Cybersécurité des infrastructures énergétiques. Regards croisés Europe/États-Unis

Arnault Barichella

Études de l'Ifri

CYBERSÉCURITÉ DES INFRASTRUCTURES ÉNERGÉTIQUES

Regards croisés Europe/États-Unis

Arnault BARICHELLA

Février 2018

ifri Centre Énergie

L'Ifri est, en France, le principal centre indépendant de recherche, d'information et de débat sur les grandes questions internationales. Créé en 1979 par Thierry de Montbrial, l'Ifri est une association reconnue d'utilité publique (loi de 1901). Il n'est soumis à aucune tutelle administrative, définit librement ses activités et publie régulièrement ses travaux.

L'Ifri associe, au travers de ses études et de ses débats, dans une démarche interdisciplinaire, décideurs politiques et experts à l'échelle internationale.

Cette étude est publiée dans le cadre du projet ENERGEO financé par le Conseil supérieur de la formation et de la recherche stratégiques (CSFRS).

CSFRS
Conseil Supérieur de la Formation et de la Recherche Stratégiques

ISBN : 978-2-36567-796-7

Comment citer cette publication :
Arnault Barichella, « Cybersécurité des infrastructures énergétiques. Regards croisés Europe/États Unis », *Études de l'Ifri*, Ifri, février 2018.

Ifri

27 rue de la Procession 75740 Paris Cedex 15 – FRANCE

Tél. : +33 (0)1 40 61 60 00 – Fax : +33 (0)1 40 61 60 60

E-mail : accueil@ifri.org

Site internet : Ifri.org

Auteur

Arnault Barichella est doctorant à l'Institut d'études politiques de Paris dans le programme doctoral en science politique. Ses recherches portent sur l'analyse comparative des politiques climatiques et énergétiques en Europe et aux États-Unis.

Auparavant, il a travaillé à l'Organisation des Nations unies pour l'éducation, la science et la culture (UNESCO) et ensuite au Programme des Nations unies pour l'environnement (PNUE) sur le développement de projets concernant l'efficacité énergétique et la production et consommation durables, dans le cadre de la préparation de la COP21. Il a également travaillé au Sénat pour la rédaction du *Livre Vert de la Défense* portant sur l'impact des enjeux énergétiques et environnementaux sur la sécurité nationale.

Arnault Barichella est titulaire du master Affaires européennes de l'Institut d'études politiques de Paris et d'une licence en histoire de l'université d'Oxford.

Avant-propos

Cette étude a été réalisée en prenant appui sur une revue de la littérature, ainsi que sur une quinzaine d'entretiens avec des experts et des professionnels dans les domaines de la cybersécurité et de l'énergie en Europe et aux États-Unis.

L'auteur souhaite remercier toutes les personnes interrogées pour leur soutien et les informations apportées sur ce sujet sensible. Les entretiens se sont déroulés aux États-Unis et en Europe avec des personnes issues d'un large éventail aussi représentatif que possible des différents acteurs concernés, à la fois dans le secteur public et privé.

Les personnes interrogées ayant souhaité garder leur anonymat, les informations issues de ces entretiens et ayant servi à la rédaction de cette étude n'ont pas été attribuées.

Résumé

L'accélération de la numérisation des infrastructures énergétiques apporte de nombreux bénéfices économiques, notamment en termes de rationalisation de la consommation d'énergie avec des gains d'efficacité. Néanmoins, cela a aussi pour conséquence d'augmenter les risques de cyberattaques, où des logiciels malveillants tirent avantage de la digitalisation croissante des équipements. Les récentes cyberattaques qui ont visé les infrastructures critiques ukrainiennes soulignent que la menace est réelle et grandissante. La vulnérabilité n'est pas cantonnée aux infrastructures situées dans l'Union européenne (UE) ou aux États-Unis : certaines attaques dont a été victime l'Ukraine se sont propagées à de nombreuses entreprises occidentales notamment à travers leurs filiales, soulignant le danger de contagion par le biais de logiciels malveillants.

