ZEI INSIGHTS

Cybersecurity at EU and national level – the expansion of economic policy

No. 65 June 2019

By Jan-David Blaese

Undeniably, the share of digital services and products is increasing. New production processes are set up more digitally. Business models based on IT technology are emerging. In addition, the existing economy is also being digitised. In fact, hardly any product or service is not linked to ICT products, services or processes. Along with increasing digitisation, the number of digital security incidents is also increasing. the number of attacks with blackmail software alone, for example, tripled between 2015 and 2017.[1]

The importance of security in information technology has skyrocketed in the course of this development in recent years. This trend is likely to continue: the roll-out of new technologies, such as 5G networks, and subsequent (digital) services, such as autonomous driving or the "Internet of Things", will require even more attention to security in the future.

In addition to the direct safety aspect, there is also the question of sensibly regulated market access for ICT products, services and processes. Here, security concerns overlap with those of economic governance. With the Cybersecurity Act[2], published in June 2019, the European Commission has an instrument that does not only increase security per se, but can also be used to steer economic policy through regulatory requirements. The same applies, for example, to the planned German IT Security Law "2.0". This short article should serve as an introduction to the civilian components of cybersecurity.

Cybersecurity at EU level

At EU level, cybersecurity has long been a focus topic, as the transnational coordination of security standards can create significant and quick additional gains. As early as 2004, the European Union Agency for Network and Information Security (ENISA) was established. Its purpose is to increase the national cyber resilience of the EU's member states, in particular through constant risk analysis and the establishment of exchange networks with representatives from national capitals, including industry. In 2012, the establishment of a Computer Emergency Response Team (CERT) to protect the IT systems of EU institutions followed. The European Cybercrime Centre was established in 2013 to explicitly combat cybercrime. In addition, this year the first cybersecurity strategy of the EU was published, which also included an explicit definition of cybersecurity:

"Cyber-security-related communications and information-infrastructures that can be used to protect the cyber-domain, both in the civilian and military fields, from those threats. Cyber-security strives to preserve the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein."[3]

The EU definition refers to both civilian and military components in cyberspace. The military dimension of cybersecurity is not illuminated in this article, but in itself represents a very complex and extensive topic.

In July 2016, the Directive on measures to ensure a high common level of security of network and information systems in the Union was published. This includes the obligation for all Member States to define a national strategy for the security of network and information systems and, above all, to designate national competent authorities to perform their tasks regarding the security of network and information systems.

In June 2019, EU lawmakers passed the so-called EU Cybersecurity Act. This increases the scope of ENISA's competence and in particular makes the agency responsible for the promotion of a new cybersecurity certification framework.

Certification under the EU Cybersecurity Act

The EU Cybersecurity Act also establishes a European certification framework for cybersecurity. In this framework, ICT products, services and processes should be assessed for compliance with applicable security requirements. The European Commission will present its so-called strategic priorities with regard to the certification framework in a work programme (for the first time until the end of June 2020). This key focus of the certification framework is organised through ENISA, which in turn works with stakeholders such as the European Cyber Security Certification Group. The certification scheme, which still is to be developed, is likely to work with low, medium and high levels of trust. In the actual implementation, the manufacturer or provider of ICT products, services or processes could base the trustworthiness score „low" on a self-assessment. For the ratings "medium" and "high", however, other actors, who have not yet been further identified, would have to submit a certification assessment. This will likely create expenses and thus costs for businesses.

Adherence to the planned European certification framework will initially be voluntary according to the EU Cybersecurity Act. However, the legal act states that the question of whether the requirements are binding will take place for the first time in December 2023 and is then re-examined every two years. This gives the impression that providers of ICT products, services or processes will have little option, but to proactively meet the requirements; otherwise they run – in the worst case – the risk of losing approval for the sale of their products, services or processes in the event of a change in the scheme.

In the planned European certification framework, a normative force of explicitly voluntary standards is manifests itself. These standards also leave room for shifts due to switching policy interests, if necessary. Since the exact requirements for the "medium" and "high" classifications are yet to be published, an accurate assessment cannot yet be made at this time. It is clear, however, that such requirements can also exclude certain producers or service providers; this is the very meaning of an access-regulating certification. Thus, the planned European certification framework is also an instrument for pursuing an EU-wide economic policy – no longer digital economic policy "only", since almost all technically advanced products and services in the value chain feature ICT components.

