Répondre à la menace cyber par la régulation

Synthèse de conférence

Conférence organisée par la Chaire Gouvernance et Régulation en coopération avec le Conseil Général de l'Economie

Université Paris-Dauphine, 5 décembre 2019

DEBATE

Dauphine | PSL

CHAIRE GOUVERNANCE ET RÉGULATION

Conférence organisée par la Chaire Gouvernance et Régulation
en coopération avec le Conseil Général de l'Economie

CONSEIL GÉNÉRAL DE L'ÉCONOMIE
DE L'INDUSTRIE, DE L'ÉNERGIE ET DES TECHNOLOGIES

Table des matières

Répondre à la menace cyber par la régulation

Conférence de la Chaire Gouvernance & Régulation et du Conseil Général de l'Economie
5 décembre 2019

Si les risques d'atteinte à la confidentialité, l'intégrité, l'authenticité et la disponibilité des données ne sont pas nouveaux, la transformation numérique leur confère une nouvelle dimension et rend les différentes composantes de nos sociétés de plus en plus vulnérables. Qui plus est, les systèmes d'information et de communication deviennent à la fois les moyens et les cibles des cyberattaques.

Pour relever les nombreux défis de la menace cyber, comment articuler les initiatives d'autorégulation de la part des utilisateurs ou des acteurs du numérique, les efforts de régulation nationale et la coopération internationale ?

1ère table ronde : la menace cyber et la régulation nationale

Président de session : Côme Berbain | RATP

Les infrastructures critiques

Yves Verhoeven
Agence nationale de la sécurité des systèmes d'information (ANSSI)

La France s'est pleinement mobilisée sur le sujet *cyber* dès 2009, en créant l'ANSSI dans la foulée de la publication du Livre blanc sur la défense et la sécurité nationales qui faisait figurer le risque de survenue d'un indicent *cyber* majeur parmi les trois plus grands.

En effet, l'espace numérique est à la fois un espace de développement économique et sociétal, mais aussi un espace de conflits entre États et d'opportunité pour les *cyber*criminels. L'action de l'État s'inscrit dans ce cadre, de même que l'Appel de Paris prononcé en novembre 2018 par le Président de la République et qui engage la France dans la stabilité du *cyber*espace, afin de tirer les pleins bénéfices de la transformation numérique.

Chaque État doit prendre ses responsabilités, à commencer par assurer la *cyber*sécurité de ses infrastructures critiques, puis en préparant sa gestion de crise. D'autant que le phénomène de *cyber*attaque n'épargne aucune organisation.

L'état de la menace

L'ANSSI distingue cinq grandes catégories de menaces : l'espionnage ; les opérations de déstabilisation et d'influence ; les attaques de la Supply Chain pour toucher les sous-traitants des grandes entreprises ; le pré-positionnement, qui se traduit par des *cyber*attaques contre des réseaux d'infrastructures critiques qui ne contiennent pas d'informations sensibles, dans le but de les cartographier en vue de préparer de futurs conflits ; la *cyber* criminalité, notamment via des rançongiciels profitant du développement des crypto-monnaies.

Durant des années, le risque *cyber* était appréhendé comme un sujet d'experts. C'est pourtant un risque comme les autres qui doit, à ce titre relever du *risk management*. L'ANSSI et l'Association pour le management des risques et des assurances de l'entreprise (AMRAE) ont d'ailleurs publié, en novembre dernier, un guide conjoint sur la maîtrise du risque numérique.

Les infrastructures critiques

Ce sujet a émergé à l'Onu dès la fin des années 1990 et l'OCDE a publié ses lignes directrices en la matière en 2008. C'est également à cette époque que la France a rédigé son Livre blanc sur la défense et à la sécurité nationales. Pour autant, ce n'est qu'à compter de 2011, avec la transposition du Paquet télécom, que l'État a commencé à confier à l'ANSSI des pouvoirs formels de régulateur en dehors de la sphère publique. Depuis la loi de programmation militaire de 2013, c'est le régulateur de tous les opérateurs d'importance vitale, publics et privés. Au nombre de 250, ils sont considérés comme des

opérateurs prioritaires chez lesquels une attaque *cyber* majeure ne saurait être tolérée. Cette législation a fait de la France un pionnier dans le domaine. La directive NIS de 2016 sur la sécurité des réseaux et des systèmes d'information s'est ensuite calquée sur le cadre français, même si elle s'applique à un champ différent – les opérateurs de services essentiels à l'économie et à la société – puisque l'Union européenne n'est pas compétente en matière de sécurité et de défense nationales.

Cette directive a été transposée en droit français de manière à étendre le champ de réglementation de l'ANSSI à la sphère économique et sociétale. Les opérateurs sont appelés à identifier les systèmes d'information qui soutiennent leur activité critique, pour lesquels ils se voient imposer des règles de *cyber* sécurité. Ils doivent par ailleurs déclarer à l'ANSSI tout incident significatif sur un de ces systèmes. L'ANSSI peut aussi réaliser des contrôles *in situ* ou les déléguer à des auditeurs du secteur privé. Le dernier volet de la réglementation concerne la gestion de crise et permet à l'ANSSI, face à des *cyber*attaques significatives, de donner des ordres aux opérateurs au nom du Premier ministre.

Une régulation spécifique

L'ANSSI impose et contrôle, mais elle intervient aussi en soutien. Elle a ainsi été impliquée pour soutenir Enedis dans la sécurisation du dispositif Linky. Elle est également en mesure d'intervenir sur le terrain, comme elle l'a fait lors de la *cyber*attaque de TV5 Monde qui mettait en jeu l'image de la France.

Par ailleurs, l'ANSSI est un régulateur transverse, dans la mesure où le risque *cyber* traverse toutes les verticales métier des infrastructures critiques. Cela lui impose de porter une politique et une réglementation en articulation avec les régulateurs sectoriels. Cette démarche est lourde et sophistiquée, mais nécessaire à la crédibilité de l'action publique.

