Issue 29
December 2017

CREOGN Research Note
French Gendarmerie Officers Academy Research Centre

PUBLIC-PRIVATE COOPERATION AT THE EU LEVEL

The emergence of a European "regulatory state" for cybersecurity

By Pierre Berthelet, CREOGN associate researcher

In its desire to organize the cybersecurity sector, the European Union intends to promote a European digital market and stimulate the competitiveness of its companies. It also aims to defend its own interests, inherent to the economic, societal and security values it intends to preserve. As a "regulatory state", it is part of a global perspective of multi-level and multi-dimensional collaboration with both the Member States and the private sector. The modes of action are diverse, ranging from imposing legal obligations to creating dialogue platforms and awarding grants to finance projects in the field of research and innovation (R&I). The contractual public-private partnership (cPPP) is an example of a proactive policy led by the EU, where the focus is on R&I to organize and densify the European cybersecurity sector.

Public-private cooperation in cybersecurity is crucial. The Bockel parliamentary report of 2012 judged the level of cooperation with the private sector to be insufficient, even though companies are an essential link in the cybersecurity chain. One of the measures recommended was to increase the use of public funding for research and development in the field of information systems security.
This is precisely the path that the European Union is going to take, whose involvement in cybersecurity was to be strengthened, according to the recommendations of the same report. There has been a major change in perception in this respect in recent years. Initially, cybersecurity was first associated with the security of information and communication networks, seen as a means to foster the growth of the digital economy. However, cybersecurity goes beyond digital security itself. It is not only a question of ensuring Europe's prosperity, by guaranteeing the proper functioning of the economic market, but also ensuring the defense of European values, in particular the preservation of democracy and fundamental rights. In other words, cybersecurity has a political and societal dimension. The 2013 cybersecurity strategy recalls two key elements in this regard: first, security is a shared responsibility; second, the private sector owns and operates significant parts of cyberspace[1]. As such, its inclusion is fundamental in the definition of a Union-wide cybersecurity policy, the manifestation of a European "regulatory state" in this field.

1. Including the private sector in an embryonic European cybersecurity

The protection of information systems dates back to the late 1990s. At the time, the measures taken were intended to promote the emergence of an information society in Europe. The action plan known as *eEurope* called for the establishment of a European framework for the protection of information systems. A communication from the European Commission in 2001 led to the establishment of an important legislative base in the fight against computer crime, a phenomenon whose victims are not only individuals, but also businesses[2]. A proposal presented in April 2002 led to the adoption in 2005 of a framework decision called "cyber attacks" aimed at approximating national criminal rules against attacks on information systems[3].

1 JOIN(2013)1.
2 COM(2000) 890, p. 2.
3 Recital 5 of Framework Decision 2005/222/JAI.

The threat posed by cybercrime requires greater intervention, not only from the Union, but also from the private sector. At the operational level, efforts are focused on the fight against illegal content on the Internet, in particular against child pornography. They are translated into financial support for projects in this field.
This operational cooperation, within the framework of concrete projects, is coupled with a more institutional cooperation. Various companies, including software manufacturers, are in a position to combat cybercrime, in particular attacks on information systems that are so serious as to jeopardize the achievement of a digital society. A Permanent Stakeholders Group (PSG) was set up for this purpose within the European Network and Information Security Agency (ENISA) to maintain regular dialogue between them and the private sector[4]. The same applies to Europol. Europol's Anti-Cybercrime Unit (EC3) is an Internet investigation center at the service of Member States. Validated in 2012 by the EU Council, EC3 collaborates with the private sector. To this end, Europol has signed memorandums of understanding with several major information and communications companies to carry out its missions.
The European cybersecurity strategy, which was approved the same year the EC3 was inaugurated, in 2013, places the private sector as the essential link in a security that can only be collective. Wishing to promote cyber-resilience in the Union, it considers that only an effective collaboration between public authorities and businesses can achieve this objective.
In this sense, the Union is setting itself up as a regulatory body[5]. The "regulatory State" is in the wake of the "propulsive State "[6] described by Charles-Albert Morand, responsible for correcting market fluctuations and ensuring that major balances are maintained[7] . Preferring flexible law, it does not, however, shy away from the use of more traditional, i.e., more restrictive law. This ambivalence of the State as a producer of "neo-modern" law, mixing flexible regulation and more authoritarian regulation, is found from the point of view of the Union, in its modes of intervention. The *regulatory State* is placed in the perspective of transnational governance. The Union, as a *regulatory State*, is in fact part of the global perspective of a multi-level and multidimensional collaboration, both with the Member States and with the private sector[8]. The modes of public action are diverse, ranging from granting subsidies for projects in the field of research and innovation to increasing institutionalized dialogue, as well as imposing obligations in a more traditional regulatory framework.
It is a matter of the Union working closely with the private sector, recognizing it as an essential partner in order to achieve the political goals it has set itself (fighting against cyber threats as part of the preservation of the growth of the European digital market), but also subjecting it to a series of legal obligations in this area. The most important of these is the Network and Information Security Directive (NIS Directive)[9] which compels operators of essential services and digital service providers to notify national authorities, in the event of cyber incidents.