Cybersecurity in Germany

The developments at EU level correspond with those in the Federal Republic of Germany. Nevertheless, the situation in Germany is even more complex with regard to the actors involved (and the framework or drafting documents written): The key actor for Information Security is the "Federal Office for Information Security" (BSI, under the responsibility of the Federal Ministry of the Interior, for construction and homeland). The BSI is at the same time the national authority designated to the EU to perform its tasks regarding the security of network and information systems. However, the BSI is far from being the only cybersecurity player in Germany. For example, the "Stiftung Neue Verantwortung" drew an impressive overview of the numerous players involved, still leaving the federal states and local authorities largely in the foreground.[4]

An overarching cybersecurity strategy for Germany was first published in 2011. Based on the strategy, a national Cyber Defense Center was set up. Following the update of the Cyber Security Strategy in 2016, the Defense Center was further developed and "Mobile Incident Response Teams" were created within the BSI for the rapid analysis and resolution of cyber incidents.[5]

One of the other actors in German cybersecurity is the National Cyber Security Council, which was set up in 2012 and meets at State Secretary level (deputy ministers) at least three times a year under the chairmanship of the Federal Government Commissioner for Information Technology. In its work, the National Cyber Security Council partly focuses on so-called Critical Infrastructures (CRITIS); the results were included in the IT security law published in 2015, among others.[6] This implies that the Federal Ministry of the Interior – explicitly without the consent of the Parliament, but in agreement with the other ministries – determines which facilities or parts thereof are considered Critical Infrastructures within the meaning of the IT Security Act. Critical infrastructures can belong to the so-called sectors energy, information technology and telecommunications, transport and traffic, health, water, nutrition, finance and insurance, state and administration as well as media and culture. They are of high importance for the functioning of the community, because without them significant public supply or public security threats would appear.[7] In general, operators of CRITIS infrastructures must have a contact point vis-à-vis the BSI and they must report IT disruptions. Furthermore, they have to implement state-of-the-art technology. To enable oversight, they have to undergo audits every two years. This results in concrete expenses or financial burdens for the CRITIS-operators.

The IT security law should soon receive an "update". It can be expected that the revised law will expand the target group to critical infrastructures, the BSI will be given new powers and the possibilities of law enforcement authorities will be bolstered. Also, e.g. CRITIS operators will have to provide trusted endorsements for their entire supply chain.[8]

Conclusions

The development at the European and national level in the field of security in information technology has been – analogously to the technical development – a dynamic undertaking. Existing institutions were expanded, new ones created, and basic documents refined. In particular, the forthcoming introduction of the certification framework by the EU Cybersecurity Act of June 2019, but also the discussions surrounding the German IT security law are part of a development, in which IT-related policies are applied less "in cyberspace" than in the "real economy". Regulation and standard requirements are classic economic policy instruments. Since more and more physical products contain IT components, these requirements have a high impact on products, services and processes.

Regarding the forthcoming years, there is no indication that the importance of these topics is weakening. Rather, with reference to new technologies such as 5G as a basis for autonomous driving or the so-called "Internet of Things", a further increase in the importance of defined security standards and their enforcement authorities will be likely. Thus, the influence of such national and supranational regimes on the real economy will continue to increase sharply. Two challenges appear directly: First, the avoidance of unnecessarily high bureaucratic burdens and costs, and second, the reduction of "arbitrary" political influence.

Jan-David Blaese, *ZEI Master Alumnus "Class of 2011", is a Strategy Expert at the BWI GmbH in Bonn, Germany.*

Endnotes:

[1] *see Reform of cybersecurity in Europe: https://www.consilium.europa.eu/en/policies/cyber-security/, last accessed on 06 June 2019.*

[2] *see Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act): https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=DE, last accessed on 13 June 2019.*

[3] *European Commission / High Representative of the European Union for Foreign Affairs and Security Policy: Cybersecurity-Strategy of the European Union. An Open, Safe and Secure Cyberspace: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/policies/organized-crime-and-human-trafficking/cybercrime/docs/join_2013_1_en.pdf, last accessed on 06 June 2019.*

[4] *see Stiftung Neue Verantwortung: Zuständigkeiten und Aufgaben in der deutschen Cyber-Sicherheitspolitik: https://www.stiftung-nv.de/de/publikation/zustaendigkeiten-und-aufgaben-der-deutschen-cyber-sicherheitspolitik#collapse-newsletter_banner_bottom, last accessed on 13 June 2019.*

[5] *see Bundesministerium des Innern: Cyber-Sicherheitsstrategie für Deutschland 2016: https://www.bmi.bund.de/cybersicherheitsstrategie/BMI_CyberSicherheitsStrategie.pdf, last accessed on 13 June 2019.*

[6] *see Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vom 17. Juli 2015: https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&start=//*%255B@attr_id=%27bgbl115s1324.pdf%27%255D#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl115s1324.pdf%27%5D__1560416122170, last accessed on 13 June 2019.*

[7] *see Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz) mit Stand vom 23.06.2019, Art. 2 (10): https://www.gesetze-im-internet.de/bsig_2009/BSIG.pdf, last accessed on 13 June 2019.*

[8] *see CRonline. Portal zum IT-Recht: IT-Sicherheitsgesetz 2.0 – Referentenentwurf von März 2019: https://www.cr-online.de/blog/2019/04/11/it-sicherheitsgesetz-2-0-referentenentwurf-von-maerz-2019/, last accessed on 13 June 2019.*