RÉPUBLIQUE
FRANÇAISE

Liberté
Égalité
Fraternité

PAPIERS NUMÉRIQUES

Septembre 2021

PAPIERS NUMÉRIQUES

Septembre 2021

REMERCIEMENTS

L'ANSSI remercie toutes
les personnes interviewées ayant
permis l'élaboration du contenu :

Interviews externes
Jean-Yves Le Drian
ministre de l'Europe et des Affaires étrangères
Karel Řehka
directeur du NÚKIB (République tchèque)

Interviews ANSSI
Guillaume Poupard
directeur général de l'ANSSI

Antoine Berthier
coordinateur sectoriel en charge
des télécommunications
Anne-Charlotte Brou
cheffe du bureau Presse, crise et
communication internationale
Chloé Chabanol
cheffe de la cellule CERT-FR
Jean-Baptiste Demaison
président du conseil d'administration
de l'ENISA, responsable de
l'innovation publique à l'ANSSI
Agathe Favetto
chargée de mission affaires politiques
européennes et internationales
Jonathan Gimenez
chargé de la mise en œuvre
du Cyber Security Act
Aude Le Tellier
cheffe du bureau Affaires politiques
européennes et internationales
Célia Nowak
chargée de mission en management
des crises cyber
Amélie Perron
cheffe adjointe du bureau Affaires
politiques européennes et internationales
Sylvie Pigeon
cheffe adjointe de la division
Coordination internationale
Louis Rouxel
responsable des activités
de coopération du CERT-FR
Anne Tricaud
cheffe de la division Coordination
internationale
Yves Verhoeven
sous-directeur Stratégie

OURS

Papiers numériques – Septembre 2021
édités par l'Agence nationale de la sécurité
des systèmes d'information (ANSSI)

Directeur de rédaction
Guillaume Poupard

Coordination ANSSI
Aline Barrault (projet, interviews et rédaction)
Marc Renaudin (supervision graphique)

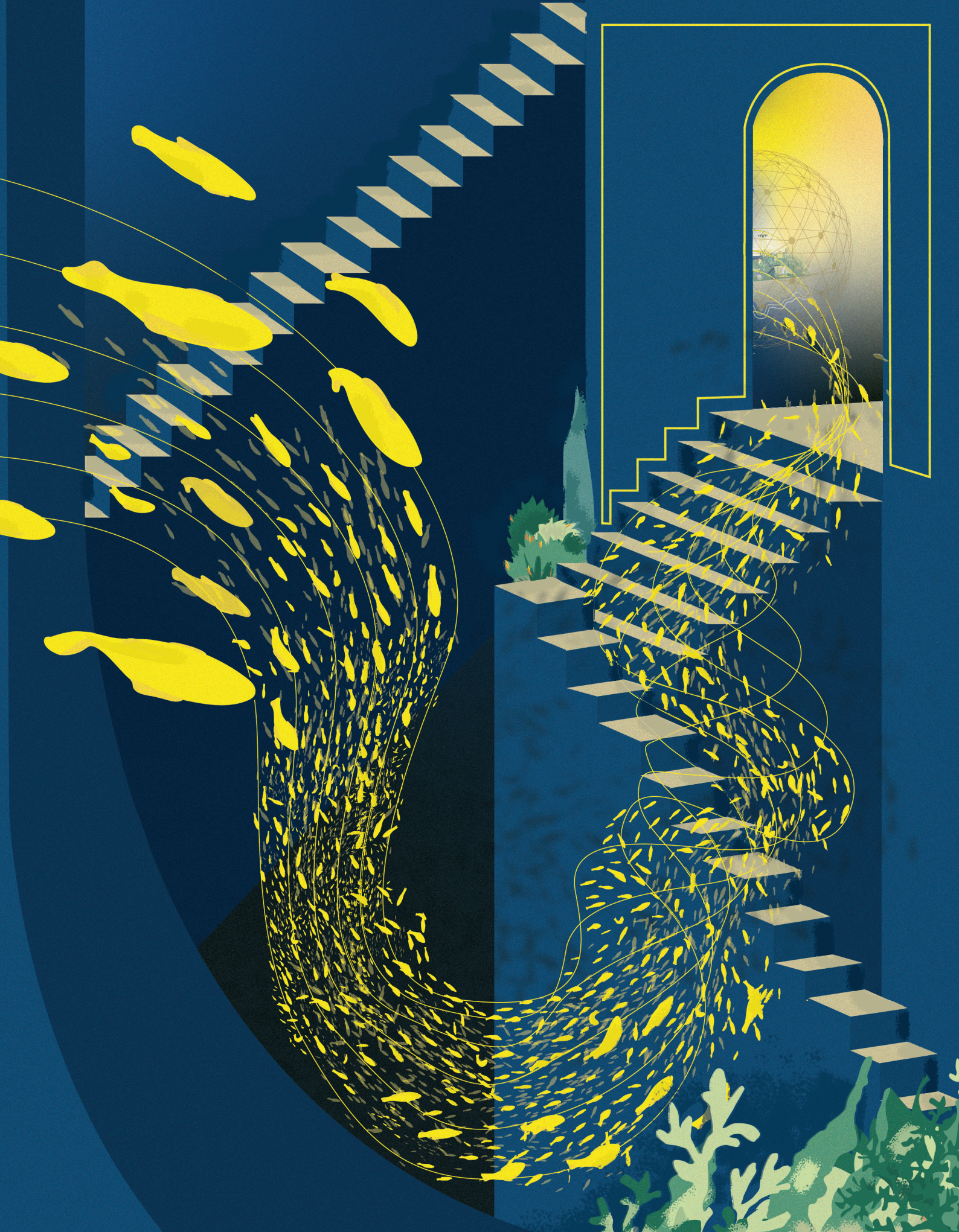
Direction artistique, maquettage
et illustrations
Cercle Studio (www.cerclestudio.com)

Traduction en anglais
Acolad (www.acolad.com/fr)

Dépôt légal
Août 2021

AGENCE NATIONALE DE LA SÉCURITÉ
DES SYSTÈMES D'INFORMATION
51, boulevard de la Tour-Maubourg
75700 PARIS 07 SP

www.ssi.gouv.fr
communication@ssi.gouv.fr



CYBERSÉCURITÉ EUROPÉENNE : HISTOIRE D'UNE MUE CULTURELLE

Au premier semestre 2022, la France présidera le Conseil de l'Union européenne. Une occasion qui, en matière de cybersécurité, offre la perspective d'amplifier des dynamiques en cours depuis quelques années. En préparation de cette échéance, dans les murs de l'ANSSI, quelques maîtres mots résonnent : ambition, passage à l'échelle, coopération, solidarité, souveraineté numérique. Des intentions qui, il y a seulement une décennie, n'étaient pas si intuitives. Retour sur un domaine qui, d'année en année, s'est considérablement « européanisé ».

