental rights and freedoms, through responding to both existing and future threats’.

The most relevant 2017 measures in view of cybersecurity industrial policy were:

- Strengthening **ENISA**: the agency is to get more resources and new tasks in particular to work with industry on certification
- Cybersecurity **Certification**: industry can voluntarily comply with certification schemes that will have EU-wide recognition and supersede national schemes
- **Competence networking**, EU Cybersecurity Research and Competence Centre: intention to propose in 2018 networking of competence centers and a European facility.
- **Coordinated response** to large scale cybersecurity incidents and crises: a.o. linking economically-based response mechanisms (NIS Directive) and political cooperation-based ones (Integrated Political Crisis Response).

Figure 2 below gives both an overview of the 2013 Strategy and of the 2017 additions of which several are proposals that still are under negotiation with the co-legislators, the Council of the EU and the European Parliament.



2017 Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace *

Achieving cyber resilliance
- Increasing Member States' and private sector capabilities *
- Improving information sharing *
- Increasing cybersecurity awareness *

* ENISA new mandate
* Blueprint

Drastically reducing cybercrime
- Ensuring swift transposition of existing laws *
- Enhancing operational capability to combat cybercrime *
- Improving coordination at the EU level

* e-evidence
* non-cash fraud

Developing cyberdefence policy and capabilities
- Assessing EU cyber-defence requirements, promoting EU cyber-defence capabilities and technologies
- Developing EU cyberdefence policy framework to protect networks within CSDP missions and operations *
- Promoting dialogue and corordination between civilian and military actors in the EU
- Ensuring dialogue with international partners, including NATO *

* Activate PESCO
* Cyber education & training platform

Developing industrial and technological resources for cybersecurity
- Promoting a Single Market for cybersecurity products *
- Fostering R&D investments and innovation *

* Research & Competence Centre

Establishing a coherent international cyberspace policy for the EU and promote EU core values
- Mainstreaming cyberspace issues into EU external relations and CFSP
- Supporting the development of norms of behaviour and confidence building measures in cybersecurity
- Supporting the promotion and protection of fundamental rights, access to information, freedom of expression
- Supporting global cybersecurity capacity building *

* cyber toolbox

* additions/updates Sept 2017

Picture sources: EC SWD(2017) 295

Figure 2 Overview of measures in EU Cybersecurity Strategy (source: European Commission)

3.2 Cybersecurity Policy Measures with Relevance for Industrial Policy

The following subsections highlight the relevance for cybersecurity industrial policy, drivers, and international topics in relation to specific policy developments mentioned before. Each measure is classified where relevant in the UNCTAD scheme of trade measures and the related policy is mapped against the Carman and Harris scheme. Each measure is also assessed in terms of its policy intensity and discriminatory intent vis-à-vis foreign enterprises.

Figure 3 below provides a timeline of a number of the measures and shows the interplay between the EU level, industry and Member States, which we will return to in the next section.

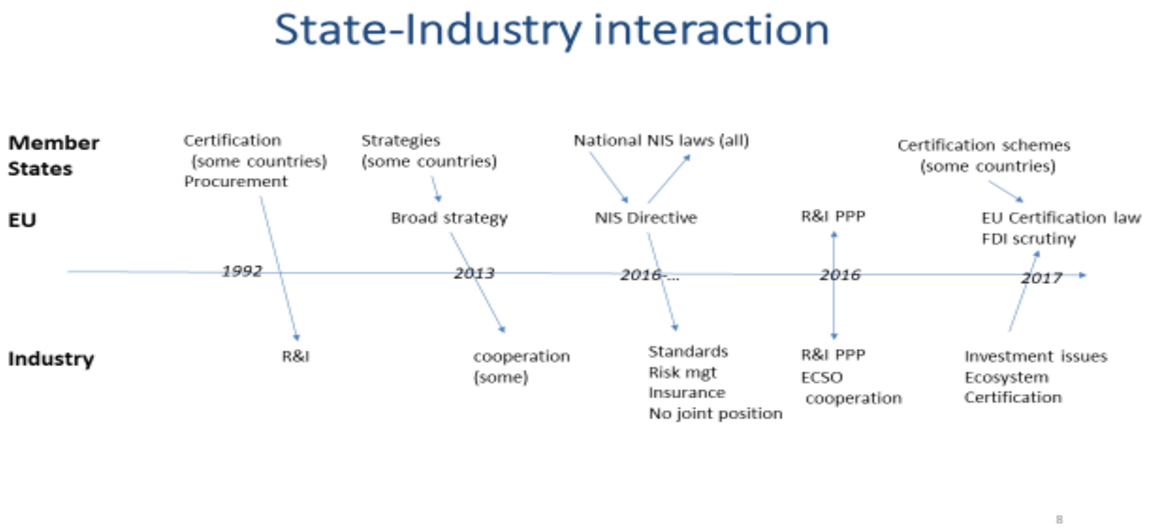


Figure 3 State-industry interaction in EU cybersecurity policy

3.3 Overall Cybersecurity Strategy

The Strategy itself cannot be considered an UNCTAD non-tariff trade measure while in terms of its economic effects it is largely enabling an arrival at a common understanding of market-related developments and can thus, analyzing it economically, be viewed as market facilitating (MF). It had a rather high effect intensity evidenced by the numerous discussions on it and its endorsement in Council and Parliament and is consequently rated '+' in Table 1 below.

3.4 SOG-IS

The 1992 Senior Officials Group on Information Systems Security and the related 1997 Mutual Recognition Agreement sought to enable a high level of security certification, to have more certified products in the market, and to eliminate duplicate evaluations. Relevant certification standards included the international ITSEC and the Common Criteria CC. The CC defines assurance levels (EAL 1-7) and procedures for ICT security certification, for selected ICTs.

SOG-IS illustrates historic dependencies in this field. It was created at a time when governments still held a major interest in critical infrastructures and security requirements (the 1985 Orange Book for Trusted Computer System Evaluation Criteria which was in 2005 replaced by the CC). As a result, the domestic defense industry was often present. Promoting the acceptance of certification through public procurement was an important. Certification and public procurement are viewed as industrial policy measures, though they were not intended as such at the time of their implementation.. CC certification is in UNCTAD terms a B83 (Certification) Technical Trade measure. It is a specific instance of modifying the characteristics of market-delivered objects (i.e. security products/services) and of market facilitation (creating common specifications), i.e. both an MM and MF measure. Even if it involves a limited number of EU member states for those it had a high impact in the market, with a well-established conformity assessment system in several countries, an effective gateway for government procurement is created, i.e. the intensity of the effect is high ('++' in Table 1 below).

3.5 European Network and Information Security Agency ENISA

The European Network and Information Security Agency (ENISA) created in 2004, has undergone a mandate renewal in 2013 and as of September 2017 a proposed mandate revision is being negotiated. ENISA's legal basis is the internal market[12]. While its main focus is on increasing cyber-resilience knowledge and capabilities (ENISA Cyberthreat Landscape, training of national CERTs, and cybersecurity exercises), ENISA also contributes to take-up and development of European legislation (NIS Directive, Certification Regulation, see below) and to standards, is expected in the 2017 proposal to become a key party in implementing an EU-wide cybersecurity certification approach and works with partners internationally. ENISA informs research priorities based on industry needs and supports private-public sector cooperation such as the contractual PPP. ENISA, as expert advisory, contributes to discussions on industrial competitiveness (ENISA 2016a).

