Une agence au cœur de la cybersécurité européenne

Par **Jean-Baptiste DEMAISON**
ENISA

Une prise en compte précoce des enjeux de cybersécurité au niveau européen

Une agence européenne, avant l'heure

Base Héraklion

Alors que la plupart des États membres de l'Union européenne (UE) ne disposaient pas encore d'agence dédiée aux enjeux de cybersécurité, le Conseil de l'UE et le Parlement européen ont décidé en 2004 (1), la création de l' « agence européenne pour la sécurité des réseaux et de l'information », l'ENISA. Son mandat a été prolongé à deux reprises en 2008 puis en 2011 avant d'établir l'agence à titre permanent en 2019 (voir *infra* « Le *Cybersecurity Act* : révolution certification »).

Basée en Grèce et initialement établie à Héraklion selon le souhait des autorités grecques – avant son déplacement progressif à Athènes – l'ENISA a vu son positionnement progressivement renforcé au sein de l'écosystème institutionnel européen ainsi qu'auprès des États membres, à mesure que l'enjeu de la cybersécurité s'est imposé au cœur des préoccupations des décideurs publics. Chargée en priorité de conseiller les États sur le développement des capacités de cybersécurité (*capacity building*), l'ENISA s'est notamment illustrée dans le développement de corpus méthodologiques et d'offres d'accompagnement ayant permis la mise en place de plusieurs CSIRTs (2) gouvernementaux (équipes de réponse à incidents) et de stratégies nationales de cybersécurité.

Très tôt, l'ENISA a également choisi de jouer un rôle actif en faveur du développement de la coopération entre États, en particulier au travers du cycle d'exercices « Cyber Europe ». Organisé tous les deux ans depuis 2010, celui-ci a permis de simuler des crises d'origine cyber de dimension européenne affectant des secteurs critiques (énergies, télécommunications, etc.) et de tester la capacité des États à y faire face ensemble. Ces exercices ont, en outre, permis de préfigurer le développement de mécanismes de coopération technique et opérationnelle, tels que des procédures standards opérationnelles (3).

L'agence européenne a été sollicitée pour accompagner l'élaboration et la mise en œuvre des politiques publiques européennes en matière de cybersécurité. L'ENISA a notamment joué un rôle actif auprès des États dans le cadre de la mise en œuvre de l'article 13a du « paquet télécom », première législation européenne à avoir inclus des obligations en matière de cybersécurité pesant aujourd'hui sur les opérateurs de télécommunications.

Sécurité économique vs. sécurité nationale

Imaginée par la Commission européenne au début des années 2000, l'ENISA devait, à l'origine, répondre à la nécessaire sécurisation de l'Internet européen, afin de garantir la sécurité du marché

(1) Règlement (CE) n°460/2004 du Parlement européen et du Conseil du 10 mars 2004 instituant l'Agence européenne chargée de la sécurité des réseaux et de l'information (texte présentant de l'intérêt pour l'EEE).
(2) *Computer Security Incident Response Team*.
(3) *Standard Operating Procedures ou SOPs*.

unique à l'heure de sa transformation numérique. Celle-ci a ainsi été établie sur la base juridique du marché intérieur, domaine de compétences partagées entre l'UE et les États membres. L'arrivée de l'agence n'a, de ce fait, pas été sans susciter une certaine prudence de la part d'États habitués à traiter seuls des enjeux de sécurité informatique *via* le prisme régalien de la sécurité et de la défense nationale.

À plusieurs reprises par la suite, la question de la compétence de l'UE et du rôle de l'ENISA sur les aspects les plus sensibles de la cybersécurité s'est posée. L'ENISA a notamment vu son rôle encadré en matière de soutien opérationnel aux États victimes de cyberattaques, dont le caractère volontaire a été très tôt consacré, à l'initiative d'États – dont la France – ayant considéré qu'il incombait à chacun de se doter d'une capacité de réponse autonome. *A contrario*, un modèle centralisé au niveau européen aurait-il été privilégié à l'époque, plutôt qu'un modèle de capacités décentralisées et de coopération, il y a fort à parier que ces capacités européennes seraient insuffisantes pour protéger l'UE face à la menace cyber actuelle.