Quand, au début des années 2010, les instances de l'Union européenne (l'UE) proposent aux États membres un projet de règlementation européenne pour la sécurité informatique, beaucoup se montrent intéressés, mais aussi… prudents.

Prudents, car à l'époque, cybersécurité et cyberdéfense sont principalement perçues comme des affaires régaliennes, relevant de la compétence des États. L'idée que des instances extérieures puissent avoir droit de cité sur ces sujets souverains semble alors contre-intuitive aux *aficionados* du domaine.

Si aujourd'hui, les enjeux de souveraineté nationale restent d'actualité, la façon d'aborder le sujet « cyber » au niveau de l'Europe a bien changé. En une décennie, les échanges entre États et instances de l'Union se sont intensifiés pour aboutir sur des règlements, groupes de coopération, recommandations, référentiels, postures communes et projets d'ampleur. Autant de briques posées en seulement quelques années, qui permettent désormais d'affirmer la valeur inestimable de la coopération européenne. C'est qu'en matière de cyber, l'histoire s'écrit à vitesse grand V.

Pour éviter que ne se développe une Europe de la sécurité à deux vitesses, avec des États plus ou moins vulnérables, la mise en place de mécanismes de protection à l'échelle de l'UE était en fait inéluctable. D'autant que les « frontières » du cyberespace sont poreuses : une attaque affectant les systèmes d'information d'un opérateur au sein d'un État peut, par effet rebond, avoir un impact sur les services qu'il fournit dans d'autres pays. Quand on parle de protection informatique, les intérêts des uns sont souvent aussi ceux des autres.

DÉVELOPPER LES CAPACITÉS NATIONALES

La proposition de directive émise poursuivait donc un objectif louable et nécessaire : défendre une zone d'intérêt commun sur les plans économique et sociétal, l'UE. Mais comment ?

↓
QUAND ON PARLE DE PROTECTION INFORMATIQUE, LES INTÉRÊTS DES UNS SONT SOUVENT AUSSI CEUX DES AUTRES.
↑

« Quand le sujet de la construction d'une cyberdéfense européenne a émergé, le réflexe était de dire qu'il fallait faire à l'échelle européenne ce que l'on faisait à l'échelle nationale », se souvient Guillaume Poupard, directeur général de l'ANSSI. « Nous, on s'y est plutôt opposé. Non pas par défiance, mais par pragmatisme. »

Remettons les choses en perspective. « La partie la plus emblématique du travail de l'ANSSI, historiquement, c'est de stopper les attaques informatiques menées contre les systèmes d'information les plus critiques et d'aider à réparer les dégâts », rappelle Anne Tricaud, cheffe de la division Coordination internationale. « Si une instance européenne avait endossé ces mêmes missions, elle aurait été amenée à intervenir sur les réseaux sensibles d'opérateurs critiques – ministères, grosses entreprises, etc. – des États. » Soit, sur un champ très régalien.

La question de la souveraineté des États membres n'est pas la seule objection posée à l'époque. « Nous n'étions pas convaincus de l'efficacité d'une unique équipe opérationnelle ayant à gérer des crises aux quatre coins du continent », concède Anne Tricaud. « On s'est donc demandé comment construire une cyberdéfense européenne qui soit un plus pour la cyberdéfense nationale », poursuit Guillaume Poupard. « Pour nous, il y avait une priorité : que chaque État développe ses propres capacités à détecter et à réagir aux incidents. »

↓
« POUR NOUS, IL Y AVAIT UNE PRIORITÉ : QUE CHAQUE ÉTAT DÉVELOPPE SES PROPRES CAPACITÉS À DÉTECTER ET À RÉAGIR AUX INCIDENTS. »
↑

GUILLAUME POUPARD
directeur général de l'ANSSI

Pendant trois ans, la France, les États membres et les institutions de l'UE négocient alors ce qui deviendra la directive *Network and information security* (NIS), avec pour principe central le développement des capacités étatiques. La directive prévoit notamment que soient désignées des autorités de cybersécurité au sein de chaque État.

CAP SUR LES OPÉRATEURS ESSENTIELS

Mais l'ambition de NIS ne s'arrête pas là. Dès les premiers échanges, la volonté émise est d'édicter, au niveau européen, des exigences de sécurité pour certains opérateurs critiques.

Lorsque ce sujet émerge à l'échelle européenne, en France, le sujet de la protection d'opérateurs sensibles contre les attaques informatiques est déjà dans les tiroirs du Secrétariat général de la défense et de la sécurité nationale (SGDSN) et de l'ANSSI. Choisissant d'agir à travers la Loi de programmation militaire (LPM), la France ajoute en effet dès 2013 un volet « cyber » à un dispositif déjà existant : la sécurité des activités d'importance vitale (SAIV). En clair, celui-ci impose à un ensemble d'entités publiques ou privées, dont l'activité est considérée comme indispensable à la survie et à la stabilité de la Nation, l'application de mesures de sécurité pour leur protection.

Pour les initiés, on parle alors d'opérateurs d'importance vitale (OIV). Quelques centaines d'organismes sont répartis parmi douze secteurs. Transport, activités militaires, santé, gestion de l'eau ou encore énergie : on imagine assez vite – ou plutôt, on préfère ne pas imaginer – les conséquences potentiellement dramatiques d'une attaque à leur encontre. En plus de prescrire un certain nombre de mesures de sécurité pour les systèmes d'information les plus critiques[1], la LPM impose aux OIV la notification de tout incident cyber à l'ANSSI, autorité nationale en la matière.

Dans la continuité de ces développements en France, ou de manière comparable en Allemagne, c'est donc au niveau européen qu'est ensuite portée la volonté d'actionner le levier règlementaire pour protéger les organisations sensibles d'une menace cyber grandissante. Dans la terminologie de la directive, on ne parle pas d'OIV mais d'OSE : opérateurs de services essentiels.

L'enjeu est alors de taille pour la France, attachée à préserver les ambitions de sa loi nationale. « C'était une vraie rupture », commente Anne Tricaud, cheffe de la division Coordination internationale. « On avait deux textes qui avaient vocation à encadrer la sécurité des infrastructures critiques. Il fallait donc articuler les deux, d'autant que l'on considérait que la cybersécurité restait une question de sécurité nationale. »

Jean-Baptiste Demaison, pilote des négociations à l'ANSSI à l'époque, raconte : « La complémentarité s'est faite en distinguant les types d'opérateurs régulés par les deux textes. La loi française concernait les OIV, critiques pour la sécurité nationale. Quant à la directive NIS, elle s'attachait aux OSE dont la protection vise à sécuriser le marché intérieur. » Un aboutissement qui, pour Yves Verhoeven, sous-directeur Stratégie, marque un jalon fort en matière de cybersécurité : « À une époque où les débats étaient vifs sur le rôle de l'OTAN en la matière, elle a acté, pour l'Europe, le caractère avant tout civil des enjeux de cybersécurité pour les opérateurs essentiels, qui relèvent majoritairement du secteur privé. »

RENFORCER LA COOPÉRATION

Au développement des capacités des États membres et à la protection des structures critiques, la directive européenne ajoute un troisième pilier : le développement de réseaux de coopération. Là encore, l'enjeu est de taille. Car coopérer autour d'activités très techniques, intrinsèquement nationales et souvent confidentielles nécessite une certaine dose d'inventivité.