ENISA, in a limited sense, is a Technical Trade measure (B83), though its main effects are market facilitation (MF in Table 1) next to market substituting MS (education, capabilities raising) and market modifying MM (certification). Even if ENISA is relatively small compared to several of the national agencies, it has a high profile as an authoritative cyber-resilience reference (by law and/or by achievement). Its mandate decision required intense involvement of lead policy makers in Europe amongst others because of the agency's seat. It also has intense cooperation with the European Commission for EU-level cybersecurity policy implementation and development. In terms of intensity it is thus rated as '++'.

3.6 NIS Directive

The NIS Directive (European Union 2016b) is a landmark EU law whose primary objective is strengthening cyber-resilience to ensure the smooth functioning of Europe's internal market, i.e. the free flow of people, goods, services and capital between EU Member States. The internal market legal basis shows that the NIS Directive has a strong economic anchor and is, by consequence, (but not by objective) linked to cybersecurity industrial policy.

[12] In EU parlor the internal market as a legal basis means that legislation is based upon the part of the Treaty that concerns the 'establishment and functioning of the internal market'(Article 114 TFEU).

The Directive addresses national capabilities, strategic and operational cooperation of Member States, as well as incident notification and risk management for specified market operators. It recognizes that, in the grand scheme of things, critical infrastructures are run by private sector operators, as well as recognizing that cyber protection cannot be perfect. Therefore, regulation should be limited and “a culture of risk management, involving risk assessment and the implementation of security measures appropriate to the risks faced, should be promoted and developed through appropriate regulatory requirements and voluntary industry practices.”[13] Member States must ensure risk management by the relevant service providers. Focusing on risk management also is technologically neutral, which reflects an approach often encountered in EU digital policy[14].

With regard to the international dimension, the NIS Directive states that “given the global nature of security problems affecting network and information systems, there is a need for closer international cooperation to improve security standards and information exchange, and to promote a common global approach to security issues”[15]. This translates into the possibility for international agreements with third countries or international organizations for participation in the strategic cooperation of Member States (not yet in use). It also encourages the use of European or international standards and specifications. It does not, however, put in place standardization activities.

The Directive leaves a lot of room on the national level with regard to providers of traditional critical infrastructures (called essential services providers) whereas, on the contrary, a harmonized common EU-wide approach is taken with regard to critical digital service providers. The reason for this is related to the national interest ‘market failure’ (see above).

The 2017 revised EU Cybersecurity Strategy recommends the risk management and notification approaches defined under the NIS Directive also be applied to other sectors and public administrations. At the same time, the EC issued a detailed recommendation on coordinated response to large-scale cyber incidents, beyond the NIS response. Undoubtedly this has an industrial dimension, for example secure systems will have to be deployed to enable such response.

The NIS Directive can be classified as a Technical Trade measure (product requirements B7, presence for importers B15 in case of an international agreement). Its effect is market modification (MM, for a limited part of the market). As the first and major EU cyber-resilience law and notably due to its perceived impact on national security in its negotiation, there is no

[13] Recital 44 NIS Directive (ibid).

[14] Technology-neutrality is a principle in EU telecoms legislation since 2002 though some argue that law needs to address technology in specific cases in order to counter adverse effects eg on fundamental rights, see eg (Hildebrandt and Tielemans 2013).

[15] Recital 43, NIS Directive (ibid).

doubt that it saw intense and high-level political involvement and is therefore rated in terms of intensity as '++. The NIS Directive is a relatively high-level prescription, leaving a lot of leeway for Member States and industry. Nevertheless, its impact is amplified because of its close linkage to the EU's General Data Protection Regulation (GDPR). The latter has in recent years become one of the most talked-about laws impacting the digital world. Cybersecurity breaches more than once lead to personal data breaches (the GDPR which imposes hefty fines[16]).

3.7 Certification Framework

The 2016 Communication was followed up in September 2017 with a proposed Regulation on EU-level certification framework (combined with a new mandate for ENISA). From an industrial policy perspective, this is one of the most important EU-level measures. Its objectives include increasing trust, reducing fragmentation in Single Market, lowering certification costs, and easing public procurement. It is a framework in the sense that it establishes principles, procedures for agreeing on certification schemes, and governance and should thereby be flexible, achieve EU-wide recognition, supersede national schemes based on voluntary use by industry, and promote security-by-design and 'duty of care', as well as provide for levels of security (basic, substantial, high). When using such an EU-agreed scheme companies benefit from one-stop compliance verification.

Certification can be of great importance for buyers and users of ICT-based products and services. It is also an important instrument in industrial policy. Certification may have a legal anchoring and can range from self-declaration of compliance, third-party compliance, product cyber resilience certification, to full cyber resilience certification.
Certification implies testing and validation to meet requirements as formulated in criteria and standards. Certifying bodies can be national, third-country or international agencies, sector-based organizations, third-party commercial entities or companies themselves. Specific labs can perform the actual testing and validation.
Many products and services are self-certified or not certified at all such as most consumer equipment like printers, TVs, baby-monitors, and other IoT/connected devices.

Preparation for the proposal made in 2017 on a Certification Regulation benefitted from the expertise of ENISA, SOG-IS members and industry and input from EU cyber-certification projects such as ERNCIP[17] on an Industrial Automation Control Systems[18].

[16] A personal data breach due to non-compliance with its security principle (GDPR Art 5.1f) can be fined up to 4% of worldwide annual turnover. GDPR Art.32 spells out security requirements appropriate to risks.

[17] https://erncip-project.jrc.ec.europa.eu/.

[18] See e.g. https://www.enisa.europa.eu/events/ict-security-certification-for-industry/ict-security-certification-for-industry-meeting-minutes.

Existing certification criteria include important international schemes ITSEC, Common Criteria, ISO 27001. An existing governance scheme in Europe is SOG-IS MRA. Existing certification bodies include BSI in Germany and ANSSI in France. Security certification can also be done by sector-specific organization e.g. in banking, energy, or telecommunications. An example is the GSMA organization of mobile operators and equipment vendors.

EUlevel cybersecurity certification must be organized against the backdrop of national level activities since national security is excluded from the EU Treaties as well as a result of the emergence of lightweight certification such as the French Certification de Sécurité de Premier Niveau (CSPN) and sector-specific and general ICT schemes (such as for cloud and IoT).

A general EU scheme for the accreditation of certification bodies and other market surveillance measures is the 2008 EU Regulation on Accreditation and Market Surveillance (RAMS). In RAMS, based on the internal market, mutual recognition is an essential element, mutual recognition meaning that certification done by an accredited body in one country is sufficient for the whole EU market. For certain product categories international mutual recognition agreements (MRAs) also exist, with anchoring in the RAMS regulation. RAMS is not applicable for cybersecurity MRAs such as the SOG-IS MRA or the CC-MRA. Of importance is the fact that the 2017 certification proposal foresees accreditation of conformity assessment bodies consistent with the RAMS regulation, which would bring cybersecurity certification (for the relevant schemes) firmly into the fold of the Single Market.