2. Progressive organization of the European cybersecurity sector

A communication published on July 5, 2016, the day before the SRI Directive was adopted, aims to create industrial capabilities in the field of cybersecurity at the EU level[10]. This text has two dimensions that are two sides of the same coin: the obverse side highlights the private sector as a target of cyber threats. As the manager of certain critical infrastructures, it is vulnerable to cyber incidents, some of which large-scale. The reverse side highlights the private sector as a provider of cyber security. This communication therefore intends to promote competitiveness and innovation. The idea is not so much to promote free competition as to ensure, on the contrary, regulation of the European cybersecurity sector, echoing this idea of the "regulatory state". Indeed, the Union suffers from a lack of interoperable solutions in case of cyber incidents. It is therefore a question of making up for the failures of the single market by taking a series of measures to structure this sector as well as possible.
Noting the failure of the Lisbon strategy, the new strategy of March 2010, called "Europe 2020", intends to ensure the development of a strong industrial base. Among the seven initiatives retained by this strategy are the improvement of the competitiveness of the European Union's industry on a global scale and increased efforts in research and innovation. The Horizon 2020 program is part of this approach, as it

4 Currently defined by Regulation (EU) 526/2013, this group includes representatives from the cybersecurity industry as well as academia.
5 On this thesis of the regulatory state in Europe, see Majone, G., *La Communauté européenne : un État régulateur*, Paris, Montchrestien, 1996.
6 Morand, C.-A., *Le droit néo-moderne des politiques publiques*, Paris, LGDJ, 1999.
7 Chevallier, J., « L'État régulateur », *Revue française d'administration publique*, vol. 111, n° 3, 2004, p. 473-482.
8 Chowdhury, N., Ramses A. Wessel, R. A., « Conceptualising Multilevel Regulation in the EU: A Legal Translation of Multilevel Governance? », *European Law Journal*, vol. 18, n° 3, mai 2012, p. 337-338.
9 Directive (EU) 2016/1148.
10 COM(2016) 410.

aims to ensure the financing of research and innovation in the Union for the period 2014-2020. With a budget of 79 billion euros for the period 2014-2020, it is structured around three priorities, including "industrial primacy" and "societal challenges".
To understand the emergence of a European cyber industry, it is important to go back to the 2004 attacks on the Atocha train station in Madrid. An action plan was approved in 2006 and a directive adopted in 2008 to strengthen the protection of critical infrastructures. The action plan recalls that the protection of this type of infrastructure is the responsibility of the Member States, but a concerted approach is necessary for infrastructures of European scope. The 2008 Directive establishes a Europe-wide procedure for the identification and designation of European Critical Infrastructures (ECI). Infrastructure related to the Information and Communication Technologies (ICT) sector is addressed in a 2009 Communication that sets out an action plan for the protection of "Critical Information Infrastructures" (CII)[11] . Demonstrating the desire to move forward quickly, a communication was published in 2011 to take stock of the 2009 action plan[12] . At this stage, however, there is no European action truly dedicated to cybersecurity, in the sense that CCI protection is included in an overall framework, with cybersecurity as its theme. The 2013 strategy dedicated to it aims to fill this gap. It establishes five priorities, including achieving cyber resilience and developing industrial and technological resources for cybersecurity.

