# Protection des infrastructures critiques : cinq ans après la loi

Par **Yves VERHOEVEN**
Agence nationale de la Sécurité des Systèmes d'Information (ANSSI)

## Génèse d'un dispositif réglementaire

### Émergence d'une préoccupation globale

Les enjeux de cybersécurité sont désormais bien connus : aux vagues successives de virus subies par le grand public depuis le début des années 2000 viennent s'ajouter les révélations d'attaques ciblées hautement sophistiquées, conduites à l'initiative d'États. Outre des activités de cyberespionnage, ces révélations ont mis au jour des attaques de sabotage contre des infrastructures soutenant des activités économiques ou industrielles, à l'image de l'opération Olympic Games contre les centrifugeuses iraniennes en 2010, de la cyberattaque à des fins de sabotage contre la chaîne TV5Monde en 2015, ou encore des attaques en 2015 et 2016 contre la grille électrique ukrainienne, privant d'électricité plusieurs centaines de milliers de foyers ukrainiens.

Ces événements éclairent *a posteriori* les préoccupations des premiers pays qui, dès la fin du XX$^{e}$ siècle, ont identifié le risque de déstabilisation majeure des cyberattaques et ont commencé à se mobiliser. Ainsi, la première résolution de l'Assemblée générale des Nations Unies sur le sujet (résolution 53/70 issue du premier comité sur le désarmement et la sécurité internationale à l'initiative de la Russie, « Les progrès de la téléinformatique dans le contexte de la sécurité internationale ») date du 4 janvier 1999.

La cybersécurité des infrastructures critiques est rapidement apparue prioritaire, puisque la poursuite des travaux sur le sujet au sein des Nations Unies a abouti en 2004 à la résolution 58/199 portant sur la « Création d'une culture mondiale de la cybersécurité et protection des infrastructures essentielles de l'information ». Dans cette résolution, l'Assemblée générale « note que désormais, par suite des progrès de l'interconnectivité, les infrastructures essentielles de l'information se trouvent exposées à des menaces et à des faiblesses toujours plus nombreuses et diverses qui donnent lieu à de nouvelles préoccupations en matière de sécurité » et « invite les États membres et toutes les organisations internationales compétentes à tenir compte, notamment, de ces éléments et de la nécessité de la protection des infrastructures essentielles de l'information ».

Quelques années plus tard, en 2008, c'est l'Organisation de coopération et de développement économique (OCDE) qui produit, *via* son groupe de travail sur la sécurité de l'information et la vie privée, et adopte lors de sa 1 172$^{e}$ session, le 30 avril 2008, la « Recommandation de l'OCDE du Conseil sur la protection des infrastructures d'information critiques [C(2008)35] ». Dans celle-ci, le Conseil de l'OCDE « [reconnaît] que le fonctionnement de nos économies et de nos sociétés est de plus en plus tributaire de systèmes et réseaux d'information qui sont interconnectés et interdépendants, au plan tant intérieur qu'international ; qu'un certain nombre de ces systèmes et réseaux sont d'une importance nationale critique ; et que leur protection est un domaine prioritaire pour la politique publique nationale et la coopération internationale ».

### L'action de la France

Ces recommandations trouvent une traduction concrète en France à partir de 2008, *via* le Livre blanc sur la défense et la sécurité nationale. La menace contre la nation liée aux cyberattaques

y figure pour la première fois parmi les menaces stratégiques, en troisième position en raison de sa probabilité élevée de survenue et de l'impact majeur qu'elle est susceptible d'avoir. Cette orientation amène la France à créer l'Agence nationale de la Sécurité des Systèmes d'Information (ANSSI) dès 2009. Celle-ci commence rapidement à travailler avec des opérateurs publics et privés d'infrastructures critiques, en développant un modèle de coopération public-privé aujourd'hui encore envié à l'étranger. Mais il faut attendre 2011 et l'article L33-10 du Code des postes et communications électroniques pour que les opérateurs de communication électronique soient les premières infrastructures critiques en France à voir leur cybersécurité régulée. Et ce n'est pas avant 2013 qu'apparaît une orientation explicite sur la cybersécurité de l'ensemble des infrastructures critiques pour la défense et la sécurité nationale.