Both the 2016 Cybersecurity Strategy Communication and the 2017 Certification Regulation affirm that a framework for security certification of ICT products and services should account for developments on the international level with international partners and that certification schemes should be built upon internationally recognized or EU standards.

Other relationships to be considered for certification are data protection (GDPR refers to ensuring a level of security appropriate to the risk) and consumer protection. While consumer legislation and product liability is harmonized across the EU, existing legislation does not fully cover cybersecurity liability for consumer or IoT products (Cybersecurity Raad 2016).

The certification measure would constitute a B83 Technical Trade measure. As this is about voluntary certification, this measure concerns both market facilitation and market modification (MF and MM). As shown above, it is generating a rather high level of political engagement, although ground has already been broken by the NIS Directive (therefore intensity '+'). However, given significant industry interests and the relation to established interests in national level certification (notably SOG-IS) for which one – potentially contentious - option is that it will get 'Europeanized' it is not excluded that intensity will increase to '++' (pending the outcome of negotiations on this legislation).

3.8 Supporting Research & Innovation (R&I) and Cyber-Competence

At the EU-level, funding for cybersecurity R&I was only available as part of general ICT research until 2012 when that policy changed. Since the end of the 1980's, ICT accounted for about 20% of the budget of the seven consecutive EU Framework Programs for research and technology development. Security R&I, addressing physical resilience and crime, had, in parallel, been growing as a separate part of EU funding. EU Member States decide jointly on the contents of EU R&I upon proposal by the EC, which on its turn performs extensive consultation with stakeholders, usually every two years. Associated countries such as Israel, Norway, and Turkey are also involved.

With a major restructuring in 2012, EU R&I security and cybersecurity applied research were put together getting their own identity within Horizon 2020, the 8th Framework Program. Nevertheless, ICT technology research with strong relevance for cybersecurity continued within the ICT part of Horizon 2020. Some applied cybersecurity research got also included in the health, energy and transport parts of Horizon 2020. Altogether this evolution reflects the growing importance and coherence of cybersecurity R&I, though it still only has a moderately-sized budget[19]. The budget, about 2 B€ over 7 years, included a substantial industry contribution which was strengthened by the 2016 contractual private-public partnership (cPPP). That last measure is an example of both market creation (the right to influence EU level R&I strategy) and market facilitation (the partnering aspect).

Public support for R&I can be classified as an UNCTAD Subsidies (L) measure and is market substituting (MS). In the past, deciding upon R&I in this field was politically a relatively low-intensity activity. Recently this has been changing due to increasing cyber threats to economic, societal, and democratic autonomy as well as the increasing prevalence and use of words like 'strategic autonomy' and 'digital sovereignty' (without being well-defined) are used in conjunction with calls for stepping up EU-level R&I cybersecurity although it is usually not the most powerful ministries that get involved in R&I programming. Therefore, in terms of intensity of engagement, this can be rated as '+'. Generally, companies from third countries can participate to the EU R&I programs subject to certain financing restrictions under rules for participation that are not specific to cybersecurity. Additionally, in the field of cybersecurity, security scrutiny is applied which does not *a priori* discriminate with regard to the country of origin of a participant.

As mentioned above, in 2018, a proposal is expected to support networking of cyber competence centers. This is also to include a European Research and Competence Centre. Some priorities

[19] In June 2018 the European Commission proposed a budget of 2 B€ for cybersecurity development and deployment as part of a new Digital Europe programme. This would come on top of research and innovation funding in the new Horizon Europe programme which is the successor to Horizon 2020 for the period 2012-2017.

might be assistance to certification and professional skills development, as well as research on encryption. Importantly and consistent with a general trend of bringing civil and defense sectors closer together is that this facility could also address cyber defense 'in full respect of the Treaty provisions related to the Common Security and Defense Policy'. These market-substituting measures (MS) do not fall within the UNCTAD classification. So far, they have received a moderate level of political and administrative attention (rated as '0' in Table 1 below). No specific restriction is mentioned for foreign participation.

3.9 Other Cybersecurity Policy Measures

Above, several measures related to the *resilience* dimension of cybersecurity have been analyzed. Other measures address awareness and capability building and cyber exercises as well as international cyber dialogues. They are classified in table 1 as well. As an example, support to capability building is mainly concerning national CERTs, provided by ENISA and complementing the NIS Directive. This is a market substituting measure, MS. For the Member States with weaker capabilities this has an important effect, therefore the intensity is rated '+'.

In addition, in the EU, many policy developments have been taking place related to combating cybercrime, terrorism, and state actor threats. Examples are the 2013 Directive on Attacks against Information Systems (European Union 2013) and the 2016 Communication on a Joint Framework on Countering Hybrid Threats (EC and EEAS 2016). Such policies and measures often call for raising awareness of and enhancing of cooperation with providers and promoting the adoption of solutions from the cybersecurity industry and security standards, thus having (indirect) industrial impacts. They also generally promote cooperation with third countries.

There is a gradual rapprochement between the civil and defense worlds, with the update in 2017 of the EU Cybersecurity Strategy referring to enhanced EU-NATO collaboration in response to hybrid threats (EU-NATO 2017) and in research & innovation, next to references to cyber defense competence and research as mentioned above.

3.10 Related Digital, Horizontal and Sectoral Policies

Digital Single Market DSM

Cyber-resilience policy is firmly anchored in the EU's digital policy, the 2015 Digital Single Market (DSM) strategy. DSM addresses digital economic and social development in the broad sense. Its 16 concrete measures are now being implemented or subject to legislative negotiation.

In DSM, parlor cybersecurity safeguards trust in the digital economy and society and is one of DSM's priorities. DSM highlighted the industrial dimension by calling for a more joined-up approach to step up the supply of more secure solutions by EU industry and to stimulate their take-up by enterprises, public authorities, and citizens. The 2016 contractual partnership and 2016 Strengthening Communication are implementing this part of the DSM strategy.

In other DSM actions, cybersecurity, in its industrial dimension, also plays a prominent role. Examples are the 2016 ICT standardization policy, IoT and cloud strategies as well the Digitizing Industry initiative (cf Industrie 4.0). The May 2017 review of the Digital Single Market policy re-iterated the commitments of the 2016 Strengthening Communication and also expressed the intention to enhance international cybersecurity cooperation with main trade partners on cybersecurity for IoT.

One of the measures preceding the DSM was the Regulation on electronic ID and trust services (eIDAS), adopted in 2014. In an important area of cybersecurity (notably e-IDs and e-signatures) eIDAS puts in place a process for certification based on high levels of security and (preferably) standards. Reducing market fragmentation and creating a legal basis for the acceptance of electronic identification and authentication, this Regulation stimulates the related supply-side industry as well as major user industries such as banking to take up such solutions. eIDAS foresees recognition of trust service providers established in a third country be it subject to recognition under an agreement concluded between the EU and the third country. International aspects are amongst others dealt with in UNCITRAL and bilaterally e.g. EU-USA.

General Data Protection Regulation GDPR

Among the horizontal policies, the General Data Protection Regulation (GDPR), adopted in 2016 and entered into force on 25 May 2018, should be mentioned. The GDPR obliges to take proper information security measures to protect personal data. The NIS Directive and the GDPR work back-to-back if a cyber incident leads to a data protection incident, which often will be the case. Data protection issues may also arise in incident handling and information sharing between CERTs. The GDPR – while based on protecting a fundamental right - influences innovation in the cybersecurity industry as well as trade. A prime example of the latter are the EU-US and EU-Switzerland Privacy Shield agreements. Such agreements show the importance of bilateral cooperation and illustrate possible models for wider international agreements.