Un cadre de régulation en développement

La protection des infrastructures critiques

À mesure que l'enjeu de la cybersécurité a pris de l'ampleur au niveau politique européen, l'utilité d'une action coordonnée des États et de l'UE pour relever le défi commun de la souveraineté numérique de l'Europe face aux menaces pour la sécurité et la confiance numériques, s'est progressivement imposée comme une évidence.

Après deux communications de la Commission européenne dédiées à la protection des infrastructures d'information critiques (*Critical Information Infrastructure Protection* ou CIIP), une étape importante a été franchie en 2013 avec la proposition de directive sur la sécurité des réseaux et des systèmes d'information (« directive NIS »). Adoptée en 2016 [4], la directive NIS a étoffé et étendu les règles de sécurité contraignantes applicables aux opérateurs de télécommunications, à des « opérateurs essentiels au maintien d'activités sociétales et/ou économiques critiques » dans des sept secteurs incluant l'énergie, la banque ou encore les transports : obligation de mise en œuvre de règles de sécurité, clarifiées dans un document de référence non contraignant adopté par l'ensemble des États membres de l'UE en 2018 [5] ; obligation de notifier les incidents informatiques ayant un impact significatif sur leurs services essentiels, à leur autorité nationale compétente ou à leur CSIRT national/gouvernemental.

La directive NIS a également établi un cadre de coopération formel entre États en matière de cybersécurité, au travers de deux enceintes respectivement de niveaux politique et technique. Premièrement, le « groupe de coopération », réunissant des représentants des agences nationales de cybersécurité, la Commission européenne et l'ENISA, chargé de soutenir et de faciliter la coopération stratégique entre les États membres ; faciliter l'échange d'informations, renforcer la confiance mutuelle et élever le niveau global de maturité et les capacités nationales de cybersécurité. Deuxièmement, le « réseau des CSIRTs », premier réseau de coopération technique et opérationnelle réunissant l'ensemble des États membres de l'UE et du CERT-EU, activement soutenu dans son fonctionnement par l'ENISA. Lancé en 2017, ce réseau a rapidement confirmé son utilité en ayant facilité les échanges entre CERTS nationaux de plusieurs États membres, dont la France et l'Estonie, en réponse aux crises *Wanna Cry* et *NotPetya*.

(4) Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union.
(5) http://ec.europa.eu/information_society/newsroom/image/document/2018-30/reference_document_security_measures_0040C183-FF20-ECC4-A3D11FA2A80DAAC6_53643.pdf

Peu de temps après, le Conseil de l'UE s'est également doté d'un premier groupe informel consacré à la cybersécurité (le groupe des amis de la présidence cyber) devenu en 2017, groupe de travail formel, chargé de traiter des enjeux stratégiques et diplomatiques de la cybersécurité (le groupe de travail horizontal sur les questions cyber).

Une stratégie pour l'Europe

Proposée en 2013, la directive NIS l'a été à l'occasion de la publication de première la stratégie européenne de cybersécurité [6], offrant pour la première fois des orientations stratégiques en matière de cybersécurité sur l'ensemble du spectre des domaines de compétences de l'UE.

Au-delà de la cybersécurité du marché unique du numérique, pris en compte par l'ENISA et dans la directive NIS, la stratégie a souligné l'importance d'un positionnement de l'UE sur les enjeux cyber diplomatiques et de défense. Ce volet émergent du portefeuille cyber européen a vu le jour dans la continuité des travaux conduits depuis plusieurs années à l'ONU, avec l'implication de plusieurs États européens dont la France, sur les règles de droit international et les normes de comportement responsables des États dans le cyberspace. En 2017 [7], cette orientation s'est concrétisée par l'adoption, par les États membres, d'une boîte à outils cyber diplomatique établissant une doctrine de prévention, de coopération et d'escalade contrôlée de l'UE, pouvant aller jusqu'à des mesures coercitives, face aux cyberattaques malveillantes dont pourraient être victimes ses États membres.

