An agency at the heart of European cybersecurity

Jean-Baptiste Demaison,
ENISA

Abstract:
Whereas most EU member states have not yet set up a cybersecurity agency, the European Union founded the European Network and Information Security Agency in 2004. In charge of developing the capacity of member states in cybersecurity, ENISA's scope of action has been broadened under a more ambitious EU framework regulation that led to the adoption in 2013 of a European cybersecurity strategy. Fifteen years after ENISA's creation, the Cybersecurity Act has confirmed this agency's indispensable role and bolstered its assignments by setting up a system, unique in the world, for certifying cybersecurity in Europe. A new era is opening for an agency with new duties. Nonetheless, questions are still standing. What model to follow to upgrade EU actions in cybersecurity? What is the next legislative step for more digital security in Europe? How should ENISA respond to the many initiatives being undertaken in several sectors?

A precocious European awareness of cybersecurity

An EU agency ahead of its time

The Heraklion office

While most member states did not yet have an agency devoted to cybersecurity, the Council of the European Union (EU) and the European Parliament decided in 2004 to create the ENISA, the European Network and Information Security Agency.[1] This agency was prolonged twice, in 2008 and then 2011, before being made permanent and renamed in 2019, as explained hereafter.[2]

Initially based in Heraklion at the request of Greek authorities but then gradually moved to Athens, ENISA steadily carved out a stronger place for itself among European institutions and member states as the issue of cybersecurity came to compel recognition from public decision-makers. Its priority was to advise member states about capacity-building in cybersecurity. ENISA developed a set of methods and support services that would help several national governments form computer security incident response teams (CSIRT) and draft cybersecurity strategies.

ENISA soon chose to actively foster cooperation among member states, in particular through Cyber Europe, a series of crisis management exercises. Organized every two years since 2010, these drills have simulated emergencies on a European scale involving cyberattacks on critical sectors (energy, telecommunications, etc.). They test member states' ability to work together. These exercises prefigured the development of standard operating procedures (SOPs).

[1] Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency (Text with EEA relevance) available at https://eur-lex.europa.eu/search.html?qid=1584188180827&text=460/2004%20of%2010%20March%202004&scope=EURLEX&type=quick&lang=en.

[2] This article has been translated from French by Noal Mellott (Omaha Beach, France). The translation into English has, with the editor's approval, completed a few bibliographical references. All websites were consulted in March 2020.

This European agency has been asked to follow up on the drafting and implementation of public cybersecurity policies in Europe. In particular, ENISA actively worked with member states to enforce Article 13a of the "Telecoms Package", the first EU legislation that imposed cybersecurity obligations on telecommunication operators.

Economic vs. national security

As imagined by the European Commission at the turn of the century, ENISA had the task of working out a response to the need for a secure European Internet. ENISA's legal grounds were the single European market, a topic for which the EU and member states shared competence. The purpose was to guarantee the security of the Single Market as it underwent the digital transition. The introduction of this agency did not fail to arouse wariness among governments who were used to handling by themselves — as sovereign states and as a matter of national defense — the security of their information systems.

Several times since, questions have arisen about the EU's competence and about ENISA's role in relation to the most sensitive aspects of cybersecurity. The role of providing operational support was limited to the countries that fell victim to cyberattacks of a deliberate sort. For member states, such as France, each state was responsible for developing an autonomous capacity for responding to attacks. Had emphasis at the time been placed on centralization at the European level (instead of decentralized capacities and cooperation), Europe would probably nowadays be incapable of protecting the EU from cyberattacks.

An evolving regulatory framework

Protecting critical infrastructures

As cybersecurity became an issue of growing concern to European policymakers, the usefulness of coordinating actions between member states and the EU in response to threats against Europe's digital sovereignty — against our security and confidence in digital technology — has gradually come to be taken for granted.

After two communications from the European Commission on critical information infrastructure protection (CIIP), a major step was made in 2013 when a proposal was placed on the table for a directive on the security of network and information systems. Adopted in 2016, this so-called NIS directive made rules of security binding on telecommunication operators and expanded them to cover services "*to be considered as essential for the maintenance of critical societal and economic activities*" in seven sectors (including energy, banking and transportation).[3] Among these requirements were the legal obligations to implement security regulations (as clarified in a nonbinding document adopted by all EU member states in 2018)[4] and to report cyberincidents that had a significant impact on essential services to the competent regulatory authority or CSIRT at the national level.