FDI scrutiny

Related to the updated Strategy of 2017 is a proposal for a Foreign Direct Investment (FDI) regulation responding to concerns about strategic acquisitions of European companies with key technologies by foreign investors, especially state-owned enterprises. This FDI measure can be considered in UNCTAD terms an I9 trade-related investment measure with its effect intended to be market proscribing (MP, see also Table 1 below). The debate about FDI has reached the highest political levels and therefore has a rather high (political) intensity level. It remains to be seen, however, what its effect intensity on the market is, given that negotiations still are ongoing on this proposal and EU competence for FDI scrutiny is contested by some countries and the proposed measure itself is not very constraining (rated ‘0’ in Table 1).

Export controls

The EU establishes export controls, implementing a.o. the Wassenaar Agreement. In September 2016 a significant revision of the export controls regime was put forward by the EC (European Commission 2016b), introducing a 'human security' dimension in export controls applicable to certain cyber-surveillance products that result in violation of human rights. This is in UNCTAD terms a P13 Trade Measure and is market proscribing (MP) affecting specific but limited parts of the EU cybersecurity industry. The debate on export controls in the EU tends to have a moderate political profile although European Parliament engagement can be significant at times as is also the case for industry lobbying. In terms of intensity this is therefore rated '0'.

Horizontal and sectoral industrial policies

Horizontal EU industrial policy (European Commission 2017a) which updated in 2017 following a request by the Council (Council of the EU 2017) does not directly add to cybersecurity industrial policy measures but instead cross-references measures mentioned above.

On the contrary, sectoral policy development increasingly addresses cybersecurity with significant industrial consequences. One might expect that EU security industrial policy would be *primus inter pares* amongst sectoral policy, but at the time this was developed, in 2012, 'cyber' was hardly articulated (European Commission 2012c). Clear other examples, though, are the recently proposed revision of legislation in the field of electricity which addresses responsibilities of market actors and codes for network operation (particularly the proposed Regulation on risk-preparedness in the electricity sector which complements the NIS Directive and the related draft Electricity Market Regulation) and the ongoing cooperation of industry and authorities on intelligent transport systems in the C-ITS Platform addressing issues such as encryption standards for connected cars.

Sectoral work has also their own international platforms. For example, the USA, Japan, and the EU have jointly discussed intelligent transport systems and the EU and the USA have discussed the definition of a smart grids reference framework. Rich insight in the variety of authorities involved in cybersecurity and certifications in fields such as electricity, health, rail transport, and telecoms can be found in (ENISA 2016c).

3.11 European Parliament and Council of Ministers

While the EP cannot propose legislation itself, it does put forward influential studies such as (European Parliament 2015) and political statements. The Council of Ministers can also come forward with own-initiative statements.

Two examples of work of the EP are a 2013 Report and a 2014 Resolution on the Snowden affair. These have clear references to industrial policy measures such as calling "on all the Member States, the Commission, the Council and the European Council to give their fullest support […] to the European innovative and technological capability in IT tools, companies and providers […] including for purposes of cybersecurity and encryption and cryptographic capabilities; [the EP] calls on all responsible EU institutions and Member States to invest in EU local and independent technologies […]" (European Parliament 2014). The Council of Ministers established a Cyber Issues Horizontal Working Party (formerly Friends of Presidency Cybersecurity Group) which addresses a.o. the EU cyber defense industrial capability (Council of the EU 2014). Cybersecurity is also discussed in sectoral Council formations (e.g. telecoms, maritime). Much work has also been undertaken to address hybrid threats amongst others by the development of a diplomatic 'toolbox'.

3.12 Classifying Measures

An overview of the above-mentioned measures is in Table 1 below, which applies the UNCTAD international classification of non-tariff measures (UNCTAD 2015), the Carman and Harris framework for intervention intent (Harris and Carman 1984), and adds the intensity of the effect of a measure on the market, and whether or not it differentiates between domestic and foreign firms.

If there are no trade restrictions at EU-level, there may still be such measures at a national level. For example, it has been reported that some Chinese ICT suppliers were excluded from specific instances of public procurement in Germany and in the UK due to security concerns (Economist 2012).

Table 1 Classification of European cybersecurity measures with industrial relevance (intervention type abbreviations: MC = Market Creating, MF = Market Facilitating, MM = Market Modifying, MS = Market Substituting, MP = Market Proscribing)

Measure	**Category (UNCTAD)**	**Intervention type**	**Intensity (--,-,0,+,++)**	**Discrimination**
Cybersecurity Strategy (2013, 2017)	Not applicable	MF	+	No
SOG-IS	B	MM, MF	++	No
ENISA agency Regulation	B (only some activities)	MF, MS, MM	++	No
Network & Information Security Directive	B (partially)	MM	++	No (international agreements possible)
Certification Regulation (proposed)	B	MF, MM	+, possibly becoming ++	No
EU R&D support	L	MS	+	Yes (rules for third country participation)
Private-Public Partnership for R&D	Not applicable	MC, MF	0	No
Cyber-dialogues (bilateral)	Not applicable	MF	0	Possibly (each side may involve industry)
Awareness raising	Not applicable	MF, MS	-	No
Capability building	Not applicable	MS	+	No
Cyber-exercises	Not applicable	MS	0	Case-by-case
Competence centre + networking (proposed)	Not applicable	MS	0	No
FDI scrutiny (proposed)	I	MP	+	Yes (by definition as it is about *foreign* investment)
Export controls	P	MP	0	No

4. State-Society Dynamics

4.1 Industry Responses

In the early days of cybersecurity, industry involvement was limited to a few topics such as identity and secure access management. The smart cards international industry organization Eurosmart 20 years ago responded to the 1999 EU Directive on electronic signatures and more recently to the eIDAS Regulation. Defense and internal security industries successfully took action to raise EU level support for security R&I in the early 2000's. Cybersecurity was hardly present in that picture, though. At that time, ICT and telecoms also promoted some cybersecurity technology research within mainstream EU ICT R&I, with an interest in certification within their domain, however, without there being a comprehensive industrial approach.

The significantly increased attention to cybersecurity in 2012/2013 included addressing industrial relevance in the 2013 Strategy, which called for closer private-public cooperation and market development. Immediately following the adoption of the EU Cybersecurity Strategy early 2013, an informal consultative cooperation with industry was set up by the European Commission – the NIS Platform. Public administrations were also welcome to this Platform to which some 200 parties joined amongst which a significant number of international companies with headquarters outside the EU, notably in the USA. The intention was to develop common understanding and specifications related to selected economic and industrial aspects of the Strategy. The NIS Platform concentrated its efforts on risk management, incident information sharing, and a future R&I agenda.

Subsequently, supply and demand in cyber-industry has become increasingly more organized, with the creation of groups such as in 2015 the high-level industry group ECIL mentioned before, the growing interest in cybersecurity amongst the security industry working together in the European Security Organisation ESO, and ultimately, with the formation of a new broad industry alliance, ECSO, in 2016. Its creation was also catalyzed by the EC's political intention to give greater strategic focus to R&I money in the Horizon 2020 program. ECSO's agenda goes far beyond R&I, addressing all of the industrial topics in EU cybersecurity policy and pro-actively defining further agenda items. Given its interesting model, we return to ECSO below.