QU'EST-CE QU'UN CSIRT ?

Un *Computer Security Incident Response Team* (CSIRT) ou *Computer Emergency Response Team* (CERT ; marque déposée) est un centre d'alerte et de réaction aux attaques informatiques.

Il en existe trois types principaux : les CERT internes aux organisations, les CERT de prestataires commerciaux et les CERT gouvernementaux et/ou nationaux.

Les missions du CERT gouvernemental et national français (baptisé CERT-FR, anciennement CERTA) sont assurées par la sous-direction Opérations de l'ANSSI.

2004
Création de l'ENISA

2009
Création de l'ANSSI

2011
Schéma de certification de sécurité de premier niveau (CSPN) pour les produits de sécurité en France

2013
Loi de programmation militaire (LPM)
Protection des opérateurs d'importance vitale (OIV) en France

2016
Directive européenne *Network and information security* (NIS)
Développement des capacités nationales, protection des opérateurs de services essentiels (OSE), création du CSIRTs Network et du groupe de coopération

2019
Cyber Security Act
Adoption d'un mandat permanent pour l'ENISA et d'un cadre européen de certification

2021
Règlement établissant le Centre européen de compétences cyber et le Réseau de centres nationaux de coordination

2022
Présidence française du Conseil de l'Union européenne

[1] On parle alors de systèmes d'information d'importance vitale (SIIV).

L'idée n'est pourtant pas nouvelle : plusieurs mécanismes d'échange[2], informels et basés sur le volontariat, rassemblent alors déjà des CSIRT nationaux et gouvernementaux (voir encadré). Et à l'ANSSI, on connaît leur utilité : l'exemple souvent utilisé dans les murs est celui de la vague mondiale d'infection *WannaCry*, en 2017, pendant laquelle les échanges multilatéraux ont nettement contribué à limiter les dégâts dans l'Hexagone.

Partant du principe qu'encourager la coopération des États permettrait d'élever le niveau global de sécurité de l'Union, la directive NIS crée alors le CSIRTs Network : le premier réseau de coopération et de partage d'informations techniques entre CERT gouvernementaux et nationaux. « Concrètement, on y échange des marqueurs techniques permettant d'anticiper voire d'endiguer des attaques ou des conseils en termes de développement d'un CSIRT », détaille Chloé Chabanol, cheffe de la cellule CERT-FR à l'ANSSI.

Au-delà des États membres, les institutions européennes ont aussi leur propre CERT dédié : le CERT-EU. Yves Verhoeven raconte : « Face à la sophistication de la menace, il est apparu évident que les institutions européennes devaient s'organiser pour disposer d'une capacité commune de réponse aux incidents. » Créé en 2011 à l'initiative de plusieurs États partenaires, dont la France, celui-ci prend également part au CSIRTs Network.

Quelques années après son lancement, le réseau européen est rodé et fructueux. Réunions plénières, plateformes, *mailing-lists*, *chat* dédié… Le réseau tourne et se développe en continu. Louis Rouxel, responsable des activités de coopération du CERT-FR, confirme : « Tous les États

[2] On peut citer le Forum of Incident Response and Security Teams (FIRST), l'International Watch and Warning Network (IWWN) ou encore l'European Government CERT Group (EGC).

↓
« TOUS LES ÉTATS MURISSENT ET DÉVELOPPENT LEURS CAPACITÉS À COOPÉRER. L'ÉCHANGE D'INFORMATION EST VRAIMENT DANS NOTRE ADN. »
↑

LOUIS ROUXEL
responsable des activités de coopération du CERT-FR

murissent et développent leurs capacités à coopérer. L'échange d'information est vraiment dans notre ADN. »

DU NIVEAU TECHNIQUE AU NIVEAU STRATÉGIQUE

C'est avec cette directive bien ficelée que débute ce qu'Anne Tricaud appelle la « mue européenne » de l'agence. « On a pu constater que la directive NIS nous permettait de renforcer le niveau de sécurité de l'ensemble de l'Union, de protéger plus d'acteurs, de nous coordonner avec nos partenaires… et ainsi, de contribuer à renforcer la sécurité nationale. Alors on a commencé à se dire que traiter le sujet cyber à l'échelle européenne… c'était une très bonne chose ! »

D'autant que NIS permet aussi la création d'un groupe de coopération stratégique. Initialement pensé pour échanger sur la mise en œuvre de la directive, l'enceinte a évolué pour accueillir des sujets plus larges, comme la sécurisation des technologies liées à la 5G. Un sujet qui n'est pas étranger aux intérêts de grandes puissances mondiales, aux positions parfois antagonistes, face auxquelles la voix de l'Europe se doit d'être concordante. Antoine Berthier, coordinateur sectoriel en charge des télécoms à l'ANSSI, dresse le bilan : « Nous avons trouvé une position équilibrée en nous concentrant sur les enjeux techniques et de sécurité. Chaque pays a fait son analyse de risque pour faire émerger un ensemble de recommandations. » Pour Yves Verhoeven, la création de cet instrument est un double succès : « D'une part parce qu'elle est le fruit d'une coopération intelligente entre la Commission et les États membres face à un grand défi technologique de notre époque. D'autre part, parce qu'elle constitue une première illustration de ce que peut être la souveraineté numérique européenne : ni naïve, ni autarcique. »

Plus récemment, le groupe a fait un petit en incubant… CyCLONe[3]. Dédié à la gestion de crise, ce tout jeune réseau rassemble les homologues européens du directeur général de l'ANSSI. « En 2018, l'organisation d'un exercice de gestion de crise au niveau européen a mis en lumière le besoin d'un échelon de coopération à un niveau plus stratégique que le CSIRTs Network, qui a une vocation technique », raconte Agathe Favetto. À ce constat s'est ajoutée la volonté émise par Guillaume Poupard de pouvoir se préparer à une crise de grande ampleur avec ses homologues européens. L'événement Blue OLEx, organisé à Paris en 2019, permet alors une première rencontre et, dans la foulée, la création formelle de CyCLONe.

« On n'a pas encore eu à tester le grand soir » se rassure Guillaume Poupard. « Mais le travail de préparation que l'on fait aujourd'hui sera autant de temps de gagné quand le moment viendra. » Plus à même de prendre du recul sur les incidents techniques, d'avoir une vision globale des impacts et de conseiller le niveau politique, CyCLONe continue de se rôder, en développant aussi ses interactions avec le CSIRTs Network.