Enfin, la dimension internationale est prégnante. En effet, le *cyber*espace s'abolit des distances. Ainsi, un opérateur critique pour la France peut l'être pour les pays limitrophes voire l'ensemble de l'Union européenne.

Le secteur privé et la cyberdéfense

Nicolas Arpagian
Orange Cyberdefense

Même si l'activité de Défense est traditionnellement associée au monde militaire, le secteur civil est lui aussi, désormais, visé par des *cyber*attaques. Il faut donc que les entreprises s'imprègnent de l'approche de *cyber*défense et de *cyber*sécurité.

L'effet structurant de la réglementation

Le secteur privé est poussé par la réglementation (loi de programmation militaire de 2013, RGPD, directive NIS…), qui impose un cahier des charges, un agenda, un régime de responsabilité et de contrôle ainsi qu'un barème de sanctions. Les entreprises doivent notamment dégager des marges budgétaires pour investir dans leur sécurité et permettre la continuité de leur activité. Dans un premier temps, la plupart des entreprises ont appliqué ces textes dans une logique stricte de mise en conformité, sans réelle appropriation des enjeux, allant souvent jusqu'à considérer que les investissements qui leur étaient imposés en matière de *cyber*sécurité altéraient leur modèle économique et leur profitabilité. La régulation était donc vécue comme une contrainte.

Aujourd'hui encore, l'état de *cyber*sécurité n'est pas encore appréhendé comme un argument différenciateur. Aucune entreprise ne communique sur le fait que tel de ses objets connectés est vendu plus cher au motif qu'il est protégé et qu'il protège contre les *cyber*attaques, car les clients ne sont formellement pas demandeurs de ces éléments de sécurité. Le secteur privé reste donc mal à l'aise vis-à-vis de cette régulation qu'il ne peut pas traduire dans son offre commerciale comme un élément de valorisation. Cette tendance évoluera, comme pour les exigences environnementales et sociales, avec l'évolution des mentalités.

La pression des marchés financiers

Par ailleurs, le secteur privé voit émerger une régulation par les acteurs des marchés financiers. Dans le cadre du RGPD par exemple, les entreprises peuvent encourir des amendes allant jusqu'à 4 % de leur chiffre d'affaires mondialisé. Ces sommes doivent donc être provisionnées. Les marchés financiers – notamment les agences de notation - demandent des gages de durabilité de l'entreprise face à des *cyber*attaques au travers de ratios comptables. Au point que les sociétés dont le niveau de sécurité ne serait pas jugé satisfaisant verraient leur note dégradée avec un effet sur leur valorisation boursière. Cette pression s'exerce bien au-delà du domaine réglementé et de la communauté des opérateurs d'importance vitale ou de services essentiels. Des législations financières mettent désormais en cause la responsabilité des entreprises en cas de défaillance à la suite d'une *cyber*attaque.

Une redéfinition de la notion de concurrence

Dans ce contexte de menaces exacerbées, les acteurs outrepassent les règles habituelles de la compétition économique pour partager, alors qu'ils sont concurrents, des informations au nom de l'intérêt supérieur de la sécurité collective. Cela se déroule au

sein de Computer Emergency Response Teams (CERTs) à l'échelle internationale et dans les secteurs publics et privés.

En outre, l'exigence croissante de transparence a donné lieu à une communication accrue. En mars 2019, par exemple, alors qu'il subissait une *cyber*attaque, le deuxième producteur norvégien d'énergie a fait appel à une équipe de journalistes chargée de filmer la direction en situation réelle de crise. Les dirigeants témoignaient publiquement dans les jours qui ont suivi le début de la crise. Une stratégie de transparence qui a été très appréciée par les observateurs.

Dans le même ordre d'idée, la création du campus *Cyber*, auquel travaille Orange à l'initiative du Président de la République et du Premier ministre, vise à réunir dans un même lieu des acteurs frontalement concurrents commercialement pour répondre à une menace. Face à des périls protéiformes il faut envisager de nouvelles formes de coopération qui mêlent la technologie, l'économie, les ressources humaines et les intérêts stratégiques nationaux.

Une responsabilité en continu

La chaîne économique se caractérise désormais par une responsabilité en continu, ce qui conduit à écarter certains sous-traitants. Les grands donneurs d'ordre ne voulant pas être fragilisés ou voir leur responsabilité mise en cause en cas de défaillance d'un sous-traitant. La véritable régulation est donc effectuée par les donneurs d'ordre, qui effectuent nécessairement un tri dans leurs fournisseurs, par exemple au regard de leur conformité au Règlement Général sur la Protection des Données (RGPD).

Le point de vue du consommateur

Le consommateur lui-même tend à devenir un élément structurant de la régulation. Certes, les scandales relatifs à l'usage des données par Facebook, par exemple, n'ont pas encore d'impact tangible sur la fréquentation de ce réseau social. Mais des mouvements de coalition des consommateurs pourraient commencer à façonner certaines décisions d'entreprise – retrait de certaines activités ou, au contraire, explication de certaines pratiques.

Régulation future et responsabilité des acteurs systémiques

Florian Escudié
Ministère de l'Europe et des Affaires étrangères

Une diplomatie du numérique incluant un volet *cyber* se développe depuis plusieurs années, visant plusieurs objectifs : préserver Internet comme un espace ouvert, libre, stable et sécurisé ; protéger les intérêts de sécurité nationale dans un contexte où le numérique fournit à la fois un espace de confrontation stratégique entre Etats et des « armes » dont l'usage par certains acteurs est déstabilisateur.

Le paysage sécuritaire

Tout en s'accroissant, le risque *cyber* s'est diversifié : les moyens *cyber* sont utilisés à des fins d'espionnage, de sabotage, de déstabilisation, etc.... Il existe aussi un continuum entre la *cyber* criminalité, activité privée par nature, et les enjeux de sécurité nationale. Certaines attaques prennent ainsi l'apparence d'actions crapuleuses, avec l'usage de *phishing* ou de rançongiciels par exemple, alors qu'elles poursuivent en fait des objectifs politiques. La surface d'attaque s'est, elle aussi, significativement étendue avec la numérisation de nos sociétés. Par défaut d'hygiène *cyber* et de résilience, de nombreux points de vulnérabilité demeurent – dans notre société et *a fortiori* dans celles qui n'ont pas encore développé de culture de *cyber*séurité. Or les frontières étant abolies dans l'espace numérique, le risque qui existe chez nos voisins peut s'étendre chez nous. La généralisation de la 5G et de l'Internet des objets ne fera qu'accroître les vulnérabilités potentielles.