Sectoral organizations also increasingly play a role in policy. In energy, there is the ENCS, in banking, cybersecurity is part of the established and international banking cooperation in SWIFT, and cybersecurity is a top priority in new sector coalitions such as the EATA alliance on connected and automated driving. The European Commission has been stimulating the emergence of sector-specific cooperation, for example by setting up a cybersecurity energy experts group, addressing cybersecurity in stakeholder cooperation for intelligent road transport

C-ITS and providing a joined-up political vision which helped bringing together automotive and telecoms industry on automated driving in EATA. Industry cooperation is also promoted by sector-specific agencies such as EASA for aviation in Europe.

Industry responded in a variety of ways to the proposed NIS Directive, which shows the groupings of interests in industry:

- A number of ICT service and cloud companies, mostly from the US, have argued strongly against any regulation of internet platforms and services (e.g. mandatory incident reporting, adhering to minimal requirements), predictably given their ‘no regulation’ approach frequently advocated for digital policy. The final NIS Directive includes obligations for online marketplaces, search engines, cloud service providers but not for social networks.
- Providers in physical critical services infrastructure were less vocal and engaged. An explanation for this phenomenon may be greater national orientation, lower levels of awareness, and already being accustomed to a regulated industry.
- Smaller companies, though responding to public consultations, had less of a voice due to a lack of cybersecurity SME industry organization at the EU level and the fact that cybersecurity was not yet a top-level issue for broad-based SME organizations.
- The few established industry organizations that are close to cybersecurity did make themselves well heard, generally being supportive of more regulatory clarity and certainty.
- Finally, hardware/software suppliers were not directly targeted by this cyberlaw though it was suggested by some parliamentarians.

In the 2017 preparatory phase for EU certification, US-based suppliers argued against regulatory approaches, whereas European semiconductor industry takes a more nuanced approach. The EC proposal of September 2017 has a mixed approach: voluntary use of certification schemes but mandatory EU-wide recognition.

4.2 Industry Organization - ECSO

ECSO has over 200 members, of which about half suppliers, one quarter users and one quarter research organizations (see Figure 4 below). They are spread across Europe with the largest numbers of members from Italy, Spain, France, Germany and UK. Internationally headquartered companies need to have a legal entity in the EU (eg Ireland for IBM).

ECSO is an interesting case study of industry response in itself. Its formation was clearly in response to EU cybersecurity and research & innovation policies, but it is developing a momentum beyond these. ECSO’s interest went beyond being involved in the programming of EU R&I funding only. Their cooperation therefore would address a broad agenda, including standardization, certification, investment, education, next to R&I, and involve not only industry but also public authorities.

Firstly, ECSO provided the private sector signatory to the R&I contractual private-public partnership with the European Commission. Secondly, ECSO decided to go well beyond R&I and also address topics such as the industrial ecosystem, investment, certification and others, all topics already identified by ECIL but not all corresponding to EU policy documents. Thirdly, ECSO decided to build a broad industrial membership of both large and small companies, both suppliers and buyers, and even being open to white hacker communities. Fourthly, ECSO decided to bring in public administrations from Member States, in their role as buyers and influencers of procurement specifications. Finally, ECSO is open for international participation (eg US, China, Israel, Norway) notwithstanding that its initiators were EU-originated companies and the concerns as expressed eg by ECIL about the lack of European competitiveness notably in the face of US competition and potential national concerns.

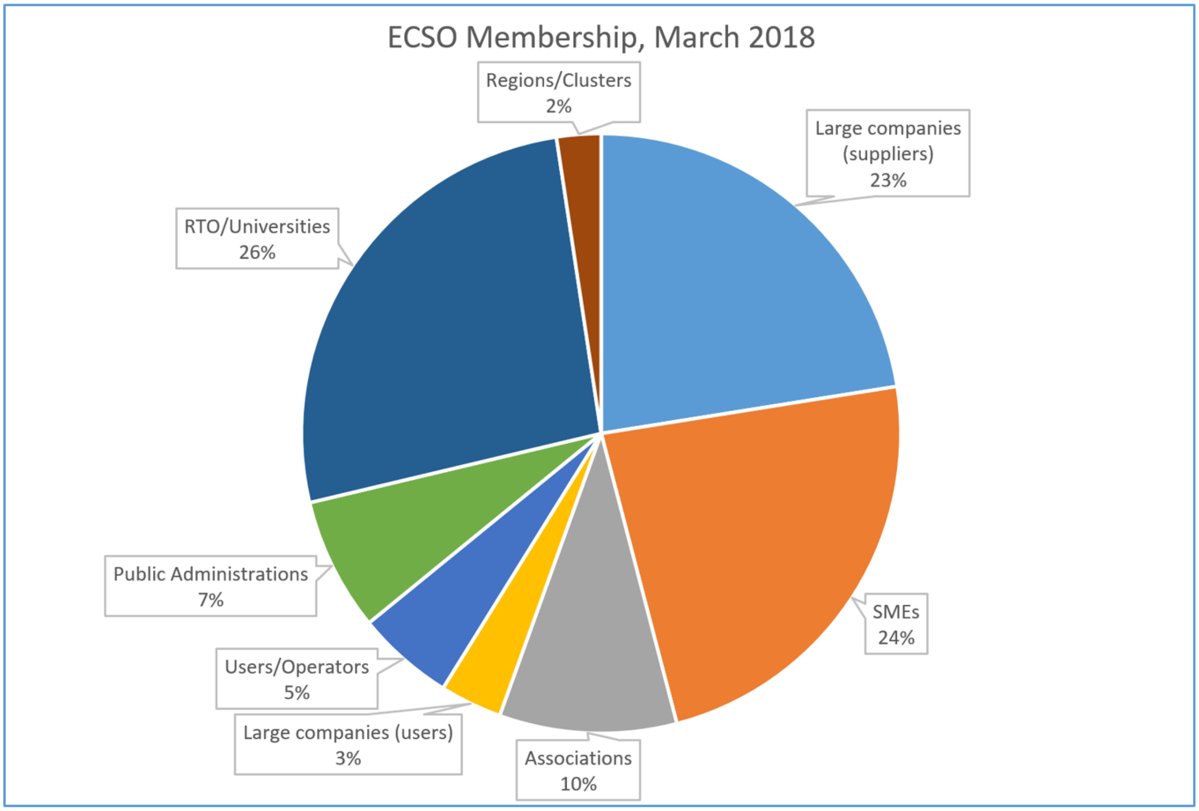


Figure 4 ECSO Membership as per March 2018, data from ECSO (https://www.ecs-org.eu/).

4.3 Member States Responses

One may also wonder how Member States react to the EU-level policy developments. Cybersecurity law (notably the NIS Directive) is still too recent to see whether countries properly implement these. In addition, EU law often includes voluntary cooperation and guidance which may be effective too. For example, in the field of cyber incident management in telecommunications, common European guidance from ENISA is used by 40-60% of NRAs (ENISA 2016d).