Au cours des dernières années, l'UE et les États-Unis ont progressivement adopté une série de mesures et de réglementations pour protéger les infrastructures énergétiques face au risque cyber. Cependant, les approches américaines et européennes présentent de nombreuses différences. En effet, les États-Unis ont privilégié une stratégie sécuritaire de fond (« security in depth ») avec des réglementations strictes et détaillées dans des secteurs précis, appliquées par des institutions aux pouvoirs coercitifs. En revanche, l'UE a adopté une stratégie plus souple et générale, couvrant un large éventail de domaines et laissant une marge de manœuvre importante aux États membres dans la mise en application des normes. Toutefois, ces approches sont aussi potentiellement complémentaires, dans la mesure où les forces du système américain peuvent servir de modèle pour améliorer certaines faiblesses dans l'approche européenne, et réciproquement, puisque les États-Unis pourraient aussi tirer un certain nombre d'enseignements de l'UE.

En effet, le modèle américain est en avance sur l'UE au niveau du développement de normes précises et détaillées pour la cybersécurité, ainsi que dans la mise en application de ces normes. Seule une poignée d'États européens, dont la France, ont un niveau de normes équivalent et l'UE souffre de manquements et de faiblesses tant à l'échelle communautaire que nationale. Néanmoins, les États-Unis peuvent apprendre de l'UE concernant la protection de la vie privée et des données à caractère personnel, la cybersécurité appliquée aux technologies bas-carbone, ainsi que la protection des réseaux de distribution électrique. De plus, la Californie et la

France présentent un certain nombre de spécificités pertinentes en la matière.

C'est pourquoi il est essentiel de renforcer la coopération transatlantique afin de permettre à l'UE et aux États-Unis d'apprendre chacun du modèle de l'autre. Cela pourrait avoir lieu à travers différentes plateformes, ce qui inclurait un renforcement de la collaboration bilatérale entre les gouvernements, ainsi qu'une meilleure coopération au sein de structures multilatérales telles que l'Organisation du traité de l'Atlantique nord (OTAN) et le G7, et finalement au niveau des partenariats public-privé. L'objectif serait de développer l'harmonisation des normes entre l'UE et les États-Unis afin de pouvoir progressivement mettre en place des standards transatlantiques communs en matière de cybersécurité. Il est important de noter que le président Trump a manifesté un vif intérêt pour les questions liées à la cybersécurité en renforçant la politique de son prédécesseur en la matière. Par conséquent, malgré les divergences actuelles entre l'UE et les États-Unis sur de nombreux sujets, la cybersécurité représente un domaine où il existe une réelle opportunité pour approfondir la coopération transatlantique dans les années à venir.

Ainsi, les standards transatlantiques communs pourraient ensuite devenir des normes internationales de cybersécurité rigoureuses, permettant de réduire les risques de propagation. Il y a aussi une dimension économique essentielle, où tout retard de l'UE en matière de cybersécurité risque de diminuer la compétitivité des entreprises européennes spécialisées par rapport aux entreprises américaines, avec des pertes potentiellement significatives dans un marché qui a vocation à représenter des centaines de millions d'euros d'investissements et des milliers d'emplois par an pour le seul secteur de l'énergie dans l'UE.