Les Etats et les entreprises ne sont pas seuls concernés. Le citoyen, par essence vulnérable attend une protection de la part de l'État, dans la vie *cyber* de la même façon que dans la vie physique. C'est le cas, par exemple, avec le développement du vote électronique, qui conduit le citoyen a exiger une protection de l'intégrité de son vote contre les tentatives d'ingérence dans les processus électoraux.

La *cyber* diplomatie

Le diplomate a deux moyens d'action : la prévention des crises par la régulation ; la gestion l'organisation de la réponse de l'État et la gestion de crise. Il en va de même pour le *cyber*-diplomate. On s'intéresse ici au premier volet.

Historiquement, la régulation du *cyber* espace a d'abord été l'affaire des États. Cela a longtemps conduit à laisser de côté les acteurs privés, à la fois en tant qu'acteurs et objets de la régulation. Les grandes entreprises étaient alors plutôt dans un rôle de protection de leurs clients. Aujourd'hui, elles ont à rendre des comptes et doivent être régulées dans trois domaines en particulier : la vente d'outils informatiques pouvant être utilisés à des fins d'attaque, notamment d'intrusion dans des systèmes informatiques tiers ; le mercenariat, ou la vente de services à d'autres entreprises cherchant à se prémunir ou à se venger d'attaques au mépris du monopole de la violence légitime reconnu à la puissance étatique ; la sécurité des produits proposés dans le *cyber* espace, lesquels doivent être transparents, sécurisés, empêcher la divulgation des failles de sécurité et appliquer le principe de la sécurité par défaut. Ce dernier point trouve en particulier à s'appliquer pour les fournisseurs dont la part de marché les rend, *de facto*, incontournables, voire systémiques.

Si plusieurs développements positifs sont à noter, notamment sous l'impulsion de la France, comme l'Appel de Paris de novembre 2018 ou la mise en place de groupes de travail au sein de l'OCDE, un long chemin reste à parcourir pour renforcer la régulation dans ce domaine. Des différentes d'approche demeurent entre les pays, ne serait-ce qu'au regard de la place de la règle de droit dans l'organisation de la régulation ou encore des degrés différents de sensibilités en matière de protection des données personnelles. Pour sa part, la France considère qu'il existe une voie médiane de la régulation, entre l'approche libertarienne californienne et la vision autoritaire chinoise. En tout état de cause, la régulation ne saurait être déléguée à des producteurs de normes privés qui imposeraient leurs propres règles à tout le marché. En tant que puissance normative, l'Union européenne a un rôle éminent à jouer à cet égard, comme elle l'a démontré avec le RGPD.

La cyber criminalité boursière

Alexandre Neyret
Autorité des marchés financiers (AMF)

La *cyber* criminalité boursière est un phénomène ancien, auquel l'ensemble du secteur financier est confronté du fait de sa forte automatisation,de sa concentration et bien sûr de l'argent y circulant. Le risque *cyber* est même systématiquement classé au premier rang par quasiment toutes les institutions.

Si les stratégies de criminalité n'ont pas fondamentalement changé au cours des âges, la conjonction avec la digitalisation multiplie les cibles et les moyens, donc les attaques.

Éléments de définition

La *cyber* criminalité financière est très variée, avec des attaques d'envergure – contre les intermédiaires de la chaîne de paiement, contre les bourses, contre les établissements financiers ou contre les plateformes d'échange de cryptoactifs (1,5 milliard de dollars de gains subtilisés en cinq ans), mais aussi sous la forme de fraudes aux investissements en ligne. L'AMF évalue d'ailleurs ce dernier préjudice à 1 milliard de dollars au cours des deux dernières années.

Quant au sous-ensemble de la (*cyber*) criminalité boursière, il s'articule autour de trois manquements principaux :

- le délit d'initié : l'étude des cas réels montre que toute la chaîne des acteurs financiers (émetteur, avocats, diffuseurs spécialisés, régulateurs, etc…) peut être touchée par la subtilisation d'informations privilégiées. Certaines attaques sont le fait de groupes organisés et sophistiqués puisque spécialisés à la fois dans le piratage informatique et dans la finance. Les méthodes sont souvent fondées sur l'hameçonnage ciblé, et le maillon faible humain. Pour le futur, il importe de s'intéresser à plusieurs pistes : le *darkweb* pour monétiser ou obtenir les informations privilégiées, les fuites de données personnelles qui pourraient constituer la base de futurs hameçonnages ciblés , les indices et les indicateurs économiques sensibles (la sécurisation de la production des chiffres du chômage, par exemple) qui constituent des cibles potentielles et la sécurisation de tous les nouveaux points d'entrée comme l'internet connecté, *le cloud*, le nomadisme, la Supply Chain, etc ;

- la manipulation de cours : elle peut-être aussi le fait de groupes organisés et capables d'intrusion dans des applications professionnelles (dans le cas Energobank en 2015, la *cyber*attaque a fait varier la parité dollar/rouble de 15 % en quelques minutes), le cas échéant couplée avec le vol d'informations personnelles à grande échelle, mais aussi de diffusion et de manipulation (cas SHALON). La plupart des manipulations restent néanmoins dues à des intrusions de comptes de particuliers pour mettre en place des stratégies de type « pump&dump ». Les perspectives concernent la sécurisation des applications de *trading* mobiles ou fixes, mais aussi la compromission des algorithmes de *trading* ;

- la diffusion de fausses informations : le cas le plus emblématique est celui de Vinci, dont le cours avait dévissé de près de 19 % en quelques minutes en 2016. Ces attaques

se caractérisent par un faible niveau de sophistication, des motivations principalement activistes avec des variations de capitalisation importantes pour les émetteurs et un anonymat facile dû à l'Internet. Elles utilisent largement les réseaux sociaux. Les réflexions pour le futur portent sur la sécurisation du chemin de l'information financière de l'amont à l'aval, le niveau de sécurité des diffuseurs dits spécialisés et non régulés par l'AMF, l'intelligence artificielle (*deep fake*) et l'intégrité des données (*fake news* vs *fake data*).