In a number of Member States, strong differences of interest arise between the intelligence/military/home and economics/digital departments. This may vary from country to country, being historically and geographically contingent. These internal fights in countries (for example in Sweden and Finland) certainly complicated the negotiations on the NIS Directive[20]. Moreover, for various reasons countries are less willing to yield influence at the European level. The UK, for example, often tended to favor minimal regulation (and attempts were made to contest the Single Market legal base). Such tensions are also likely to increase the gravity of future negotiations on certification, where the 'Europeanization' of the SOG-IS framework may become a test case or in the debate on encryption.

On specific topics, the thinking may be shifting. An illustration is provided using government buying power. While, as in the past, a security perspective is important in Europe, it is also increasingly viewed from the perspective of 'government as a launching customer', like other areas of the digital economy such as e-government (SOG-IS/ENISA 2014). Another important illustration is in the increasing pursuit of synergies between civil and defense work.

It may appear that the economic vector has generally been increasing in strength, corresponding to growing digitization of economy and globalisation, but whether this is true remains to be seen given the parallel rise of internal and external threats (Kello 2017). In industry, as well as inside governments and between countries, this manifests itself in a range of opinions on topics such as encryption or the balance between European and international cooperation.

At the sub-national level (regions), clustering is increasingly seen as an opportunity, i.e. demand-supply linkage, involvement of authorities, triple helix approaches. An ECSO study identifies in at least 14 European countries such clusters[21].
Facilitating the interplay of authorities and industry is an important role for ENISA, though it is a relatively small agency. It developed simultaneously with industry smart grids cybersecurity specifications and has a role in the NIS Directive to work with industry. ENISA is working with industry on cyber insurance. This helps flesh out risk management as required by the NIS Directive and may stimulate the cyber insurance industry[22]. ENISA is also working on

[20] The Directive states that essential services have a direct link to physical infrastructure and therefore Member States can identify essential service operators nationally and impose stricter requirements. To some extent, however, this differentiation is part of the trade-off between international and national interests. It is an open question how this will evolve since traditional infrastructures (transport, energy, etc.) increasingly become digitized and rely on global digital platforms as foundations of their business.

[21] (ECSO 2016) and Luigi Rebuffi, private conversation.

[22] ENISA workshop 6 Sept 2017 on cyber insurance, https://www.enisa.europa.eu/events/enisa-validation-workshop-on-cyber-insurance; (Woods and Simpson 2017).

certification with semiconductor industry[23]. In 2017 ENISA's resources and mandate have been proposed to be strengthened.

Finally, in line with the regular way of policy development, the EC consults widely with industry. In 2017 consultations were launched a.o. on certification and the future of ENISA.

4.4 Conclusions on State-Society Interaction

Several conclusions can be drawn, though it is understood that evidence is limited. Firstly, industry has strongly expanded its interest and organization at the EU-level in cybersecurity since 2013. Secondly, historically industry appeared to have been more reactive to EU policy but recently timing and themes are more aligned. A two-way and mutually s synchronised relationship between the private sector and EU-level public sector and agencies is growing. This mirrors developments in Member States. This shift is illustrated in the state-industry interaction diagram (Figure 3 above).

Thirdly, it is clear that industry is not a homogeneous block and divided on many issues while pursuing combinations of competitive and cooperative behaviour. Still industry is finding enough common ground and can work together in EC-sponsored settings. Moreover, industry's recent approach (in ECSO) is to bring many interests together including working closely with public authorities, being rather open to the diversity of interests and experiencing a strongly growing interest to take part in this 'movement'. In this sense, ECSO may fit the mould of Multi-Stakeholder Organization that are considered essential for the emerging digital governance of the future (Cowhey and Aronson 2017). Whether the approach will be effective for implementation and further development of industrial policy measures cannot yet be said.

Another observation is that outright rejection by industry of any form of regulation in cybersecurity is not a winning strategy. There is likely insufficient support for such position from Member States. More success can be expected by bringing to the table sophisticated analysis as is happening in mature fields like telecoms or copyright, combined with commitment to complementary action like self-regulation.

Altogether, the dynamics of industry-state interplay is still developing much at EU level and certainly more mature than just a few years ago, even if resources both in industry and with governments and policy makers still seem to be much smaller than in the USA.

[23] Such as on certification by Infineon, NXP, STMicroelectronics and ENISA, https://www.enisa.europa.eu/news/enisa-news/enisa-works-together-with-european-semiconductor-industry-on-key-cybersecurity-areas, May 2017.

5. Conclusion and Challenges

As can be seen from this analysis, most measures concern market facilitation, market modification, and market substitution. They fit well with the logic of the Single Market model mentioned at the start of this paper: safeguarding the free flow of goods, services, capital and people between the EU Member States. Reinforcing the common vision through the EU Cybersecurity Strategy and joint political declarations makes these measures more effective. This contributes to 1) unlocking - to a degree - the debate on national security and sovereignty and 2) reducing national lock-in and 3) keeping measures driven by internal security and external relations objectives consistent with the economically-driven Single Market objectives. Figure 5 illustrates some of the dynamics of EU cybersecurity industrial policy-making.

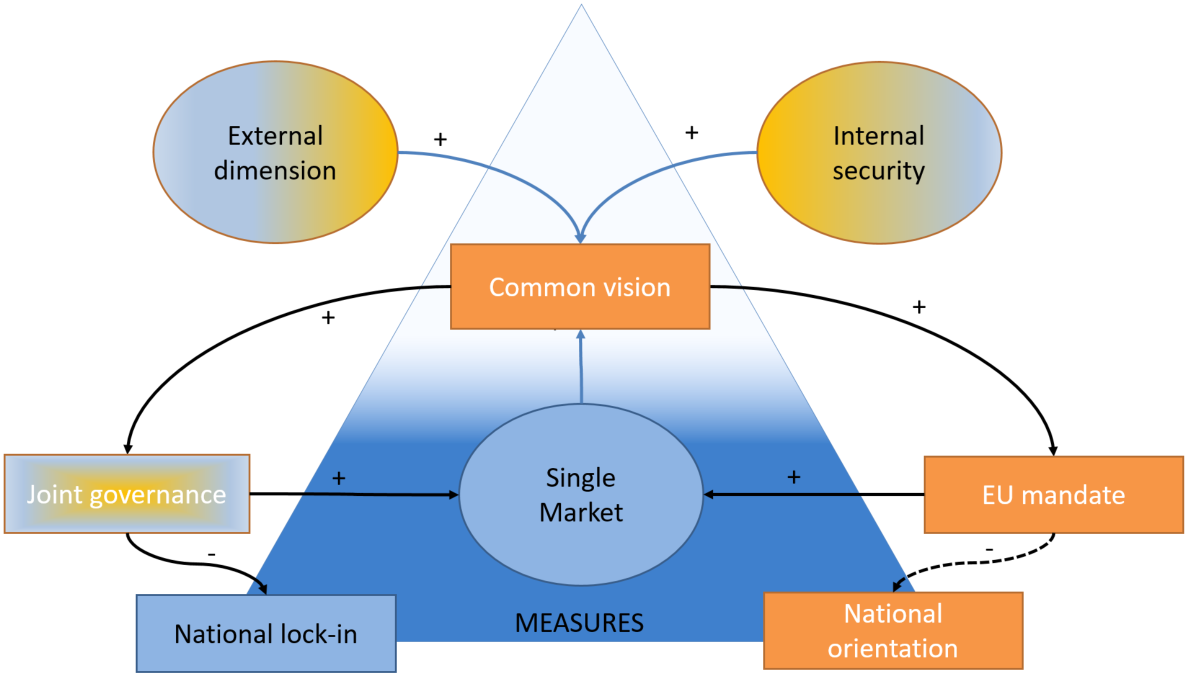


Figure 5 Illustrating dynamics of areas of policy interests and political (orange) or economic (blue) 'market failures'

In the remainder of this chapter we address challenges and limits to this model and elaborate on the perspectives that lessons learned provide on possible international cooperation or governance and agenda-setting.