Sommaire

Introduction

La cybersécurité est un enjeu de plus en plus important touchant pratiquement tous les secteurs et toutes les activités en raison de la numérisation croissante de nos sociétés. Le secteur de l'énergie possède des caractéristiques qui lui sont propres, méritant donc des règles particulières en la matière, complémentaires mais souvent différentes des autres secteurs. En effet, les technologies de l'information et de la communication (TIC) n'ont que lentement été intégrées aux infrastructures énergétiques. Cela est dû principalement à la longueur des cycles d'investissement dans ce secteur, ce qui a retardé sa digitalisation. Néanmoins, l'exigence de rationaliser la production, la distribution et la consommation d'énergie pour traiter un nombre important de données, ainsi que le besoin de faciliter la communication entre les différents sites et équipements, a contribué au déploiement progressif des TIC dans les infrastructures énergétiques. Cette numérisation induit des gains d'efficacité importants en optimisant la chaîne d'approvisionnement grâce à l'analyse de données complexes et au pilotage à distance. Le consommateur peut bénéficier de services plus personnalisés, permettant de mieux réguler sa consommation d'énergie et faire des économies. Malgré ces avantages, le déploiement des TIC dans l'industrie énergétique a aussi eu pour conséquence d'augmenter considérablement les risques de cyberattaques. En effet, le secteur de l'énergie est passé de systèmes industriels relativement isolés et protégés à un réseau ouvert employant des technologies fortement interconnectées *via* Internet et les réseaux des entreprises. De plus, en raison de la durée des cycles d'investissement, les équipements sont souvent âgés et nombre d'entre eux resteront encore en service pendant plusieurs décennies. Ces derniers ont été conçus à une époque où le risque cyber était peu développé, et n'ont donc pas intégré de fonctionnalités pour la cybersécurité, ce qui les rend vulnérables. En outre, les systèmes de protection issus du monde de l'informatique ne sont pas facilement transposables sur les infrastructures énergétiques.

Cette vulnérabilité accrue de l'industrie énergétique l'a exposé à un nombre croissant de cyberattaques au cours des dernières années. La cybersécurité inclut à la fois les virus informatiques dont l'objectif est de provoquer des dégâts matériels et physiques, mais aussi le piratage et le vol de données à des fins lucratives. En effet, l'espionnage industriel et de la cybercriminalité demeure l'une des principales motivations derrière les

cyberattaques, constituant des violations de la vie privée. En plus de l'espionnage entre entreprises ou entre pays par souci de compétitivité, les groupes criminels utilisent de plus en plus des logiciels malveillants pour parvenir à leurs fins. En outre, la dimension politique est aussi devenue un facteur majeur au cours des dernières années. Les risques importants encourus par le secteur de l'énergie furent révélés en 2010 avec la découverte du virus *Stuxnet* qui avait infecté le complexe iranien d'enrichissement d'uranium de *Natanz*. *Stuxnet* a démontré que les cyberattaques peuvent aussi être liées à des enjeux géopolitiques et conduites par des États[1].

Le rôle prépondérant de l'industrie énergétique pour l'économie nationale et pour toutes les fonctions vitales d'un pays (défense, communication, santé…) en fait une cible de plus en plus privilégiée dans les affrontements géopolitiques entre États. Cela est notamment lié au fait qu'il est souvent difficile d'attribuer avec précision la responsabilité d'une cyberattaque, permettant à un État de recourir à l'espionnage à grande échelle ou de causer des dégâts majeurs sans s'engager ouvertement[2]. Ainsi, bien que la Russie soit le premier suspect, il n'a pas été possible de définir à l'heure actuelle la responsabilité d'une série de cyberattaques qui ont récemment frappé l'Ukraine[3]. Cela inclut le virus *Black Energy* en décembre 2015 qui a déconnecté trente postes électriques du réseau ukrainien, avec plus de 200 000 personnes affectées dans huit régions pendant plusieurs heures. En mai 2017, l'Ukraine a de nouveau été victime d'une attaque par le virus *XData*, qui a servi de précurseur à une attaque beaucoup plus dévastatrice un mois plus tard avec le virus *NotPetya*. D'après les dernières estimations, ce dernier aurait infecté 18 % des entreprises de l'énergie, et au total plus de 30 % des systèmes informatiques dans tout le pays[4]. Beaucoup d'entreprises de pays occidentaux en relations commerciales avec l'Ukraine ont été affectées par le virus, notamment le groupe français Saint-Gobin et le transporteur maritime danois Maersk, ainsi que leurs sous-traitants. En effet, les grands groupes internationaux sont particulièrement vulnérables en raison de leurs filiales dispersées dans de nombreux pays. L'UE et les États-Unis avaient déjà été touchés un peu plus tôt cette année par la propagation mondiale du virus *WannaCry* le