UNE AGENCE QUI RÉUNIT

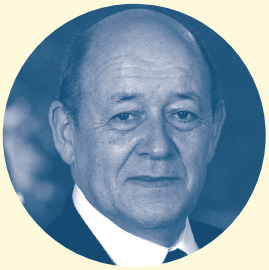
On peut dire que NIS a ouvert la voie à toutes les initiatives qui ont suivi pour la construction d'une véritable cybersécurité européenne. Qu'à partir des fondations solides qu'elle a posées, toutes les briques qui s'assemblent depuis ne peuvent que s'agencer de façon naturelle.

Mais un petit retour en arrière s'impose. Car une première pierre avait en fait été posée plusieurs années avant le tournant de la fameuse directive européenne, un peu comme pour marquer le lieu où se construirait l'édifice. Dès 2004, une institution était conçue comme un moyen de renforcer la coopération entre les États du continent ; une agence européenne pour la cybersécurité : l'ENISA[4].

Plusieurs années avant l'acceptation de la notion même de cybersécurité

[3] Cyber Crisis Liaison Organisation Network

[4] European Union Agency for Cybersecurity



« La France promeut, depuis les débuts de la mise en œuvre de la stratégie numérique européenne, une vision au cœur de laquelle se trouve la souveraineté numérique. »

JEAN-YVES LE DRIAN

Ministre de l'Europe et des Affaires étrangères

Comment la coopération entre le ministère de l'Europe et des Affaires étrangères (MEAE) et l'ANSSI permet de promouvoir les intérêts français en matière de cybersécurité ?

Le MEAE et l'ANSSI coopèrent étroitement pour conduire l'action internationale de notre pays dans le domaine de la cybersécurité. En premier lieu, nous travaillons de concert pour renforcer les coopérations avec nos partenaires. Le MEAE et l'ANSSI participent aussi aux dialogues stratégiques bilatéraux que nous entretenons avec les États les plus significatifs sur les grands enjeux de cybersécurité. En deuxième lieu, l'ANSSI appuie le MEAE dans la définition des positions françaises dans les enceintes multilatérales, notamment aux Nations unies, pour défendre notre vision d'un cyberespace ouvert, sûr, stable, accessible et pacifique. Nous portons également la conception française du rôle des acteurs privés dans la gouvernance du cyberespace, notamment à l'Organisation de coopération et de développement économiques. Enfin, au niveau de l'UE, l'ANSSI et le MEAE promeuvent l'ambition d'une souveraineté numérique européenne fondée notamment sur une cybersécurité renforcée.

Dans quelle mesure la Présidence française du Conseil de l'Union européenne représente une opportunité pour faire avancer les priorités cyber ?

Le cyber est l'une des priorités de notre Présidence du Conseil de l'Union européenne en matière de numérique. Il s'agira en premier lieu de favoriser la capacité des États membres à être solidaires en cas d'incident cyber majeur ou d'attaque. Pour ce faire, le renforcement des capacités et de la résilience de l'UE comme des États membres est essentiel. C'est pourquoi nous mettrons un accent particulier sur le renforcement de la sécurité des réseaux de l'UE. Sur le plan de l'action extérieure de l'Union, nous comptons proposer une revue de la stratégie de l'UE en matière de renforcement capacitaire pour les pays tiers, afin de mieux coordonner les actions menées. Il s'agira aussi de développer la recherche et l'innovation industrielle européenne dans le domaine cyber. Ces actions s'inscriront pleinement dans le cadre de la mise en œuvre de la stratégie de cybersécurité de l'Union.

Comment la France entend soutenir la construction d'un espace numérique sécurisé, de confiance et prospère à l'échelle européenne ?

La clé de la construction de l'Europe numérique passe par la définition d'une compréhension commune des objectifs répondant aux défis, majeurs, posés dans ce domaine. C'est pourquoi la France promeut, depuis les débuts de la mise en œuvre de la stratégie numérique européenne, une vision au cœur de laquelle se trouve la souveraineté numérique. Nous entendons par là la promotion d'un modèle fondé sur nos valeurs, qui ne se veut ni un repli sur soi ni une volonté hégémonique, mais qui favorisera au contraire l'ouverture de l'Union sur le monde, tout en garantissant son indépendance et la préservation de ses intérêts. Il doit favoriser à la fois la cybersécurité, l'innovation, des normes responsables, et la protection des grands communs numériques. Nous soutenons les initiatives européennes, en cours et futures, destinées à concrétiser cet agenda et militons pour une adoption de ces instruments qui reflète cet état d'esprit. ●

européenne et les premiers pas en ce sens, cette agence un peu pionnière fait figure d'OVNI. En une décennie, l'ENISA développe pourtant des missions qui s'avèrent essentielles. La première sur la liste : l'organisation de l'exercice Cyber Europe, ce rituel bisannuel simulant des crises d'origine cyber et testant la capacité des États à y faire face. Et en 2019, quinze ans après sa création, c'est avec l'adoption du *Cyber Security Act* que l'ENISA prend une autre dimension.

Ce règlement confère à l'ENISA un mandat permanent et des missions clairement définies. Pour Jean-Baptiste Demaison, président du conseil d'administration de l'agence européenne depuis 2016, « l'ENISA assure un rôle essentiel de coordination. Dans le cadre des différents groupes et réseaux rassemblant les États membres sur les sujets cyber, c'est tout naturellement elle qui assume l'animation et la synthèse des travaux. »

Au-delà de cette première fonction, l'ENISA porte une mission cruciale de mise à disposition de bonnes pratiques et de sensibilisation. « C'est sans doute le champ sur lequel elle a été la plus essentielle », commente Jean-Baptiste Demaison, « avec ses formations, ses guides, ses exercices et le pilotage du Mois européen de la cybersécurité (baptisé Cybermoi/s en France, NDLR). Elle a aussi pris de la légitimité sur les politiques publiques européennes, où elle peut être consultée pour bâtir des orientations. Enfin, elle peut conseiller les États victimes d'incidents qui en font la demande ».

Loin des incertitudes premières, l'ENISA démontre à présent son caractère indispensable. « C'est une grande alliée dans l'écosystème cyber européen qui est extrêmement varié et complexe. Sans instance de coordination, il y aurait un vrai risque d'éparpillement », conclut Jean-Baptiste Demaison.

GARANTIR LA CONFIANCE DANS L'ÉCOSYSTÈME

Et le *Cyber Security Act* confère à l'ENISA une autre mission fondamentale. Car le règlement de 2019 ajoute un nouvel étage à la fusée en créant un cadre européen de certification de sécurité (voir encadré). Un véritable tournant pour la sécurité et la confiance numérique en Europe.