La stratégie européenne de cybersécurité a également mis au centre du débat public l'enjeu de l'autonomie stratégique de l'UE en matière de produits et de solutions numériques et de sécurité. Actant pour la première fois à ce niveau les risques de « dépendance » de l'Europe à l'égard de solutions développées en dehors de son territoire, cet axe de travail a notamment conduit à la signature d'un partenariat public-privé entre la Commission européenne et l'organisation européenne de cybersécurité (ECSO), avec pour objectif de rassembler des représentants publics, privés et académiques en vue de stimuler le développement de l'écosystème industriel cyber européen.

La création en 2012, peu de temps avant la publication de la stratégie européenne, d'un CERT dédié aux institutions, agences et entités de l'UE avait également été signalé comme une décision majeure de l'UE en faveur du renforcement de sa propre cybersécurité. Confirmé dans son rôle et ses missions, le CERT-EU constitue aujourd'hui l'un des garde-fous pour la sécurité des données sensibles de l'UE et celles confiées à l'UE par les États membres.

Une nouvelle agence, à l'aube d'une nouvelle ère

Le *Cybersecurity Act* : révolution certification

Un mandat renforcé

L'adoption en 2019 du règlement européen « *Cybersecurity Act* » constitue un virage pour la cybersécurité européenne. Il dote, tout d'abord, l'ENISA d'un nouveau mandat, désormais permanent, confirmant le caractère incontournable de l'agence dans la prise en compte des enjeux de cybersécurité au niveau européen. Actant, par ailleurs, son implantation à Athènes avec le soutien des autorités grecques, le règlement tourne également une page de l'histoire de l'ENISA qui ne s'écrira désormais plus depuis la Crète.

(6) Communication conjointe au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, « Stratégie de cybersécurité de l'Union européenne : un cyberespace ouvert, sûr et sécurisé ».
(7) "Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities" ("Cyber Diplomacy Toolbox"), Brussels, 7 June 2017, 9916/17.

Au-delà de l'établissement durable de l'ENISA dans le paysage institutionnel européen, le *Cybersecurity Act* étoffe les missions principales de l'agence et lui en attribue de nouvelles. En changeant de nom et en devenant l'« agence européenne pour la cybersécurité », l'ENISA entre dans une nouvelle ère [8]. Le rôle de l'ENISA en matière de soutien à la coopération opérationnelle des États en réponse aux incidents informatiques est ainsi renforcé, en permettant notamment à l'agence de faciliter désormais, à la demande d'États, la gestion technique d'incidents ou de crises dont ils seraient victimes. Active depuis plusieurs années en faveur de la sensibilisation du grand public au risque numérique, au travers du « mois européen de la cybersécurité » [9], son action en la matière est érigée au rang de mission principale, au même titre que le soutien au développement capacitaire des États et le développement d'une expertise européenne en matière de cybersécurité.

Un cadre pour la certification en Europe

Nouvelle mission majeure pour l'ENISA et véritable rupture pour l'Europe, le *Cybersecurity Act* établit également un « cadre européen de certification de sécurité numérique », inspiré d'un accord de coopération (SOG-IS) ayant réuni jusqu'à plus d'une dizaine d'États membres, qui avaient accepté la reconnaissance mutuelle des certificats de sécurité émis dans leur pays respectifs.

Derrière l'appellation technique experte se cache une révolution en germe pour la sécurité et la confiance numérique en Europe. Ce cadre établit des principes et mécanismes communs à l'ensemble des États membres de l'UE, permettant d'évaluer et de certifier le niveau de sécurité de potentiellement tout type de solution ou de service numérique bénéficiant d'un schéma de certification, à différents niveaux d'exigences de sécurité (élémentaire, substantiel, élevé). *Cloud*, systèmes embarqués, systèmes de contrôle industriels… le champ des possibles est gigantesque et permet d'entrevoir un espace numérique européen où les citoyen(ne)s, entreprises, industriels et administrations seront un jour en mesure de s'appuyer sur une évaluation fiable, et reconnue partout en Europe, du niveau de sécurité des solutions numériques qu'ils souhaitent déployer.