Les actions de l'AMF

L'AMF participe à de nombreux groupes de travail internationaux et européens. En France, elle s'inscrit dans une démarche de coopération et de partage de compétences sur la sphère financière avec l'ACPR et l'ANSSI. Elle conduit aussi des actions de sensibilisation des acteurs régulés ou non. Par ailleurs, la loi Pacte lui a conféré de nouveaux pouvoirs de contrôle des prestataires de services numériques. L'AMF contrôle également le niveau de *cyber* sécurité de certains acteurs régulés (sociétés de gestion de portefeuille).

En interne, l'AMF assure une veille active sur toutes les nouvelles formes de technologies et sur la *cyber* criminalité boursière. Elle sensibilise et forme ses collaborateurs au sujet *cyber*, y compris à sa propre *cyber* sécurité.

Au-delà de la menace cyber, réguler la confiance dans le numérique ?

Côme Berbain
RATP

Le texte le plus important de la décennie en matière *cyber* est le RGPD, qui porte une définition très extensive de la notion de données personnelles. C'est un levier d'amélioration très puissant de protection, du fait du montant des sanctions envisagées. Plusieurs acteurs, y compris américains, ont d'ailleurs commencé à changer de comportement. Apple, par exemple, fait désormais une communication agressive sur la protection des données de ses clients.

La sécurité des algorithmes

Ce sujet n'est pas encore vraiment traité. Lorsqu'un algorithme ne comprend pas certaines entrées, il adopte un comportement aberrant. Or les possibilités d'altération délibérée, sans qu'il s'agisse à proprement parler de *cyber*attaque, sont multiples, en témoigne l'inventivité des manifestants hongkongais pour échapper aux systèmes de reconnaissance faciale. Pour les véhicules autonomes, par exemple, l'enjeu *cyber* est de taille. En effet, il convient d'empêcher quiconque d'en prendre le contrôle. Mais l'altération peut aussi se faire en plaçant un piéton de part et d'autre du véhicule, ce qui entraîne son arrêt immédiat : il est donc possible de paralyser le système sans lui porter atteinte, en piratant l'algorithme sans toucher à son exécution.

Dans ce domaine, la régulation et la gouvernance sont encore émergentes. Une première étape est l'explicabilité des algorithmes dans la sphère publique – par exemple celui de Parcoursup.

La sécurité des informations

Face à la diffusion croissante de fausses informations, il existe un embryon de régulation dans le cas extrêmement précis des périodes électorales. Les réseaux sociaux commencent eux aussi à adapter leurs algorithmes et leur politique interne. L'objectif consiste à générer de la confiance dans l'information diffusée et à lutter contre ceux qui cherchent à la saper volontairement.

Perspectives

Désormais, les attaquants jouent sur plusieurs niveaux simultanément. Une attaque *cyber* peut ainsi viser à extraire des informations personnelles pour les tronquer et les rediffuser sous la forme de fausses informations sur les réseaux sociaux. Or ces niveaux sont régulés de manière complètement différente. Cela pose le défi collectif de la gestion et de l'interaction des réglementations, à l'échelle nationale mais aussi internationale avec la montée en puissance des conflits d'extraterritorialité du droit.

La confiance réside dans la cohérence des actions à chacun des niveaux, laquelle requiert des capacités opérationnelles et des moyens adaptés. De nouvelles méthodes de démonstration de la confiance commencent à apparaître : bug bounty ; open data ; publication des politiques internes de gestion des données ; explicabilité des algorithmes ; non-discrimination des petits acteurs sur les plateformes de e-commerce ; cohérence, crédibilité et transparence de la communication et de l'information.

Échanges avec la salle

De la salle

L'Arcep allemande impose, y compris aux plus petits opérateurs, d'avoir un plan de cyber sécurité et de nommer un responsable de la cyber sécurité. Pourquoi cela n'existe-t-il pas en France ?

Yves Verhoeven

Cantonner l'action de l'ANSSI à la réglementation serait très réducteur. Nous percevons avant tout notre action comme la modulation des écosystèmes, dans une approche structurelle visant à faire évoluer les équilibres de marché. Dans cette optique, les sanctions ne sont pas prioritaires. Elles constituent avant tout des menaces vis-à-vis des opérateurs de mauvaise volonté. La première sanction que nous aurons à prononcer sera d'ailleurs, pour nous, une forme d'échec.

Par ailleurs, nous avons créé à destination des entreprises, des collectivités locales et du grand public la plateforme GIP cybermalveillance.gouv.fr, qui apporte des réponses concrètes en cas de *cyber*attaque. Nous faisons également en sorte de convaincre les acheteurs qu'ils peuvent et doivent même imposer du *cyber* dans les produits. C'est ainsi que le marché des offreurs se reconfigurera, pour atteindre le niveau de sécurité attendu par les utilisateurs.

En somme, nous considérons que la régulation doit se faire par la modification des équilibres structurels plus que par la réglementation, qui n'intervient qu'en dernier recours.

De la salle

Que pensez-vous de la proposition de la chancelière allemande de créer une agence européenne de certification en matière de cyber sécurité ?

Yves Verhoeven

Le législateur français a considéré que l'approche qui consistait à se focaliser sur la sécurité intrinsèque des produits était réductrice. C'est la raison pour laquelle il a défini un cadre réglementaire avec différents critères de sécurité, qui ne sont pas seulement techniques mais portent aussi sur les conditions de déploiement et de téléopération, l'architecture du réseau, etc.

De la salle

N'est-il pas de temps de définir une véritable politique européenne de défense ?