1. En effet, plusieurs enquêtes ont permis d'émettre l'hypothèse que le niveau de sophistication du virus *Stuxnet* nécessitait des moyens très avancés, probablement soutenus au niveau étatique. Voir : G. Desarnaud, « Cyberattaques et systèmes énergétiques : faire face au risque », *Études de l'Ifri*, Ifri, janvier 2017, disponible sur : www.ifri.org.

2. Voir J. R. Lindsay, « Tipping the Scales: The Attribution Problem and the Feasibility of Deterrence against Cyberattack », *Journal of Cybersecurity*, vol. 1, n° 1, 1er septembre 2015, p. 53-67.

3. Voir : *Global Cybersecurity Summit 2017*, qui s'est tenu à Kiev en Ukraine du 14 au 15 juin 2017, https://gcs17.com.

4. A. Guiton, « Enquête : Les cobayes de la cyberguerre », *Libération*, 28 juillet 2017, disponible sur : www.liberation.fr.

12 mai, faisant selon Europol plus de « 200 000 victimes » dans 150 pays, causant des dégâts importants dans de nombreux secteurs.

Afin de faire face à ces risques et menaces réels, les États-Unis et l'UE ont progressivement mis en place un certain nombre de réglementations, de lois et d'institutions pour protéger le secteur énergétique face aux cyberattaques. La première partie de cette étude analysera ce que l'UE peut apprendre des États-Unis dans ce domaine. La deuxième partie examinera ensuite ce que les États-Unis peuvent apprendre des approches et règles européennes. La Californie et la France seront présentées comme exemples d'État américain et de pays membre de l'UE ayant des spécificités pertinentes en la matière. La troisième partie proposera des solutions pour renforcer la coopération transatlantique afin que l'UE et les États-Unis puissent développer des standards internationaux communs en matière de cybersécurité dans le secteur de l'énergie.

L'enjeu de la protection des infrastructures nucléaires contre les risques cyber revêt une importance fondamentale. Cette dimension spécifique fait l'objet depuis longtemps de travaux et prescriptions au sein de l'Agence internationale de l'énergie atomique (AIEA) qui est l'autorité de gouvernance mondiale du nucléaire civil et n'entre pas dans le cadre de cette étude[5].

5. AIEA, « Computer Security at Nuclear Facilities », *Security Series,* n° 17, 2011.

Regards croisés : ce que l'Union européenne peut apprendre des États-Unis

Le développement de normes strictes, détaillées et exhaustives concernant la cybersécurité

Les attentats du 11 septembre 2001 ont eu un effet d'accélérateur sur le développement de normes exhaustives et détaillées en matière de cybersécurité aux États-Unis. Les autorités américaines ont progressivement pris conscience de l'importance stratégique d'y inclure le secteur de l'énergie. En 2005, le Congrès a ratifié le *Energy Policy Act*, donnant à la *Federal Energy Regulatory Commission* (FERC) la responsabilité de désigner une entité (*Electric Reliability Organization*, ERO) pour établir des standards de sécurité pour le réseau électrique à l'échelle fédérale. Ce fut la *North American Electric Reliability Corporation* (NERC), une organisation privée[6], qui fut désignée en tant que ERO pour l'ensemble des États-Unis et placée sous la supervision de la FERC. La NERC a développé une série de normes pour la cybersécurité, ciblant les entités de production et de transport d'électricité (*Bulk Power System* – BPS). Rassemblés sous le nom de *Critical Infrastructure Protection Standards* ou NERC-CIPs, les premiers NERC-CIPs ont été approuvés par la FERC en janvier 2008. Ils représentent des standards parmi les plus détaillés et exhaustifs au monde et sont obligatoires pour l'ensemble des 3 000 *utilities* (fournisseurs d'électricité) aux États-Unis. Cela inclut des mesures précises couvrant, par exemple, la sécurité des systèmes de gestion informatique, la formation du personnel, la sécurité physique du BPS, ainsi que des plans de récupération des données sur les systèmes en cas de cyberattaque. De plus, les NERC-CIPs ont été mis à jour de façon régulière afin de faire face à l'évolution rapide des cybermenaces. La FERC a approuvé la 5e version en 2013 et la 6e en 2016, apportant des améliorations notables. Lors de son second mandat, le président Obama a pris la décision de signer un *Executive*