Volontaire par conception, ce cadre de certification n'en est pas moins disponible, dans le cas où les législateurs européens décideraient de rendre contraignante la certification de certaines solutions ou services, dans le cadre de futures directives ou de futurs règlements sectoriels ou spécifiques à un domaine technologique. Le potentiel de ce cadre dépasse, en outre, le renforcement du niveau de sécurité numérique des européen(ne)s. Dans un contexte de prise en compte croissante de l'enjeu de la sécurité des sytèmes d'information et de la protection des données, avec le règlement général sur la protection des données à caractère personnel, l'introduction de la certification de sécurité européenne est un nouveau signal envoyé à l'international, sur le refuge que constitue de manière croissante l'UE pour les données.

Une plateforme européenne pour faire passer à l'échelle le modèle de cybersécurité européen

Un défi de gouvernance

Le *Cybersecurity Act* constitue une étape importante pour la cybersécurité européenne et un changement d'échelle pour l'ENISA. Il ne constitue toutefois qu'une étape dans le cheminement

(8) À titre d'anecdote, le nom « agence européenne pour la cybersécurité » est le résultat d'un compromis, proposé par la France, visant à réconcilier les tenants du renoncement au concept de « sécurité des réseaux et de l'information », devenu obsolète et ceux qui « ne souhaitaient pas que l'ENISA fût une "agence *de* cybersécurité" comme les autres », apparentant son champ de compétence à celui d'une agence nationale, alors que l'ENISA n'avait toujours pas vocation à assurer pour des bénéficiaires directs leur cybersécurité.
(9) *European Cybersecurity Month*.

vers une gouvernance et des mécanismes européens aptes à répondre à l'ensemble des défis posés à la cybersécurité européenne.

Dans le contexte de la transformation numérique accélérée de l'ensemble des acteurs économiques et de la société, la capacité de l'Europe et des États membres à se protéger des menaces et à y répondre, passera par un modèle de coopération efficace et respectueux des compétences nationales, qui conditionne le développement de la confiance. Au cœur de cette dynamique, l'ENISA devra basculer d'un modèle de facilitation à un modèle de « plateforme » ouverte apte à agréger et à diffuser le meilleur des connaissances, de l'expertise à l'état de l'art. Elle devra également parvenir à faire converger, lorsque cela est nécessaire, les acteurs pertinents de l'écosystème, comme dans le cadre de l'élaboration des schémas de certification.

L'ENISA devenue « plateforme européenne pour la cybersécurité » devra également signifier qu'elle est une agence apte à agir avec agilité et en tant que point de référence incontournable pour l'ensemble des institutions, agences et entités de l'UE, de plus en plus conscientes des enjeux de cybersécurité. Alors que les initiatives sectorielles prenant en compte le risque numérique, telles que dans le domaine de l'aviation ou l'énergie, vont se multiplier à l'avenir, l'ENISA devra être garante d'une prise en compte d'exigences de cybersécurité adaptées et demeurer une conseillère privilégiée auprès des instances européennes.

De nouveaux défis de régulation

Suite à la nomination d'une nouvelle Commission, de nouvelles initiatives devraient voir le jour dans les mois à venir : la question de la prochaine législation consacrée à la cybersécurité se pose d'ores et déjà. Alors que la perspective d'une version 2 de la directive NIS se fait jour, une approche alternative ou, au moins, parallèle pourrait être de choisir de faire peser les prochaines obligations réglementaires européennes en matière de cybersécurité, sur les fournisseurs de produits et services numériques eux-mêmes plutôt que sur leurs utilisateurs : disponibilité des mises à jour de sécurité, certification, sécurité par défaut, fin de vie des produits, séquestre des codes sources en cas de cessation d'activité… sont autant de pistes à explorer pour renforcer la sécurité des solutions déployées.

Les acteurs de *supply chain* numérique, tels que les intégrateurs, chargés de répercuter les mises à jour, devraient également être concernés. Une telle perspective confirmerait l'orientation stratégique du cadre européen de certification, conçu pour amener des solutions sécurisées *by design* et par défaut aux utilisateurs, et ce faisant, accroître leur confiance dans les usages numériques. De surcroît, ce choix s'inscrirait en cohérence avec les principes de l'Appel de Paris lancé en 2018 par le Président de la République en faveur de l'élaboration de principes communs de sécurisation du cyberespace.