Yves Verhoeven

En 2004, la France n'était pas favorable à la création de l'Agence européenne chargée de la sécurité des réseaux et de l'information (Enisa) dans la mesure où elle envisageait le *cyber* sous un angle essentiellement régalien. Depuis, sa vision a évolué pour considérer que le

sujet est biface, avec la défense et la sécurité nationales d'un côté et la transformation numérique de l'économie et de la société de l'autre. Or sur ce deuxième volet, l'approche nationale est strictement insuffisante et la bonne échelle est européenne. Aussi la France s'investit-elle pleinement pour promouvoir une *cyber* sécurité européenne et renforcer l'Union européenne en la matière.

Nicolas Arpagian

Faire monter l'expertise en *cyber*sécurité au niveau européen pourrait mutualiser les expertises sur une plus grande échelle par rapport aux autres grands ensemble : Russie, Chine, Etats-Unis… Mais la famille européenne reste souvent divisée lorsqu'il s'agit de définir contre qui se protéger – des criminels ou des intérêts étatiques. De fait, la fiscalité, l'économie ou l'emploi demeurent des intérêts nationaux. Une mutualisation sera organisée pour traiter des questions de sécurité. Mais le *cyber* touche aussi à l'autonomie de la prise de décision du pouvoir politique et à la capacité à assurer la durabilité des modèles économiques, qui s'apprécient nationalement. Cette dualité est très difficile à manier et demande de nouvelles formes d'alliances.

En somme, les États défendent leurs intérêts stratégiques tout en essayant de communautariser certains enjeux, étant entendu que les ressources financières et humaines demeurent limitées.

Florian Escudié

Le rôle d'évaluation par les pairs aux organisations internationales, n'est pas contradictoire avec les principes de souveraineté et de pleine responsabilisation des États dans l'application des règles de sécurité. L'Otan, par exemple, incite chacun des Alliés à renforcer la résilience de ses infrastructures de défense. Cette responsabilité nationale est donc mise en œuvre sous le regard des autres.

Par ailleurs, le rapport de la Commission européenne de mars dernier sur la 5G invite les États membres à mettre en place des audits de sécurité. Cette injonction devrait contribuer à renforcer la culture de sécurité, encore largement inexistante chez certains de nos partenaires.

De la salle

L'insouciance totale du grand public en la matière est très frappante. Comment les industriels se préoccupent-ils de la cyber sécurité, dans ce contexte ?

Côme Berbain

L'un des acteurs envers lequel le grand public a le plus confiance est Google, considérant qu'il offre un service exceptionnel et transparent – certes en échange des données de ses utilisateurs, ce qu'il sait leur imposer tout en leur laissant penser qu'ils l'acceptent. Pour les grands projets étatiques de type Linky, en revanche, la confiance n'est pas au rendez-vous. Un travail technique très complexe a pourtant été accompli, mais la communication a sans doute été insuffisante.

2ème table ronde: menace et cyber coopération internationale

Président de session : Éric Brousseau | Université Paris-Dauphine

Pour une régulation mondiale du cyber-espace

Jean-Claude Laroche
Enedis & Cigref

La sécurisation des activités et des systèmes d'information des grandes entreprises est un enjeu majeur, auquel il convient de répondre dans un contexte anxiogène.

Un climat d'insécurité

Le niveau de la menace ne cesse de croître. Le contexte n'est d'ailleurs pas seulement lourd de menaces, il est aussi marqué par des attaques réussies avec des conséquences très significatives sur l'activité des entreprises concernées. Qui plus est, la liste des vulnérabilités publiée par les éditeurs de solutions sur lesquels s'appuient les grandes entreprises s'allonge constamment. Ces vulnérabilités, y compris les plus critiques, sont même tellement nombreuses qu'il est de plus en plus difficile de s'en prémunir.

Une nécessaire régulation

Il n'est pas possible de se projeter dans un monde marqué à la fois par une course aux armements et une forme de « loi de la jungle ». Pour les entreprises, le développement du « *hackback* » ne peut pas être une réponse aux attaques cyber ; il provoque en réalité une aggravation de l'insécurité. Aussi les grandes entreprises sont-elles, de façon générale, très demandeuses d'une régulation du cyber espace. C'est la raison pour laquelle le Cigref a soutenu l'initiative qui a présidé à l'Appel de Paris du 12 novembre 2018. La régulation passe par les échanges entre États pour mettre en place un cadre de droit international pour le cyber espace.

Il importe également que les systèmes d'information critiques puissent s'appuyer sur un cadre de régulation leur assurant que les solutions – produits, services, organisations – qu'ils adoptent répondent à des normes et des règles du jeu promulguées par les pouvoirs publics. Cela passe notamment par des schémas de certification et de labellisation. Les compteurs connectés et communicants Linky, par exemple, déployés chez tous les citoyens au rythme de 30 000 par jour, font tous l'objet d'une certification sécurité de premier niveau conformément au schéma défini par l'ANSSI.

Un troisième domaine de régulation est celui des données. En tant qu'entreprise de service public, Enedis doit apporter la garantie qu'elle est un opérateur de confiance notamment dans la gestion des données énergétiques dont elle est dépositaire et qu'elle est susceptible de mettre à disposition de ses clients, des fournisseurs d'électricité, ainsi que des collectivités territoriales pour les aider dans leur transition énergétique. Si une labellisation « opérateur de données de confiance » était créée, Enedis y serait candidat au premier chef.

Une nécessaire autonomisation

Parallèlement à la régulation, et pour se prendre en mains dans le domaine de la cyber sécurité, les acteurs comme les adhérents du CIGREF travaillent à :

- être *cyber by design*, c'est-à-dire prendre en compte la cyber sécurité dans tous leurs gestes, dès l'amont ;
- charger des équipes de garantir la conformité aux textes réglementaires ;

développer des CERT (Computer emergency response teams) chargées d'observer le réseau informatique et de réagir en cas d'incident ;

- piloter les dispositifs cyber et sensibiliser l'ensemble des collaborateurs et des dirigeants ;
- effectuer un travail approfondi en matière de gestion des ressources humaines et des compétences ;
- entretenir des liens étroits avec l'ANSSI.