As for the 2017 cybersecurity strategy, it deepens the efforts initiated since 2013. It notes that despite the positive results achieved in cybersecurity, the Union remains vulnerable to cyber incidents. It intends to strengthen cyber-resilience and promote competitiveness and innovation in the European cybersecurity sector. It is no coincidence that this strategy is being presented on the same day as the revisited strategy for the Union's industrial policy[13] . Such a strategy demonstrates the Union's will to enter a new industrial era marked by major technological breakthroughs, notably robotics, the Internet of Things, and artificial intelligence. Proposing to "make European industry stronger", it aims to invest in the industry of the future. Innovation is the engine of growth, which is why this strategy intends to promote research. Aiming to "modernize industry to bring it into the digital age", according to the terms used in the revised strategy, it is intended to promote the development of the Union's industrial capacities. The Contractual Public-Private Partnership (cPPP) is part of this approach.
The cPPP aims to transcend the divisions and fragmentation inherent in the proliferation of actors, by seeking to coordinate actors from the public and private sectors, and located at different levels, European, national and local. It is characterized by an approach based on co-management, by the use of flexible law and by the networking of public and private actors (European Commission and agencies, ministries, local authorities, public research organizations, SMEs, universities and clusters).
The idea of cPPPs, which was born in Strasbourg on July 5, 2016, is not new in itself. Several Member States have already opted for this type of public action instrument. For its part, the European Union has initiated a PPP in the field of resilience. This is the EP3R, established by the 2009 Communication and dedicated to the resilience of critical infrastructure. Mentioned by the Strategy for a Digital Single Market in Europe of May 6, 2015, the cPPP follows a similar logic to the IP3R: reconciling the expectations of the European institutions, which establish general policy priorities, and technical solutions from the private sector to best fit the priorities. The total budget of the cPPP amounts to 450 million euros. The goal is to reach 1.8 billion by 2020, thanks to the investment of the companies involved.
Specified by the aforementioned communication of July 5, 2016, the creation of the cPPP is part of three complementary perspectives, the completion of the European digital market, by promoting competition between companies, the creation of a European industrial base in the field of cybersecurity and, finally, the defense of the Union's own interests. As a result, the cPPP intends, thanks to the multiplier effect of the amounts invested in R&I, to enable the development of a European cybersecurity sector that masters certain technologies to enable the Union to protect interests that it considers essential.

The 2017 cybersecurity strategy recalls that the level of investment in the United States amounted to $19 billion (€16 billion) for the year 2017, 35% more than in 2016. The cPPP is therefore a first step. It reflects an awareness not only on the part of the Union of the need to get involved in a proactive policy, but also on the part of the Member States, of the imperative to go beyond national approaches based on purely national or bilateral public-private partnerships. The cPPP is part of an era in which these partnerships are

11 COM(2009) 149, p. 6.
12 COM(2011) 163.
13 COM(2017) 479.

being conducted on a large scale, at a time when national and European interests, whether economic or societal, are more intertwined than ever.

Pierre Berthelet holds a doctorate in law, specializing in EU law, and is a security researcher at Laval University (Quebec). A former ministerial advisor, he is a member of the French Association of Security and Defense Law (AFDSD), a member of the Board of Directors of the French National Institute for Advanced Studies in Security and Justice (INHESJ), a member of the editorial board of the Cahiers de la Sécurité et de la Justice, and a research associate at CREOGN. He is the author of several books (including "Chaos international et sécurité globale. La sécurité en débats") and founder of the securiteinterieure.fr website.

Translated by SLT Guilhem SERENE and the French Gendarmerie Officers Academy Language Department