Le Livre blanc sur la défense et la sécurité nationale de 2013 comporte un chapitre sur « la lutte contre la cybermenace », qui prévoit : « S'agissant des activités d'importance vitale pour le fonctionnement normal de la Nation, l'État fixera, par un dispositif législatif et réglementaire approprié, les standards de sécurité à respecter à l'égard de la menace informatique et veillera à ce que les opérateurs prennent les mesures nécessaires pour détecter et traiter tout incident informatique touchant leurs systèmes sensibles. Ce dispositif précisera les droits et les devoirs des acteurs publics et privés, notamment en matière d'audits, de cartographie de leurs systèmes d'information, de notification des incidents et de capacité pour l'Agence nationale de la Sécurité des Systèmes d'Information (ANSSI), et, le cas échéant, d'autres services de l'État, d'intervenir en cas de crise grave. » Ce sont ainsi plus de 250 Opérateurs d'Importance vitale (OIV), publics et privés, dont la liste est classifiée, qui devront désormais respecter des exigences de cybersécurité en plus des exigences de sécurité physique déjà applicables.

Cette orientation du Livre blanc sur la défense et la sécurité nationale se concrétise par l'article 22 de la loi de programmation militaire (LPM) du 18 décembre 2013, qui crée les articles L1332-6-1 à L1332-6-6 du Code la défense. L'ANSSI se voit attribuer la capacité de fixer les exigences de sécurité pesant sur les systèmes d'informations dits « d'importance vitale » (SIIV) ainsi que de réaliser ou faire réaliser des contrôles sur ces systèmes. Les OIV doivent aussi déclarer à l'ANSSI les incidents affectant leurs SIIV. Ce cadre prévoit par ailleurs la capacité pour l'ANSSI de qualifier des prestataires pour réaliser certains types de prestations requises par la réglementation (notamment audits et détection d'incidents de sécurité). Enfin, chaque manquement aux exigences de ce cadre réglementaire peut être sanctionné pénalement par une amende de 150 000 euros.

Même si l'ANSSI est positionnée comme régulateur trans-sectoriel en matière de cybersécurité, il est évident que cette autorité ne saurait être exclusive de l'autorité que les ministères et les régulateurs sectoriels peuvent avoir sur leurs OIV. Il est donc attendu que l'ANSSI, les ministères de tutelle des OIV et les régulateurs sectoriels se coordonnent afin d'assurer une articulation efficace entre les politiques publiques dont ils sont responsables.

Alors que la France avait accumulé un retard de près d'une décennie par rapport aux pays les plus avancés dans la prise en compte du besoin de cybersécurité pour ses infrastructures critiques, ce cadre réglementaire en a fait un pays précurseur en la matière.

## La mise en œuvre des dispositions légales

### La finalisation du cadre réglementaire

Vu l'impact potentiel de cette réglementation nouvelle et le besoin d'acceptabilité de la part des OIV, l'ANSSI a opté pour une co-construction des textes d'application avec les opérateurs concernés. L'année 2014 a ainsi été utilisée pour conduire des expérimentations avec quelques OIV. Les années suivantes ont été consacrées à la conduite de groupes de travail sectoriels afin de définir les règles applicables aux OIV, en tenant compte des spécificités sectorielles. À l'issue de

plus de 200 réunions de travail, les arrêtés sectoriels ont ainsi été produits pour chacun des secteurs d'activité d'importance vitale. Tous comportent vingt règles de sécurité informatique autour des thématiques suivantes : gouvernance, gestion des risques, protection, détection, réaction et gestion de crise. Ces règles correspondent à des bonnes pratiques et ont chacune des délais propres pour la mise en conformité des OIV.