En définitive, il importe que nous nous préparions collectivement à des chocs cyber majeurs : il s'agit de pouvoir continuer à fonctionner un certain temps sans système d'information, de se doter de moyens de télécommunication internes résilients, de pouvoir réunir rapidement les personnes clés en un même lieu pour faire face à la crise, de tenir dans la durée en cas de crise, etc.

Cyberconflict management

Jason Healey
Columbia University

From the history of *cyber*conflict

One of the favourite quotations which I encountered in preparing the book «*A fierce domain : cyber conflict, 1986 to 2012*», reflects what is now common knowledge: "*Few if any contemporary computer security controls have prevented a dedicated [red team] from easily accessing any information sought*". Spoken by Lieutenant Colonel Roger Schell in 1979, it referred to the almost guaranteed vulnerability of computer security systems when assailed by hired teams of hackers, a.k.a. "red teams" – and thus any relatively skilled attacker.

The real lesson, in my mind and that of regulators, lies in the following: this fundamental aspect of cybersecurity has been unchanged for four decades, despite tens of billions of dollars and euros in investments by the most advanced societies, hundreds of patents issued, new technologies devised, laws and regulations passed, and countless hours of discussion spent and sacrifices made by members of forums such as this one in the hopes of turning the situation around. Not only have these efforts not stemmed the tide, but hackers are making progress more swiftly than any attempts to defend.

Thus, in seeking to enable infrastructure protection and regulation, it is important that we be very humble in our aims; we have little reason to believe we are smarter or more skilled than those whom we seek to counter. Will the response lie in greater consistency, an entirely different approach, even greater spending, or more patience ?

Dynamics of cyber conflict

Between cybercrime and all-out cyber warfare, there exists a grey zone, a "fat middle" in which deleterious action is being taken by nations. The United States, through its Department of Defense, has stated that, as it is the only nation actually respecting norms, its best defence will be a good offence, a typically American – and perhaps also French – stance.

Bluntly stated, we need and intend to attack our attackers by making it more difficult for them to operate. Unfortunately, it is in the grey zone that many more operations and incidents are being observed in the critical infrastructures, and especially in energy.

Work on this topic at Columbia University has been aimed at returning to the roots of cyber conflict and examining how it differs from those of traditional conflict today (in the air, on the ground, or on the oceans). Such differences in dynamic include:

- the speed of light at which these attacks take place,
- the difficulty of attribution of guilt,
- and the changed concept regarding national borders, due to the nature of the Internet.

However, more important in my view is the role of the private sector: whereas warfare as we have known it is engaged in by nations (as citizens and companies either aid the effort or take care to remain out of the way), this is fundamentally not the case with cyber conflict, especially where Western or OECD countries are concerned.

Role of private sector

Few if any major computer attacks have been decisively resolved by any government. In almost every case, the private sector has played the key role in resolution. When Estonia was attacked in 2008, the nation's leadership and even NATO had no response on hand. The private sector coordinated between the major Internet service providers and telecommunications companies to ease the attacks as they hit. The same can be seen happening today in most major attacks.

The private sector enjoys agility and the ability to move quickly, along with subject matter expertise. Most importantly, it has the ability to change the Internet and cyberspace, even "bending it" if need be. Governments, especially those belonging to the OECD, tend to lack that strength.

Instead, states can lay claim to larger budgets and more staying power. They also have access to other levers, such as the military, regulation, a President's ability to point to right and wrong from his tribune, and diplomacy.

The best solutions, including the best regulation, will bring these two strengths together. Governments should not aim, against all odds, to replicate the capabilities of the private sector.

Examples of regulation and international cooperation across infrastructure sectors

The healthcare sector, though often receiving less attention than others, has been attacked with particular effectiveness by adversaries, and above all since the advent of ransomware. The North Korean WannaCry attack on the United Kingdom's National Health Service exemplifies this. I expect such action to continue and become even more rampant, as the use of embedded medical devices, both in hospitals and in the human body, grows. However, I would note also that, to thwart these attempts, the US Food & Drug Administration has devised some of the smartest regulation I have seen, embracing innovation but doing so carefully.

For the energy sector, the threats have changed very significantly and recently. The first adversaries began hacking into the electrical grid some 10 years ago. Such attacks now appear far more common and are coming increasingly from Russia and aimed at nuclear power plants. This particularly dangerous and definitely frightening strategy arose again only last month, when North Korean hackers infiltrated an Indian nuclear power plant.

In finance, where I have spent much of my career, the FS-ISAC (Financial Services Information Sharing and Analysis Center), an industry consortium dedicated to reducing cyber-risk in the global financial system, has just celebrated its 20th anniversary and continues to carry out invaluable work. The Bank for International Settlement, the International Monetary Fund and the G20's Financial Stability Board are identifying thrusts for common regulation and finding out how different States are addressing the problem.

At Columbia University, our time has been dedicated not only to exploring the security of banks, but also considering the systemic risk to finance and the economy, making great strides in the past two years.

As to publicly-traded companies, the US Securities and Exchange Commission, in perhaps one of its finest efforts, has asked all the companies on its stock market not to meet a specific degree of security or standard, but to pledge, through their Boards of Directors, to address cyber-risk as they would any other risk faced by the organisation. No more than 6 pages long, the regulation has changed the lives of companies, ensuring investors not purported security, but indeed transparency.

Lastly, to protect consumers, cyber-ratings companies such as BitSight and SecurityScoreCard have come on the scene, attributing scores to sites to reflect their likelihood of being successfully attacked. These results are now widely used by banks and other prominent players to verify the security of their vendors and make business collaboration decisions.

La stratégie de coordination entre régulateurs européens de l'électricité pour protéger les infrastructures critiques

Roman Picard
Commission de régulation de l'énergie (CRE)

New threats, challenges and responses

Systems operators are accustomed to managing threats as an integral part of their jobs, as they strive to preserve the quality of gas and electricity supply. As they are fully familiar with threat detection, risk management, and cybersecurity, threats to critical infrastructure are but a new variety of threat to them.