5.1 Conflicts and Challenges to Address

Lack of coherence, incompleteness

Coherence and completeness of cybersecurity policy is growing but is still limited. Investment-related policy measures are only starting to be addressed, public procurement or dual-use has not yet been fully analyzed, and trade issues in cybersecurity remain a subject of discussion. Several sectors are gearing up such as finance, energy, aviation, but other sectors, such as healthcare, are lagging. New technologies such as AI are not yet fully addressed. Security interests do not always align with economic interests. Industrial measures can be contingent upon progress in international cyber diplomacy addressing norms and values of state behavior.

In many measures in Europe the strategic intent over many years has been around political objectives such as fighting crime and avoiding disruptions in the internal market rather than being focused on industrial policy objectives. It is only recently that the strategic objective of overcoming cybersecurity economic market failures has been formulated more explicitly. But this does not mean that economic objectives now dominate: with the growing impact of cybersecurity attacks and incidents both non-economic and economic objectives have risen on the political agenda. They also get more interlinked, for example the rise of state-sponsored cyber espionage increases concerns about national competitiveness and concerns about resilience rise with the growth of digital platforms that critically underpin national and international business operations. Similarly, there is an increasing interest to seek synergies between civil and defense in cybersecurity.

Politicians like Chancellor Angela Merkel and President Emmanuel Macron have been exposed to cyber incidents before and during election seasons. With massive cyber intrusions, budgets for national cybersecurity agencies have been increasing against the general trend of public sector cost-cutting thanks to attention of the top European leaders. Cybersecurity as a high political priority transpires from European Councils by Heads of State and Government and EU Presidencies[24]. Political guidance of top political leaders is sometimes necessary to unblock deadlocks arising from tensions between governmental departments[25].

At the EU-level, there is a gradual strengthening of cross-linkages, cooperation and common vision. Examples are the strengthening of horizontal coordination in the Council of Ministers, the 2013 Strategy and its 2017 revision, the inclusive approach to industry organization, and joined-up involvement in international and bilateral dialogues of the relevant departments of the European Commission and the External Action Service.

[24] Cybersecurity was a main theme at the Digital Summit of Heads of State or Government held under the Estonian Presidency of the Council of the EU, 29 Sept 2017.

[25] EC President Juncker made such an appeal in the run-up to the Sept 2017 Digital Summit.

Nevertheless, the fact that there is as no unifying EU-level cybersecurity *industrial policy* as such is a sign of incompleteness, let alone that such policy could bring the necessary coherence.

Lack of trust and understanding

Lack of trust and understanding hinder market development. There are at least two causes: one is that part of what needs to be secured remains hidden, whether intellectual property, personal data, national critical infrastructure and the military/intelligence domains. The second is that much of cybersecurity socio-technical dynamics remains poorly understood. This is exacerbated by the tension between the high-speed development of technology and cyber-exploitation (crime, espionage, etc) and the much lower speed of policy development. Trust got hit by the Snowden affair and the rise of cyber-industrial espionage is a major concern.

These are not exclusive EU challenges, however, and indeed, dealing with them also requires international effort and a combination of formal and informal forms of governance (see also below). Academics have a role and responsibility to be involved and can readily do so for example in 'track II' settings.

Moreover, the tension between EU-level and national level is a well-known challenge of industrial policy in the EU (Pelkmans 2006). In the case of cybersecurity national security concerns add to this and we have to take into account that dealing with those is not in the mandate of the EU.

5.2 International Issues

The international dimension has become ever more prominent for EU cybersecurity industrial policy even if most efforts so far have concentrated on the EU-level. Firstly, there are concrete areas where international cooperation is happening such as risk management specifications, standardization, awareness raising, and broad industry cooperation. More areas can be envisaged: certification, future R&I, even contested themes such as information sharing, encryption, minimum assurance procedures (e.g. source code disclosure, and investment).

Secondly, aside from politicians, industry leaders also emphasise international cooperation. For example, ECIL industrial leaders stated that 'harmonization of standards and best practises with the US is essential' and saw the NIS Directive as helpful in that regard (even though that Directive only prescribes requirements and encourages standardization). International orientation shows from willingness of ECIL leaders to accept or critical infrastructures also internationally recognized requirements e.g. based on ITIL, SAS 70, or NIST.

Thirdly, international cybersecurity efforts related to industrial policy are also influenced by international work on horizontal policies such as data protection, fight against terrorism and crime, and export controls, and the same for sectoral policies.

Fourthly, institutional international cooperation has well-established formal platforms such as EU-third country cyberspace dialogues and digital policy. At the same time such international cooperation is also influenced by direct country-level cooperation, reflecting the well-known two-level approach to industrial policy in Europe (namely EU vs national).

5.3 Towards an International Agenda for Cybersecurity Industrial Policy

One conclusion is clear: there is no international common agenda of cybersecurity industrial policy issues nor a corresponding governance mechanism. In fact, there appears to be a contradiction between 'international' and 'industrial policy', but as the EU case shows, in fact, there are several feasible win-win scenarios
Accepting that it makes sense to move towards an international cybersecurity industrial agenda we can give some pointers regarding its relation to other international agendas, its governance, and – easiest of all –, its contents.

Firstly, **on context**, we have recognized that cybersecurity industrial policy or – better – industrial policy measures are related to other policies, whether other cybersecurity policies or other policies for example external or internal security, trade policy, data protection, digital or sectoral policies. For now, several of these policy venues have not yet been fully mobilized for cybersecurity industrial policy – trade policy being particularly interesting as there is already an established tradition to deal there with market barriers internationally. Almost self-evident but still important to stress is that not only domestic, EU or international legislation is a policy tool but also self-regulation, industry or multi-stakeholder agreements, standardization, financial support, common political vision – and this is an incomplete list.

Secondly, **on governance**, an international agenda is not a matter of governments alone, despite the strong role of national security. Following (Cowhey and Aronson 2017), governments alone will not cope with the speed of technological development and the disruption ICT brings to many business models. One would add here, there is a fear that the cybersecurity world may also bring extreme and abrupt disruption at a large and systemic scale to administrations, companies, and citizens. In addition, we have to live with intrinsic trust and understanding gaps that hold even more internationally.