Le principe : harmoniser les pratiques de certification des États membres pour permettre une reconnaissance mutuelle au sein de l'UE. Ainsi, une prestation suédoise certifiée le serait aussi, par exemple, au Portugal ou en Hongrie.
Le développement d'un tissu industriel européen capable de délivrer des prestations de confiance est ici un sujet central. « Faire certifier des prestations demande beaucoup de ressources aux fournisseurs », précise Amélie Perron, au cœur des négociations de ce volet du *Cyber Security Act*. « Développer l'accès à un marché européen les incite donc à se lancer dans cette démarche. Et par effet domino, cela sert notre objectif : l'élévation du niveau global de sécurité. »

Le projet est donc ambitieux. « Le sujet pour l'ANSSI, c'était d'éviter que l'homogénéisation des pratiques soit synonyme de nivellement par le bas », continue Amélie Perron. Pour éviter ce risque, le règlement s'assure de la bonne maîtrise du processus par les spécialistes au sein des États membres. Des autorités nationales de certification[5] sont donc désignées et mises en réseau[6]. En France, c'est l'ANSSI qui endosse le rôle.

Il faut noter qu'en lui-même, le *Cyber Security Act* définit un cadre et une gouvernance sans pour autant préciser les règles de certification. Les produits, services et processus qui auront vocation à être certifiés feront successivement l'objet de schémas thématiques. Une déclinaison qui a donc vocation à se faire en continu par les États membres, l'ENISA tenant la plume.

L'un de ces schémas, en cours de négociation, concerne un sujet connu et emblématique : le *cloud*. Sur cette question, un enjeu de taille concerne l'immunité aux lois extraterritoriales non-européennes. Une expression technique qui dissimule un enjeu fondamental : la protection face à l'accès par des puissances étrangères, grâce à leur propre règlementation et sous certaines conditions, aux données hébergées chez leurs fournisseurs de services *cloud*. Y compris lorsque les serveurs en question sont localisés sur le territoire de l'UE.

La qualification française SecNum*Cloud* – qui sera à terme remplacée par le schéma de certification européen équivalent – intègre déjà cette « immunité » en assurant à ses utilisateurs l'application exclusive du droit européen et une maîtrise des données hébergées. En intégrant cette disposition à l'échelle du continent, après le Règlement général sur la protection des données à caractère personnel (RGPD), l'UE témoignerait une nouvelle fois de son intention d'agir pour la préservation des données des organisations et des citoyens européens. « Ne pas le faire reviendrait à condamner les utilisateurs

QU'EST-CE QUE LA CERTIFICATION ?

La certification est l'attestation de la robustesse d'un processus, produit ou service de sécurité. En France, la certification de haut niveau est délivrée sous l'appellation « Visa de sécurité » à l'issue d'un processus rigoureux de vérification, sous l'autorité de l'ANSSI.

En France, la LPM impose aux OIV de faire appel aux organismes détenteurs d'un visa de l'ANSSI pour certaines prestations. La certification confère aux utilisateurs une confiance dans le niveau de sécurité des prestations demandées et permet aux fournisseurs d'accéder à de nouveaux marchés.

[5] On parle de National Cybersecurity Certification Authority (NCCA) ; autorités nationales de certification de cybersécurité.

[6] À travers l'European Cybersecurity Certification Group (ECCG)

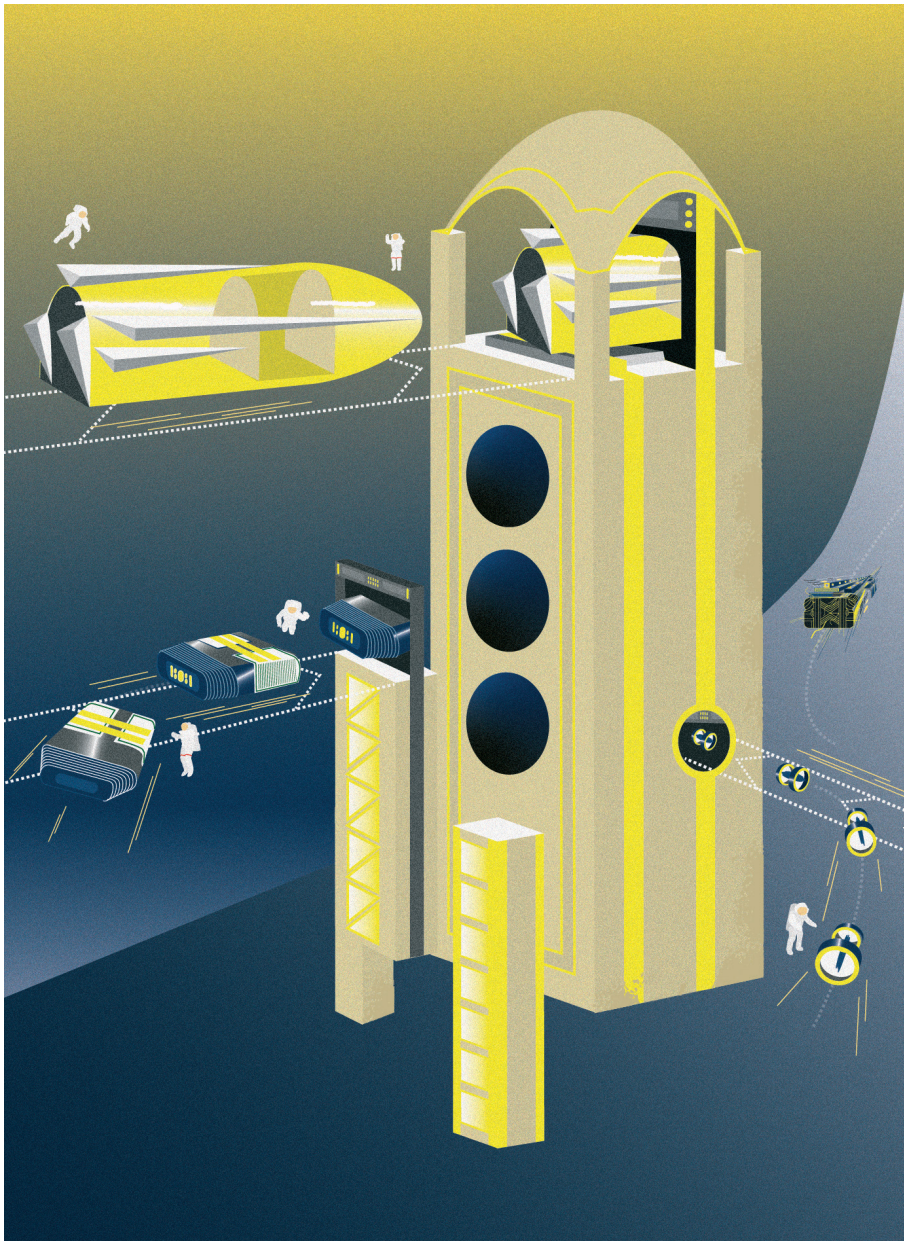
européens à une absence de maîtrise de leurs données », résume Amélie Perron. Anne Tricaud conclut : « C'est un vrai sujet de souveraineté européenne. »