They do have to address a number of new challenges however. As Europe's energy networks are completely interconnected, grid stability is conditional upon the state of all the systems, as is cybersecurity today.

Moreover, it should be emphasised that human resources are the resource of cybersecurity, much more than computers. To manage risk, system operators must engage in traditional risk mitigation by reducing frequency and severity to have them manageable..

Today's response methods include firewalls, anti-viruses, cryptography – and the aforementioned human resources, in their new framing. To meet the new challenges, four levels of action are possible:

- the state of the art;
- emergency management systems;
- cybersecurity defense;
- training.

The European NIS Directive, France's Defence Code and the order on Smart Metering of 4 January 2012 in France, all pave the way for new players in the electricity and gas markets. For system operators, it is not easy to work in the presence of multiple regulators, as each may have very different aims and understandings. A new one is ANSSI dedicated to cybersecurity and we are also seeing stronger involvement on the part of other sectorial regulators already known in the field of energy (Cnil, Arcep, ANFR).

Strong involvement of the CRE and current works

As to the French energy regulator, CRE, it sees its natural level of discussion as European, with standards that are at least European and sometimes global.

The French Energy Regulator is co-chair on the CEER (council of European energy regulators) workstream dedicated to cybersecurity. This entity is distinct in that it is co-chaired by a national regulator as well as by the ACER (Agency for the cooperation of energy regulators). It thus enjoys a broader perspective that enables it to allocate responsibilities at the most appropriate level and maintain beneficial interactions.

Lastly, through the CEER, it works in the European Commission's Smart Grid Task Force Expert Group 2 (SGTF EG2) on cybersecurity, privacy and data protection, as well as an ad hoc group dedicated to privacy, security and standardisation.

The SGTF EG2is preparing to release a report that will be used as the foundation for the Cybersecurity Network Code. A true milestone for cybersecurity and energy, it will need at least two to three years to be ready for publication. It follows the European Commission's Recommendation on cybersecurity and energy this year, as the formal mandatory document.

The CEER workstream on cybersecurity continues to produce internal reports as well as a benchmark likely to be issued in early January.

Other areas monitored include :

- legislative and regulatory developments further to the NIS Directive and the Cybersecurity Act, to be sure they are applicable and easy to integrate by the operators;
- the smart metering systems that have not yet been rolled out;
- and smart grid projects.

Les initiatives de la Commission européenne sur la cyber sécurité des infrastructures

Frederik Geerts
Commission européenne, DG Energie

What can we expect from the new European Commission?

The European Green Deal

The European "Green Deal" will likely be the topic of every conversation in the next weeks. Mentioned in the political guidelines put forward by Ursula von der Leyen, as she prepared to become President of the European Commission, it sets very ambitious targets, including a reduction in emissions of at least 55 % by 2030 and climate neutrality for Europe by 2050.

It will cover areas as wide-ranging as agriculture, cohesion, health, transport – and energy, intertwining the latter with digitalisation and *cyber*security. Executive Vice-President Frans Timmermans is responsible for bringing this Deal to fruition.

A European Climate Law, dealing first and foremost with the energy sector, responsible for 75% of EU greenhouse gas emissions', will then be rolled out by 2050.

Challenges

The future grid will be far less linear and boast features often new to us:

- a significant increase in renewables decentralised generation
- decentralised storage,
- prosumer activity,
- full digitalisation,
- automatic balancing,
- and smart homes.

The Smart Grid will necessarily be built on the basis of existing infrastructure, parts of which are up to 30 years old. While IT will give the grid its "smart" nature, it will also inevitably connect crucial networks with a multitude of other sometimes less-monitored systems, and thus spike the risk of *cyber*-attacks. It would be an error to underestimate the impact of this new form of criminal activity. Though the January 2017 attack that left Ukraine without power for weeks on end is the most remembered, the 2016 attack has yet to be fully understood. Research organisations and government agencies continue to study its ramifications, intricacies and impacts.

Legislation and soft measures

General cybersecurity legislation is evolving very quickly: from the cybersecurity strategies devised in 2013, we were provided with the NIS Directive in 2016, the *Cyber*security Package in 2017, and most recently the *Cyber*security Act in 2019. The latter gave more

power to the governing authority and greater priority to *cyber*security certification of products, services and processes.

*Cyber*security legislation with a specific focus on energy has also developed, as exemplified by the regulation on security of gas supply, the 2019 Clean Energy Package for all Europeans, and the Network Code on *Cyber*security. The Clean Energy Package left the said Code available as an option, endowing it with the same power as a regulation. It will apply to all transmission operators and is the first to specifically deal with *cyber*security.

As to the Risk Preparedness Regulation, we are working with NSOE to develop a methodology by which Nation States will be able to conduct risk assessment specifically on the electricity sector, and with respect to *cyber*security. Based on risk scenarios, it will entail evaluation at the national, as well as regional or European level.

Some wondered whether more legislation was even needed for the energy sector. Yet it had been ascertained that many real time requirements would not be addressable using the traditional challenge-response, encryption, etc. measures. Moreover, due to cascading and interconnection, action taken on one section could affect a component of the same grid (for transport, banking, etc.) in another European country or even beyond its borders. Lastly, in the new Grid, systems up to 30 years old would be expected to work in combination with smart technologies and innovations, all in a secure manner.

The decision was thus made to forge ahead with legislation. The first series of stakeholder consultations revealed a need for :

- more information-sharing,
- guidance on implementing the NIS Directive for Member States,
- and regulation beyond the said Directive.

Events and workshops were then organised, at the European level as well as with the comparable Japanese authorities. It was at the same time that the workstream on implementation in the energy sector was set up under the NIS Directive Working Group.

The Commission recommendation C(2019)2400 issued in April 2019 acknowledged the need for an immediate response, in advance of the Network Code, and helped energy sector players further their understanding of how to implement *cyber*security (use of international standards, communication, etc.).