Consequently, we need to consider governance of an international cybersecurity industrial agenda beyond traditional forums and platforms and address informal as well as formal routes. This certainly implies a key role for multi-stakeholder organizations of various sorts in a range of partnerships with governments as addressed by (Cowhey and Aronson 2017). These should include sectoral ones. A reference case might become connected and automated driving which likely requires future international agreement on common approaches to safety and thereby to cybersecurity in relation to transport infrastructure. Fortunately, with the maturing of stakeholder organization and the mainstreaming of cybersecurity in many sectors of the economy there is a basis to build upon. The transition from Safe Harbour to Privacy Shield for data protection also illustrates that richer forms of governance (for example, appeals, Ombudsman) can be constructed to provide adequacy safeguards.

Thirdly, **on contexts** for such an agenda we can readily list a number of topics: requirements definitions and classification, c.f. work done by NIST, standards, certification including procedures and levels of assurance, c.f. the historic CC-MRA and SOG-IS work (already more difficult), encryption (likely very difficult), awareness, skills and knowledge building including international cyber exercises, access to expensive testing facilities, up to and including well-known WTO work on technical barriers to trade as well as schedules and regimes such as for trade in services.

Obviously, we should not be naïve: the agenda we discuss here will be affected by complications in related agendas such as the issue of national security in the WTO. Governance will suffer if internet governance, trade forums, or international agreements get contested. Europe's role depends on the shape and mandate of the EU (c.f. the Brexit debate).

Therefore, international discussions on cybersecurity industrial policy cannot be decoupled from large-scale political developments around globalization versus national sovereignty, erosion of trust, nationalism and populism, and competition for control of powerful digital technologies, platforms and data.

References

Aggarwal, Vinod and Reddie, Andrew (2018) "Comparative Industrial Policy and Cybersecurity: A Framework for Analysis," BASC Working Paper Series, 2018-01.

Aggarwal, Vinod and Reddie, Andrew (2018) "Comparative Industrial Policy and Cybersecurity: The U.S. Case," BASC Working Paper Series, 2018-02.

CBInsights. 2017. *Cybersecurity Exits Timeline.* 31 5. Accessed 03 07, 2018. https://www.cbinsights.com/research/cybersecurity-exits-acquisition-merger-timeline/.

Council of the EU. 2014. “EU Cyber Defence Policy Framework.” 18 11. http://www.europarl.europa.eu/meetdocs/2014_2019/documents/sede/dv/sede160315eucyberdefencepolicyframework_/sede160315eucyberdefencepolicyframework_en.pdf.

—. 2017. “Press release 283/17, ‘Conclusions on a future EU industrial policy strategy’.” 29 05.

Cowhey , Peter F, and Jonathan D Aronson. 2017. *Digital DNA.* Oxford University Press.

Cybersecurity Raad. 2016. “Public-private-academic recommendations to the European Commission about Internet of Things and Harmonization of duties of care.” https://www.cybersecurityraad.nl/binaries/Report%20European%20Foresight%20Cyber%20Security%202016_tcm56-102235.pdf.

EC and EEAS. 2013. “Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace.”

EC and EEAS. 2016. “Joint Framework on countering hybrid threats, a European Union response.” http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016JC0018&from=EN.

EC and EEAS. 2017. “Resilience, Deterrence and Defence: Building strong cybersecurity for the EU.”

ECIL. 2016. *Recommendations on Cybersecurity for Europe.* European Cybersecurity Industry Leaders. https://ec.europa.eu/digital-agenda/en/news/commissioner-oettinger-receives-finalreport-european-cybersecurity-industrial-leaders .

Economist. 2012. “The company that spooked the world.” *Economist.* http://www.economist.com/node/21559929.

ECSO. 2016. “European Cybersecurity Industry proposal for a contractual Public-Private Partnership.” http://ecs-org.eu/documents/ecs-cppp-industry-proposal.pdf.

ENISA. 2016c. “Challenges of ICT certification in emerging ICT environments.” https://www.enisa.europa.eu/publications/challenges-of-security-certification-in-emerging-ict-environments.

ENISA. 2016a. “Cybersecurity as an Economic Enabler, position paper.” https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/cybersecurity-as-an-economic-enabler.

ENISA. 2016b. “Definition of Cybersecurity - Gaps and overlaps in standardisation.” https://www.enisa.europa.eu/publications/definition-of-cybersecurity.

ENISA. 2016d. “Impact evaluation on the implementation of Article 13a incident reporting scheme within EU.” https://www.enisa.europa.eu/publications/impact-evaluation-article13a.

EPSC. 2017. *EPSC Strategic Notes Issue 24, 'Building an Effective European Cyber Shield', 8 May 2017.* European Political Strategy Centre.

EU-NATO. 2017. "Warsaw Declaration." July.

European Commission. 2012c. "European Security Industrial Policy, COM (2012) 417."

European Commission. 2017a. "Investing in a smart, innovative and sustainable Industry A renewed EU Industrial Policy Strategy."

—. 2014. "President Juncker's political priorities." *European Commission and its priorities.* 15 7. https://ec.europa.eu/commission/priorities/stronger-global-actor_en.

European Commission. 2016b. "Regulation setting up a Union regime for the control of exports, transfer, brokering, technical assistance and transit of dual-use items (recast)."

European Commission. 2016a. "Staff Working Document on the public consultation and other consultation activities of the European Commission for the preparation of the EU Cybersecurity contractual Public-Private Partnership and Accompanying Measure SWD(2016)215." Staff Working Document, Brussels.

European Parliament. 2015. "Cybersecurity in the EU and Beyond." http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536470/IPOL_STU(2015)536470_EN.pdf.

—. 2014. "Resolution on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs." 12 03. http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P7-TA-2014-0230.

European Union. 2016b. "DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union." *Official Journal* L (194): 1-30.

European Union. 2016a. "General Data Protection Regulation." *Official Journal* L (119): 1-88.

—. 2005. "Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems." *Official Journal*, 67-71. http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32005F0222.

—. 2013. "Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA." *Official Journal of the European Union*, 12 08, OJ L ed.: 8-14.

—. 2014. "REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC." *Official Journal, L*, 28 08, OJ L ed.: 73-114.

European Union. 2016c. "Treaty on European Union and the Treaty on the Functioning of the European Union." *Official Journal* C (202): 1-405.

Harris , Robert G, and James M. Carman. 1984. "Public Regulation of Marketing Activity: Part II: Regulatory Responses to Market Failures." *Journal of Macromarketing* 4 (1): 41-52.

Hildebrandt, Mireille, and Laura Tielemans. 2013. "Data Protection by Design and Technology Neutral Law." *Computer Law & Security Review* 29 (5): 509-521.

ITU. 2017. *Global Cybersecurity Index 2017.* Geneva: ITU.

Kello, Lucas. 2017. *The Virtual Weapon and International Order.* Yale University Press.

Pelkmans, Jacques. 2006. "European Industrial Policy." In *International Handbook on Industrial Policy*, by Patrizio Bianchi & Sandrine Labory, 45-78.

SOG-IS/ENISA. 2014. "Minutes of 2014 SOG-IS/ENISA workshop on certification." https://www.enisa.europa.eu/events/sog-is/minutes.

UNCTAD. 2015. "UNCTAD International Classification of Non-Tariff Measures, 2012."

Woods, Daniel, and Andrew Simpson. 2017. "Policy measures and cyber insurance: a framework http://www.tandfonline.com/doi/full/10.1080/23738871.2017.1360927." *Journal of Cyber Policy* 2 (2): 209-226. doi: https://doi.org/10.1080/23738871.2017.1360927.