PASSAGE À L'ÉCHELLE

« On parle beaucoup du *cloud*, mais la certification va bien au-delà », tient tout de même à rappeler la cheffe de la division Coordination internationale. D'autant que le cadre européen prévoit trois niveaux de certification : élémentaire, substantiel et élevé. Si le dernier correspond peu ou prou au spectre historique de l'ANSSI en la matière, l'ajout des deux premiers niveaux change la donne. Dans les murs de l'ANSSI, on parle même de « révolution » : les prestations certifiées s'adresseront aux petites entreprises, associations, collectivités et citoyens… très loin des OIV et OSE historiques ! Une nouveauté qui implique donc un changement de méthode. « Au niveau élevé, l'ANSSI agrée des laboratoires d'évaluation (les CESTI[7], NDLR), valide les rapports et prononce elle-même la certification », détaille Jonathan Gimenez, en charge de la mise en œuvre du *Cyber Security Act*. « Pour passer à l'échelle sur les niveaux élémentaire et substantiel, l'ANSSI autorisera, sous certaines conditions, des organismes privés à délivrer les certifications. »

Et, alors que la « certif » concerne historiquement avant tout des produits de sécurité (cartes à puces, VPN, chiffreurs, etc.), elle englobera de plus en plus des produits numériques ayant vocation à être sécurisés *by design*, mais aussi des services ou processus essentiels à la construction d'un espace numérique sécurisé. En témoignent les travaux à venir autour d'objets connectés ou encore des processus de développement sécurisé. Les possibilités sont donc très larges et extrêmement prometteuses pour la confiance numérique sur le continent. « On se demandait au départ quels sujets méritaient d'être

[7] Centre d'évaluation de la sécurité des technologies de l'information. Voir glossaire.



↓
« LE SUJET POUR L'ANSSI, C'ÉTAIT D'ÉVITER QUE L'HOMOGÉNÉISATION DES PRATIQUES SOIT SYNONYME DE NIVELLEMENT PAR LE BAS. »
↑

AMÉLIE PERRON
cheffe adjointe du bureau Affaires politiques européennes et internationales

portés au niveau de l'Union », résume Guillaume Poupard. « De fait, quand on parle de certification, on voit bien que cela a beaucoup plus de sens de le faire avec nos partenaires européens plutôt que seuls, dans notre village gaulois. »

PRÉPARER LA SUITE

En matière de développement du tissu industriel cyber, une autre étape majeure vient d'être franchie. Car alors qu'on dénombre, au sein de l'UE, une multitude de pôles d'expertise en matière de recherche et d'innovation cyber, un nouveau règlement vient d'être adopté pour assurer leur coordination. « Il s'agit d'établir une feuille de route commune pour permettre à tous ces acteurs de travailler sur la base de priorités identifiées », précise Aude Le Tellier. « On évitera ainsi de disperser des fonds sur des projets qui ne se transformeraient pas en solutions sur le marché, ou qui ne correspondraient pas aux besoins des utilisateurs ». Pour ce faire, le règlement prévoit des mécanismes de coordination au niveau des États mais aussi au niveau européen. Ainsi, un centre de compétences cyber, localisé à Bucarest, pourra lui-même organiser des appels à projets. « Ce règlement promet d'être fondamental pour l'autonomie stratégique de l'UE».

En cours de réflexion pour l'avenir de la cybersécurité européenne, il y a aussi et surtout la révision de la directive NIS. Une « V2 » qui promet d'introduire des évolutions majeures, anticipe Anne Tricaud : « À travers cette nouvelle directive, nous pourrions être amenés à réguler un champ beaucoup plus vaste d'opérateurs. De très nombreuses entreprises et organisations seraient concernées. » Un changement de dimension nécessaire, au vu de la menace observée. Mais dont l'ampleur impliquera un véritable « changement culturel » pour l'ANSSI, qui devra faire évoluer ses méthodes comme elle le fait depuis sa création. Un peu à l'image des changements opérés pour le passage à l'échelle de la certification.

↓
LES PRESTATIONS CERTIFIÉES S'ADRESSERONT AUX PETITES ENTREPRISES, ASSOCIATIONS, COLLECTIVITÉS ET CITOYENS… TRÈS LOIN DES OIV ET OSE HISTORIQUES !
↑

Enfin, au-delà du renforcement du niveau de sécurité des États membres et de leurs opérateurs critiques, la sécurisation des institutions et des organes de l'UE sera probablement encadrée par de nouvelles règlementations protectrices.

Les efforts de coordination pour un modèle de cybersécurité européenne portent leurs fruits, enclenchent de nouvelles dynamiques et démontrent tout l'intérêt de faire de la « cyber » un enjeu stratégique et politique. Mais si cette mise en musique est primordiale, les considérations purement techniques demeurent centrales. Aussi, certains principes fondateurs, tels le recours au chiffrement, nécessitent également d'être portés à l'échelle européenne. « Depuis vingt-cinq ans, on a vu un peu partout une démocratisation des solutions cryptographiques », se remémore Guillaume Poupard. Chacune et chacun peut, dans son quotidien mesurer les conséquences de cette évolution ayant permis, notamment, la sécurisation des nombreux moyens de communication que nous utilisons en permanence à l'image des applications de messagerie chiffrées de bout en bout[8]. Le directeur général poursuit : « Depuis, il y a eu des débats aux quatre coins du monde sur l'entrave que cela pouvait constituer pour les services d'enquête. »

[8] Voir glossaire.

« Nous devons nous assurer que l'UE reste à la pointe de l'évolution technologique sans faire de compromis sur la sécurité. »

KAREL ŘEHKA

Directeur
Agence nationale de la cybersécurité (NÚKIB)
République tchèque

En 2010, la République tchèque et la France ont conclu un accord de partenariat stratégique. Depuis, nous avons entretenu une coopération de plus en plus fructueuse, notamment dans le domaine de la cybersécurité. Je suis heureux d'avoir l'opportunité de revenir sur ces nombreuses années d'engagement mutuel et, à l'approche de nos présidences respectives du Conseil de l'Union européenne, d'évoquer en quelques mots les prochains grands enjeux que nous pourrons aborder ensemble en matière de cyberpolitique européenne.

Permettez-moi tout d'abord un petit retour en arrière. Ce qui a commencé comme un engagement bilatéral de courtoisie en 2013 – lorsque mon prédécesseur a rencontré pour la première fois le directeur de l'ANSSI – avait déjà changé de braquet en 2017, avec les échanges sur la cybersécurité, le PRS Galileo, la cryptographie et les capacités TEMPEST. En 2018, nous avons ajouté l'analyse de la menace cyber, ou *Cyber Threat Intelligence* (CTI) à nos discussions. Je suis heureux que ces interactions n'aient cessé de croître au fil des années, que ce soit sur les questions de technologie ou les échanges sur les attaquants. En 2020, conscient de cette relation privilégiée, le NÚKIB a nommé un cyber-attaché pour entretenir les relations bilatérales avec la France.