Les arrêtés sectoriels résultant de ce processus sont entrés en vigueur par vagues :

- 1er juillet 2016 : alimentation, gestion de l'eau, produits de santé ;
- 1er octobre 2016 : transports et énergie (hors nucléaire) ;
- 1er janvier 2017 : finances, audiovisuel, communications électroniques et Internet, industrie ;
- 1er avril 2017 : nucléaire civil ;
- 1er octobre 2017 : activités industrielles de l'armement, espace ;
- 1er octobre 2019 : activités civiles de l'État.

## La définition d'un plan de réponse aux crises majeures cyber

L'article 22 de la LPM prévoit des dispositions relatives à la gestion de crise : « Pour répondre aux crises majeures menaçant ou affectant la sécurité des systèmes d'information, le Premier ministre peut décider des mesures que les opérateurs mentionnés aux articles L.1332-1 et L.1332-2 doivent mettre en œuvre. »

L'État s'est doté d'un plan de gestion des crises d'origine cyber, PIRANET, pour se préparer à un scénario où des OIV seraient atteints afin de produire un effet incapacitant sur la Nation. En complément, des exercices sont régulièrement organisés afin de tester le niveau de préparation des différentes parties prenantes, notamment les services de l'État et les OIV : CyberEurope au niveau européen, PIRANET au niveau national, ou encore des exercices sectoriels à l'initiative de régulateurs sectoriels ou des opérateurs eux-mêmes. L'ANSSI apporte plusieurs fois par an, outre sa participation, son expertise en matière de planification et d'organisation d'exercices en soutien à l'organisation de tels exercices.

## La mise en conformité des OIV

Le travail de sensibilisation et d'assistance de l'ANSSI auprès de certains OIV avait déjà bien démarré au moment de l'adoption de la LPM de 2013, notamment auprès des OIV victimes de cyberattaques. Un certain nombre de systèmes d'information voués à être déclarés SIIV étaient donc déjà sécurisés de manière appropriée avant la publication des arrêtés sectoriels les concernant.

Formellement, la publication de chaque arrêté sectoriel appelle la déclaration sous trois mois à l'ANSSI de la liste des SIIV de chaque OIV du secteur. Fin 2018, plus de 1500 SIIV avaient été déclarés à l'ANSSI, preuve d'une approche volontaire de la vaste majorité des OIV. Aujourd'hui, aucun manquement n'a encore justifié d'amende.

Autre signe de dynamisme dans la mise en conformité des SIIV aux exigences réglementaires : la saturation des carnets de commande des prestataires qualifiés en matière d'assistance à la sécurisation des SIIV.

La principale mesure restant en suspens jusqu'à récemment était la règle exigeant le recours à des systèmes de détection qualifiés par l'ANSSI, en raison de l'absence d'une offre suffisante. Ce point a été levé en avril 2019 avec la qualification des sondes de Thales et Gatewatcher.

## La qualification des prestataires

Vu l'ampleur du chantier de la sécurisation de l'ensemble des SIIV, la loi a d'emblée prévu la possibilité pour l'ANSSI de déléguer des activités à des prestataires privés. Dans le cadre des Visas de sécurité de l'ANSSI, on retrouve deux catégories :

- Les prestataires d'audit en sécurité des systèmes d'information (PASSI), qui réalisent des audits obligatoires préalablement à l'homologation des SIIV, peuvent offrir des services de conseil en sécurisation des SIIV, et peuvent assurer des contrôles par délégation de l'ANSSI ;
- Les prestataires de détection d'incidents de sécurité (PDIS), qui opèrent les systèmes de détection qualifiés exigés par la réglementation.

Ces prestataires jouent un rôle-clé dans la mise en œuvre de la réglementation française sur la cybersécurité des OIV. De plus, la création de ces catégories a permis de structurer le marché. En septembre 2019, on peut compter 13 PASSI qualifiés et 4 PDIS qualifiés.