The NIS directive also set up formal institutional structures for, respectively, political and technical cooperation among member states. First of all, the group on political cooperation brings together the representatives of national cybersecurity agencies, the European Commission and ENISA. Its purpose someone to support strategic cooperation among member states, facilitate exchanges of information, build confidence and raise the global level of maturity of national

[3] The NIS Directive on the security of network and information systems: 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 available at http://data.europa.eu/eli/dir/2016/1148/oj..

[4] NIS Cooperation Group (2018) "Reference document on security measures for operators of essential services", CG Publication 01/2018, 25p., available via http://ec.europa.eu/information_society/newsroom/image/document/2018-30/reference_document_security_measures_0040C183-FF20-ECC4-A3D11FA2A80DAAC6_53643.pdf.

capacities in cybersecurity. Secondly, a network of CSIRTs was formed for the purpose of technical and operational cooperation. ENISA actively supports the operations of CERT-EU, which brings together representatives from all EU member states. Launched in 2017, this network soon proved its usefulness by facilitating exchanges among national computer emergency response teams in several member states, including France and Estonia, in response to the WannaCry and NotPetya attacks. Shortly thereafter, the Council of the EU set up, for the first time, an informal group on cybersecurity. It became, in 2017, a formal work group in charge of the strategic and diplomatic aspects of cybersecurity.

A strategy for Europe

The drafting of the NIS directive (2013-2016) was the occasion for the release of the first European cybersecurity strategy, which presented strategic orientations in all fields of EU competence.[5] Beyond the cybersecurity of the Single Market and of digital technology, as covered by ENISA and the NIS directive, this strategy has underscored the importance for the EU to stake out a position on cyberthreats in relation to diplomacy and defense. This aspect of cyberpolicy emerged out of the work done for several years at the UN (with the implication of several European countries, including France) on international rules of law and the norms of state responsibility in cyberspace. In 2017, this orientation had a concrete result: the adoption by member states of a "cyberdiplomacy toolbox", which established an EU doctrine of prevention, cooperation and controlled escalation, eventually entailing coercive measures in response to malicious cyberattacks against member states.[6]

The European cybersecurity strategy also centered public debate on the issue of the EU's autonomy in matters of digital products and services. By referring, for the first time at the European level, to the risks of the continent being dependent on solutions developed elsewhere, this strategy led to the signing of a public-private partnership between the European Commission and the European CyberSecurity Organization (ECSO) with the objective of bringing together the representatives of public and private organizations and academics in order to stimulate the development of a European cyberindustry.

The formation in 2012, shortly before the publication of the European strategy, of a computer emergency response team (CERT) devoted to EU institutions, agencies and structures signaled a major decision whereby the EU sought to strengthen its cybersecurity. Confirmed in its assignments, CERT-EU is now a guardian of the security of the EU's sensitive data and of the data entrusted to the EU by member states.

[5] Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: "Cybersecurity strategy of the European Union: An open, safe and secure cyberspace", 20p., available via https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=1667.

[6] For an update, see https://eucyberdirect.eu/content_knowledge_hu/draft-council-conclusions-on-the-cyber-diplomacy-toolbox/.

A new agency, a new era

The Cybersecurity Act

The adoption in 2019 of the EU Cybersecurity Act signals a turning point in cybersecurity on the continent.[7] For one thing, ENISA, now a standing organization, is recognized to have an indispensable role in European cybersecurity. This act also endorses the installation of this agency's offices in Athens, with the approval of Greek authorities. It has turned a page in ENISA's history, which will no longer be written from Crete.