À l'approche de 2022 – année où la France, puis la République tchèque, assureront la présidence tournante du Conseil – je sais que le lien qui nous unit ne peut que se renforcer. Le programme qui nous attend est chargé. Nous serons à vos côtés (ou, plus précisément, nous resterons à vos côtés) lorsque vous ferez progresser les négociations sur la révision de la directive NIS, en vous souhaitant de mener à bien ce dossier. Nous reprendrons à notre tour le flambeau là où vous l'avez laissé en veillant à ce que les institutions, les organes et les agences de l'Union européenne puissent compter sur une cybersécurité résiliente et sur un mécanisme solide de réponse coordonnée en cas de défaillance de leurs systèmes de défense. À la suite de la pandémie de COVID-19, alors qu'il nous faut nous reconstruire, nous nous efforcerons de soutenir nos efforts numériques en mettant l'accent sur la sécurité et la disponibilité continue des technologies, y compris celles qui semblent encore émergentes, mais qui, dans de nombreux cas, sont déjà utilisées. Nous devons nous assurer que l'UE reste à la pointe de l'évolution technologique, mais en même temps, nous ne devons pas faire de compromis sur la sécurité lorsque nous cherchons à rendre les nouvelles technologies disponibles. Cela implique d'engager des discussions sur des chaînes d'approvisionnement sûres et résilientes. Dans cette perspective, nous espérons vous accueillir à nouveau, cette année et l'année prochaine, à la conférence de Prague sur la sécurité de la 5G. Comme lors des deux premières éditions, je suis sûr que votre soutien sera d'une importance majeure. ●

Ce à quoi l'ANSSI a toujours rappelé l'importance que constituent ces mécanismes pour la sécurité numérique. Mettre en place une solution systémique (visant, par exemple, à interdire ou affaiblir le chiffrement) rendrait possible des scénarios d'attaques potentiellement catastrophiques. Quant à l'intégration de portes dérobées[9] (ou *backdoors*), elle reviendrait à créer des passe-partout qui, inévitablement, se retrouveraient entre les mains des attaquants. « D'autant que ces mesures ne seraient probablement pas utiles aux services d'enquête : les personnes malfaisantes se débrouilleraient bien pour utiliser d'autres outils. Tout ce qui a été envisagé jusqu'à présent pour permettre un contournement systématique du chiffrement a démontré son inefficacité et sa dangerosité », constate Guillaume Poupard.

Pour trouver une solution à la fois viable en termes de sécurité numérique et efficace pour les services d'enquête, l'ANSSI se prononce en faveur de mécanismes spécifiques, ponctuels et ciblés. « On peut imaginer, avec les fournisseurs de services *over-the-top*[10] (OTT), des pistes intermédiaires respectueuses des données privées, mais permettant l'accès à certaines données sous requête d'un juge » propose le directeur général de l'ANSSI. « Par exemple en permettant, dans les cas qui l'exigent, l'accès à certaines informations annexes au contenu des communications. » Des solutions qui, pour constituer une alternative aux réflexes contraires qui émergent ailleurs sur le globe, méritent incontestablement d'être élaborées de façon concertée à l'échelle européenne.

PENSER LA SOLIDARITÉ

Au premier semestre 2022, la France présidera le Conseil de l'Union européenne. L'occasion pour elle de porter de grandes orientations en matière de cybersécurité. « Nous faisons face à une menace grandissante avec des incidents majeurs, aux impacts qui seront de plus en plus importants et transfrontaliers. Il nous faut donc des mesures ambitieuses », estime Agathe Favetto. Anne Tricaud abonde : « Le sens de l'histoire, c'est d'aller vers plus de solidarité. Maintenant, reste à proposer des mécanismes efficaces. »

Car en pratique, si une crise dépasse les capacités d'un État membre, comment réagir ? « On ne croit pas que la solution souhaitable soit de créer une équipe européenne permanente », prévient Guillaume Poupard. Pour mettre en place une solidarité européenne, l'ANSSI penche plus volontiers pour des mécanismes d'assistance mutuelle bien délimités et respectueux des besoins propres des États.

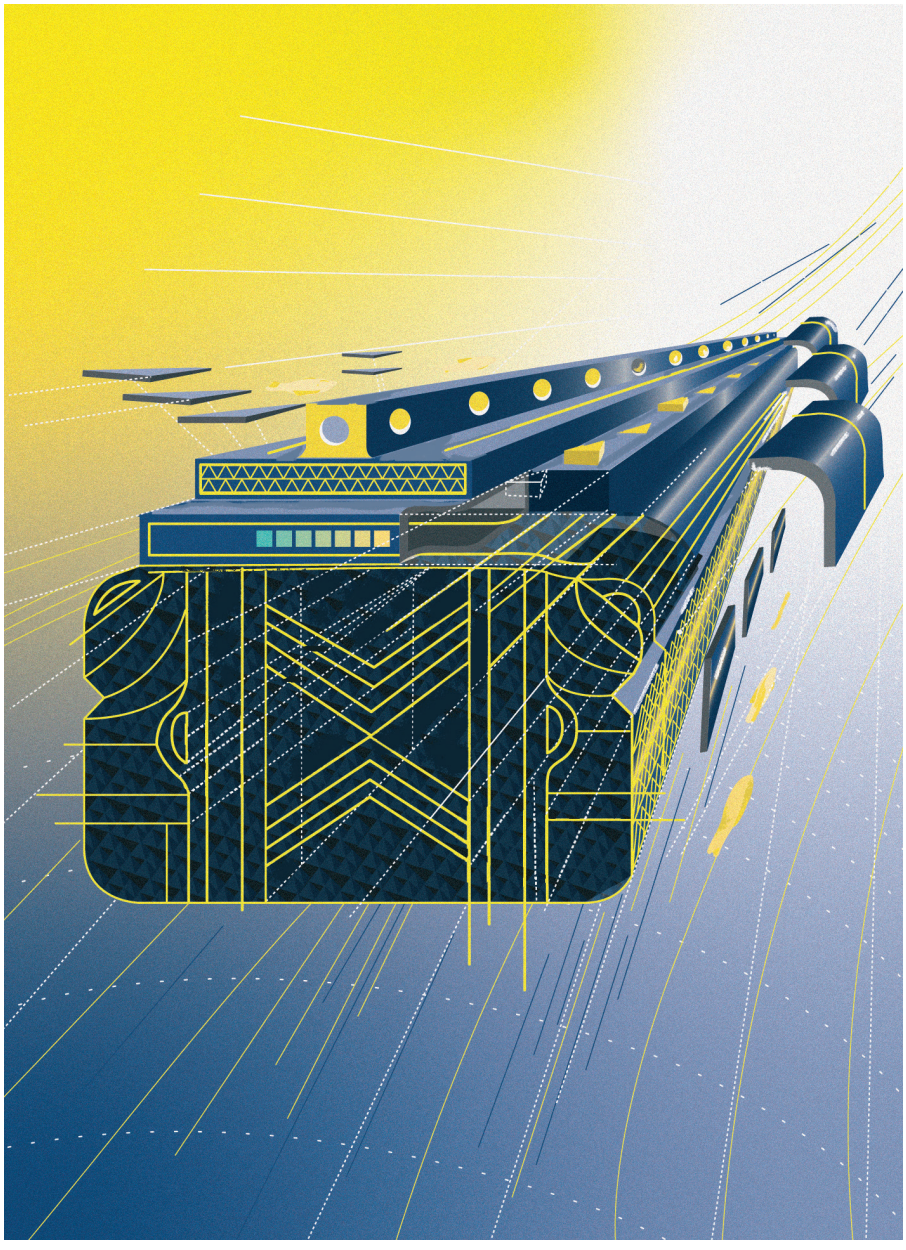
Mais surtout, une idée sort du lot : l'appel à des prestataires de services certifiés à l'échelle européenne. « La solidarité ne pourra se mettre en place que si la capacité des États est démultipliée grâce aux prestataires privés de confiance », estime Anne Tricaud. « Y compris en France, l'autorité nationale ne peut pas répondre à tous les incidents. Le modèle des prestataires de confiance permet aux opérateurs critiques de faire appel à des prestataires d'audit, de détection ou de réponse à incidents. » Guillaume Poupard abonde : « Miser sur ce modèle permettrait d'éviter d'avoir à dégarnir un front pour en fournir un autre. C'est sans doute la meilleure façon de pouvoir adapter la main-d'œuvre disponible en cas de crise, un peu à l'image de ce que l'on fait déjà à l'échelle nationale. »