An additional staff working document has been issued to provide an overview of the existing legislation on energy, international standards, commission forums for stakeholders and experts, and more. Though the players addressed by the Directive are mainly larger companies, smaller entities not falling under the label of "operator of essential services" can still benefit from these recommendations.

Next steps

Through the workstream, follow-up is being carried out on the recommendation. Review will take place with the Member States and stakeholders so that progress can continue. Until the Network Code is in existence, this recommendation will be the main instrument.

Scenarios for the electricity sector will now need to be considered both on the regional and national levels.

We will also move forward with the Network Code on *Cyber*security, involving the DSOs, to enter a more formal process at the earliest possible date.

Lastly, *cyber*security certification in the energy sector is being envisioned, currently through stakeholder hearings.

Échanges avec la salle

From the floor

Is Europe adopting the same strategy as the US, and thus aiming to "attack the attackers"? What would the United States recommend to Europe in this area?

Jason Healey

The United States *Cyber*command calls this strategy "Defending Forward": as the US will not agree to norms with Russia and China at the negotiating tables in Geneva, its only concerted action would be a contestation of those two nations' action. Concretely, if it does not agree to prohibit attacks on hospitals, intellectual property theft for profit, or involvement in electrical groups, it will contest those activities if and when they occur. To do so, it would not only enforce norms, but also specifically remove infrastructure in order to limit action. By causing disruption or friction, the United States hopes to "turn down the heat". This strategy was first developed in academia and has made its way into the political arena.

I am still of a mixed opinion on recommendations, as they could in fact encourage more criminal action. While I would not advise Europe as a whole to take the same path, France could gain from doing so, set as it is between two nations with superior offensive capability and very strong intelligence, namely the Netherlands and the United Kingdom.

Frederik Geerts

National security is a national competency in Europe. The European Commission can thus not take a position on this. It has decided on *cyber*-diplomacy, an option that might prove beneficial to some nations as well.

From the floor

The Network Code applies only to electricity. Should a Network Code on Cybersecurity not also cover the gas system, and do so in the immediate future?

Frederik Geerts

Energy of course extends beyond electricity. The recommendation issued on *cyber*security applies to all energy sectors in general. While I cannot address whether the need for a network code explicitly including gas is needed at this time, I will reassert our determination to complete the network code for electricity, an area in which the highest risk exists.

From the floor

I would suspect that consumers are also blind with regard to cyber-security. Do you know of research evidence to the contrary?

Jason Healey

Quite comfortingly, most consumers, regardless of generation, would accurately sense that Apple is more secure than PC.

Certification is not necessarily the best way to ensure that consumers are informed. It quantifies the level of a system's security, while ratings systems (e.g., that of the UK) offer a comparative assessment. In the United States, the magazine Consumer Reports has been guiding consumers in major household purchases, assessing products selected key criteria. I hope that other countries in Europe and Asia will do the same.

The *Cyber*-Independent Testing Laboratories, run by a high-profile hacker, similarly tests devices using a repeatable, standard procedure to determine how their code was compiled (memory randomisation, library substitution, etc.), and thus how securely this was done. He has made these techniques and notions testable even by novices.

From the floor

The French Minister of Defence recently stated that France is ready to launch *cyber*-attacks, marking a clear change in approach, away from its "Maginot Line" of yesteryear and into proactive thinking.

Éric Brousseau

Regulation can at best manage the war against crime. It must be followed up by crisis management task forces, and highest up on the scale, offensive capabilities.

Clôture

Luc Rousseau
Conseil général de l'économie

La transformation numérique de nos sociétés les rend dépendantes de données et de systèmes informatiques de plus en plus connectés vers des terminaux de toute sorte. Cette ouverture est source de facilité et de richesse d'usage. Elle permet aux systèmes d'évoluer au rythme très rapide des innovations réalisées par les acteurs numériques. Toutefois, cette vitesse empêche souvent de prendre le temps d'une réflexion sur les enjeux politiques et sociétaux des innovations. L'interconnexion généralisée des systèmes informatiques, y compris ceux des particuliers, pose bien évidemment un défi permanent de sécurité.

Sous certains aspects, ces questions de sécurité ne sont pas nouvelles. Le vol d'information se pratique de longue date. Mais ce qui restait autrefois un acte assez rare d'espionnage est désormais un risque d'une permanence inquiétante, au cœur de la vie des individus, des entreprises et des États. D'autant qu'avec les interconnexions électroniques, ce vol peut désormais être perpétré depuis chez soi et, pire encore, depuis des réseaux virtuels plus difficiles de débusquer.

La sécurité numérique ne se réduit pas à la *cyber* sécurité. En effet, l'exploitation abusive de données personnelles ou la diffusion de fausses nouvelles via les médias sociaux ne nécessitent généralement pas la violation d'un système d'information particulier. Cela étant, la *cyber* sécurité s'attache à protéger les données et les systèmes contre les attaques criminelles d'individus, d'organisations voire d'États.

Les débats de ce matin l'ont bien montré, il s'agit là d'un enjeu global, comme souvent dans le numérique. La coopération des régulateurs nationaux est donc essentielle, tout comme celle entre les entreprises.

Je me réjouis que ce quatrième colloque, organisé conjointement par le Conseil général de l'économie, la Chaire gouvernance et régulation et la Fondation Paris Dauphine, ait pu, comme les années précédentes, illustrer l'articulation complexe entre économie, régulation, souveraineté nationale et coopération internationale.

Il n'est de la responsabilité ni des administrations ni des universités ou des entreprises de se substituer à la décision politique. Mais chaque entité, dans son périmètre d'action et de réflexion, a le devoir de se préoccuper de la menace *cyber* et peut contribuer à éclairer la décision. En l'occurrence, cette matinée aura bien illustré notre aptitude collective à éclairer les décideurs politiques et les responsables d'entreprise sur un sujet fort complexe dans lequel se mêlent des enjeux de sécurité, de souveraineté, de technologie et d'économie.

Chaire Gouvernance et Régulation
Fondation Paris-Dauphine
Place du Maréchal de Lattre de Tassigny - 75016 Paris (France)
http://chairgovreg.fondation-dauphine.fr