## Une approche ambitieuse de la cybersécurité des infrastructures critiques

### La directive européenne pour la cybersécurité des opérateurs de services essentiels

S'inspirant de la démarche française, l'Union européenne a entamé en 2013 des travaux en vue d'adopter une directive de même nature. La négociation s'est conclue par l'adoption et l'entrée en vigueur le 6 juillet 2016 de la directive 2016/1148 (dite « directive NIS »). La directive appelle à se doter d'une stratégie de cybersécurité, d'une autorité nationale compétente en la matière, et de capacités techniques ayant vocation à fonctionner en réseau. Elle impose également la mise en place d'un cadre très similaire dans sa structure à celui existant en France pour la cybersécurité des OIV. La France a ainsi su préserver et promouvoir son approche durant les négociations. Pour autant, la directive s'appuie sur une base juridique relative au bon fonctionnement du marché intérieur. La défense et la sécurité nationale constituent une prérogative exclusive des États membres. Les opérateurs régulés au titre de la directive sont donc qualifiés d'opérateurs de services essentiels (OSE) à l'économie ou à la société, relativement à l'impact disruptif que pourrait avoir un dysfonctionnement d'un de leurs systèmes d'information dits « essentiels » (SIE).

La vaste majorité des États membres ont choisi d'utiliser la loi de transposition pour couvrir de manière indiscriminée les champs relatifs au bon fonctionnement de l'économie et de la société d'une part, et de la défense et la sécurité nationale d'autre part. La France a quant à elle choisi de dupliquer le dispositif existant dans le Code de la défense, pour produire un cadre sur une base juridique distincte, couvrant des activités complémentaires de celles couvertes par la LPM.

Par ailleurs, la France a fait le choix d'une transposition très ambitieuse. Elle ne s'est pas restreinte à la liste minimale de services essentiels figurant en annexe de la directive NIS, mais a ajouté de nouveaux secteurs.

À ce jour, la désignation des OSE est en cours d'instruction en France.

### Approche française du droit international autour des infrastructures critiques

En s'appuyant sur son expérience, la France a entrepris deux actions visant à soutenir la sécurité internationale et à éviter des déstabilisations du cyberespace liées à des actes inappropriés.

La première action a consisté en la promotion en 2015, au sein du groupe d'experts gouvernementaux des Nations Unies, du principe de diligence requise cyber *(cyber due diligence)*. Ce principe, acté dans la résolution 70/174, prévoit que : « Les États devraient répondre aux demandes d'aide appropriées formulées par un autre État dont une infrastructure essentielle est exposée à des actes de malveillance informatique ; ils devraient aussi répondre aux demandes appropriées visant à atténuer les conséquences d'activités informatiques malveillantes dirigées contre une infrastructure essentielle d'un autre État et exercées depuis leur territoire, en tenant

dûment compte de la souveraineté. » Cette approche conforte le principe de souveraineté des États dans le cyberespace, appelant prioritairement à la coopération. Elle délégitime de fait une intervention de l'État victime chez des États involontairement impliqués, pourvu que ceux-ci répondent de manière efficace aux demandes de coopération de l'État victime.

La seconde action de la France a consisté à se doter, en 2018, à l'occasion de la publication de la « Revue stratégique de cyberdéfense », d'une échelle de classement de la gravité des incidents cyber en fonction de leurs conséquences « dans le monde réel ». L'objectif est de donner les clés aux autorités politiques pour appréhender le niveau de gravité des attaques, et d'ajuster la nature de la réponse à la crise. Cette approche, inspirée de travaux anglo-saxons, constitue désormais la clé de voûte de la politique française de réponse aux cyberattaques. Elle est promue au sein de l'Organisation pour la sécurité et la coopération en Europe (OSCE) et est discutée dans les travaux des Nations Unies.

## Conclusion

Les dispositifs réglementaires français en matière de cybersécurité permettent d'appréhender largement la cybersécurité des infrastructures critiques, et ont fait de la France une pionnière en la matière.

Malgré une approche ambitieuse, certains systèmes critiques ne sont pas encore couverts par ces réglementations, tels que les dispositifs médicaux, les véhicules autonomes, les machines à voter et le vote électronique. La prise en compte de la cybersécurité dans ces systèmes nécessite aujourd'hui une forte coopération avec les autorités sectorielles. L'objectif sera qu'elles intègrent des exigences de cybersécurité, conformément à l'approche promue par la « Revue stratégique de cyberdéfense » de 2018.