Toutes ces pistes pourraient être expérimentées pendant la présidence française à travers un exercice de crise qui pourrait lier les niveaux technique (avec le CSIRTs Network), stratégique (avec CyCLONe) et politique, au niveau des ministres des Affaires étrangères. « Cet exercice nous permettrait de faire jouer ensemble ces trois niveaux et de répondre à cette question : que signifie concrètement la solidarité euro-

↓
« TOUT CE QUI A ÉTÉ ENVISAGÉ JUSQU'À PRÉSENT POUR PERMETTRE UN CONTOURNEMENT SYSTÉMATIQUE DU CHIFFREMENT A DÉMONTRÉ SON INEFFICACITÉ ET SA DANGEROSITÉ »
↑

GUILLAUME POUPARD
directeur général de l'ANSSI

9, 10 *Ibid.*



↓
« LA SOLIDARITÉ NE POURRA SE METTRE EN PLACE QUE SI LA CAPACITÉ DES ÉTATS EST DÉMULTIPLIÉE GRÂCE AUX PRESTATAIRES PRIVÉS DE CONFIANCE »
↑

ANNE TRICAUD
cheffe de la division Coordination internationale

péenne ? », anticipe Célia Nowak, chargée de mission en management des crises cyber à l'ANSSI.

Toujours est-il qu'à travers les réflexions en cours sur la solidarité, on peut dresser un bilan positif des étapes franchies jusqu'à présent. Guillaume Poupard résume : « D'abord, on a fait en sorte que les États développent leurs propres capacités et protègent leurs opérateurs critiques. Puis, on les a mis en réseau. On a ensuite travaillé à l'émergence d'un écosystème industriel de confiance. Et maintenant qu'on a posé toutes ces bases, nous sommes prêts à appréhender sérieusement cette question de solidarité européenne. »

« Au sens technique comme au sens politique, le sujet cyber est, sur certains aspects, très national », continue Guillaume Poupard « mais sur d'autres, il est aussi profondément européen. Pour construire un modèle cohérent et efficace face à la menace, le tout est d'assembler les briques dans le bon ordre. Jusqu'à présent, c'est ce qu'on a fait. » La suite de l'histoire ne demande plus qu'à être écrite… ●

GLOSSAIRE

Centre d'évaluation de la sécurité des technologies de l'information (CESTI)
Laboratoires réalisant des évaluations de sécurité de produits. Les CESTI agissent en tant que tierce partie, indépendante des développeurs et des commanditaires, et doivent être agréés par l'organisme de certification. À ce titre, les CESTI sont tenus de respecter les règles élaborées par l'ANSSI.

Chiffrement de bout en bout
Le chiffrement de bout en bout désigne les systèmes de communication avec lesquels seuls les équipements situés aux extrémités de l'échange ont accès aux clés de déchiffrement. Autrement dit, les fournisseurs de service n'ont alors pas la capacité d'accéder aux données en clair se déplaçant d'un utilisateur à l'autre.

CyCLONe
Réseau de coopération complétant les structures de cybersécurité existantes au niveau de l'Union européenne. Il relie les instances de coopération des niveaux technique (CSIRTs Network) et politique (Integrated Political Crisis Response – IPCR). Il permet ainsi l'évaluation coordonnée de l'impact lors d'une crise et des consultations sur les stratégies de réponse nationales, au profit des décideurs politiques.

Opérateurs d'importance vitale (OIV)
Opérateur conduisant une ou des activité(s), telles que mentionnée(s) à l'article R. 1332-2 du code de la Défense, dont le dommage, l'indisponibilité ou la destruction risquerait d'obérer gravement le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation ou de mettre gravement en cause la santé ou la vie de la population.

Opérateurs de services essentiels (OSE)
Opérateur tributaire de réseaux ou systèmes d'information fournissant un service dont l'interruption aurait un impact significatif sur le fonctionnement de l'économie ou de la société.

Porte dérobée (*backdoor*)
Moyen d'accéder à un système informatique ou à des données chiffées de façon dissimulée, en contournant les mécanismes de sécurité. La porte dérobée peut être matérielle ou logicielle, volontairement mise en place par le concepteur ou installée par un attaquant.

Sécurité des activités d'importance vitale (SAIV)
Le dispositif de SAIV constitue le cadre permettant d'associer les opérateurs d'importance vitale (OIV) à la mise en œuvre de la stratégie de sécurité nationale en termes de protection contre les actes de malveillance et les risques naturels, technologiques et sanitaires. Placés au cœur du dispositif, les opérateurs d'importance vitale identifiés doivent ainsi analyser les risques auxquels ils sont exposés et appliquer les mesures de protection qui leur incombent.

Service par contournement ou *over-the-top* (OTT)
Services permettant la distribution de contenu (messages, audio, images…) via une connexion internet, sans participation d'un opérateur de réseau traditionnel.