A stronger mandate

Apart from carving out a permanent place for ENISA among EU institutions, the Cybersecurity Act has expanded the agency's assignments and made new ones. ENISA, its name changed to the European Union Agency for Cybersecurity, has entered a new era.[8] Its support role for operational cooperation among member states in response to cyberincidents has been bolstered. In particular; the act enables the agency to facilitate, at the demand of member states, the technical management of incidents or emergencies related to information system security. Having been involved, for several years now, in actions for making the general public aware of digital risks via the European Cybersecurity Month, the agency now has this role listed among its main assignments along with its support for improving member states' cybersecurity capability and developing European expertise in this field.

A certification framework

Besides ENISA's aforementioned assignments, le Cybersecurity Act also provides for a European framework of certification in cybersecurity. This has come out of an agreement of cooperation (SOG-IS) between a dozen or so member states that provides for a mutual recognition of security certificates. Behind the technical term "expert", a revolution is under way in matters related to the security of, and confidence in, digital technology. This framework lays down the principles and procedures shared by all member states for evaluating and certifying the requisite security level (elementary, substantial, high) of the digital solutions or services covered by a certification scheme. The range of possibilities is vast: the cloud, embedded systems, control systems, etc. It delineates a European cyberspace where citizens, firms, industries and administrations will eventually have reliable assessments of the security level offered by the digital solutions they want to adopt, assessments that will be recognized everywhere in Europe. Designed as a voluntary procedure, this certification can, when lawmakers in Europe decide to do so, be made binding for certain solutions or services (perhaps under future directives or regulations specific to sectors or technologies).

This framework's potential reaches beyond the improvement of the cybersecurity of Europeans. Given the growing awareness about information system security and data protection (thanks to the EU's General Data Protection Regulation), the introduction of European certification sends a new, international signal about the sanctuary that the EU increasingly provides for data.

[7] 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) available via https://eur-lex.europa.eu/eli/reg/2019/881/oj.

[8] An anecdote: the new name came out of a compromise that, proposed by France, sought to rally those who wanted to abandon the now obsolete phrase "network and information security" and those who did not want ENISA to be a cybersecurity agency "like the others", with a field of competence similar to that of national agencies, even though ENISA still did not have the assignment of seeing to the cybersecurity of the states benefitting directly from its actions.

A platform for changing the scale of European cybersecurity

The Cybersecurity Act is a major step in European cybersecurity and a change of scale for ENISA. However it is but one step on the way toward governance and procedures capable of responding to all issues related to European cybersecurity.

The task of governance

Given the accelerated digital transition that our societies and economic agents are undergoing, the capability of Europe and its member states to protect themselves from cyberthreats and respond to them calls for a cooperation that, effective and respectful of national jurisdictions, prepares the grounds for confidence-building. In the midst of this trend, ENISA will have to shift from a model of facilitation to becoming an open platform for aggregating and diffusing the best know-how and state-of-the-art expertise. It will also, when necessary, have to work for a convergence of stakeholders (*e.g.*, for drafting certification schemes).

By becoming the "European cybersecurity platform" ENISA will have to prove that it is capable of acting with agility, and that it is the sure reference for all EU institutions, agencies and units as they become ever more conscious of cybersecurity issues. As more and more programs in specific sectors (such as aviation or energy) reckon with digital risks, ENISA will have to see to it that adapted cybersecurity requirements are taken into account. It will have to be a key advisor to European institutions.

New regulatory issues

Since the appointment of a new European Commission, proposals should be forthcoming. The question of the next legal text on cybersecurity is open. The prospect has been raised of a second version of the NIS directive; but an alternative or, at least, parallel approach could be adopted. The next regulatory requirements in cybersecurity could be focused on the suppliers of digital products and services rather than on users. The availability of security updates, certification, security by default, the product life cycle, the sequestering of source code when businesses close… these are some of the prospects to explore that would strengthen the security of the solutions being rolled out. Players along the digital supply chain, such as the integrators in charge of updates, should be involved.

Such an approach would confirm the strategic orientation of the European framework of certification, which has been designed so that users will eventually be offered solutions with "security by design and by default". This would increase their confidence in using digital technology. Furthermore, this choice is consistent with the principles of the French president's "Paris Call for Trust and Security in Cyberspace" made in Paris in 2018.[9]

[9] Availble via https://www.diplomatie.gouv.fr/IMG/pdf/paris_call_cyber_cle443433-1.pdf.