6. La NERC est chargée d'assurer la sécurité du réseau électrique non seulement aux États-Unis, mais aussi sur une partie du Canada et du Mexique.

Order (EO)[7] et deux *Presidential Policy Directives* (PPD)[8] afin de contourner le Congrès, qui avait bloqué le passage du *GRID Act*[9] en 2012. En outre, il est important de noter que la cybersécurité représente un domaine où le président américain actuel a choisi de continuer la politique de son prédécesseur. Donald Trump a en effet déjà signé un EO qui approfondit les mesures prises par le président Obama, prévoyant entre autres une revue de l'ensemble des normes fédérales afin d'identifier les mises à jour nécessaires, démontrant ainsi un intérêt notable pour les questions de cybersécurité[10].

Objectifs des standards NERC-CIPs (Versions 5 et 6)

Numéro	Standards NERC-CIPs (Versions 5 et 6)	Objectifs	Date d'entrée en vigueur
CIP-002 5.1a	Catégorisation des systèmes informatiques du réseau électrique	Catégoriser les différents systèmes informatiques afin d'identifier les vulnérabilités du réseau électrique et les mesures appropriées	12/2016
CIP-003-6	Contrôles de gestion pour la sécurité	Établir la responsabilité et renforcer les mécanismes de contrôle pour la gestion des incidents de cybersécurité du réseau électrique	7/2016
CIP-004-6	Personnel et formation	Minimiser les risques d'accidents liés à l'erreur humaine en renforçant la formation du personnel en matière de cybersécurité	7/2016
CIP-005-5	Périmètre de sécurité électronique	Gérer l'accès sécurisé au réseau électrique en mettant en place un périmètre de sécurité électronique autour des infrastructures	7/2016

7. *Executive Order* 13636, « Improving Critical Infrastructure Cybersecurity », (12/02/2013).
8. *Presidential Policy Directive* 21, « Critical Infrastructure Security and Resilience » (12/02/2013) et *Presidential Policy Directive* 41, « United States Cyber Incident Coordination » (26/07/2016).
9. E. O'Keefe et E. Nakashima, « Cybersecurity Bill Fails in Senate », *The Washington Post*, 2 août 2012, disponible sur : www.washingtonpost.com.
10. *Executive Order* 13800, « Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure ».

CIP-006-6	Sécurité physique des systèmes informatiques du réseau électrique	Protéger et gérer l'accès physique aux systèmes informatiques en définissant un plan de sécurité pour l'ensemble du réseau électrique	7/2016
CIP-007-6	Gestion du système de sécurité	Renforcer le système de sécurité en définissant les exigences techniques, opérationnelles et procédurales du réseau électrique	7/2016
CIP-008-5	Signalement des incidents et planification des interventions	Mettre en place des procédures pour le signalement des incidents de cybersécurité et la planification des interventions sur le réseau électrique	7/2016
CIP-009-6	Plans de récupération des systèmes informatiques du réseau électrique	Définir des plans pour la récupération des systèmes informatiques en cas de cyberattaque sur le réseau électrique	7/2016
CIP-010-2	Gestion des changements de configuration et évaluation des vulnérabilités	Évaluer les vulnérabilités des systèmes informatiques lors des mises à jour de logiciels et des changements de configuration du réseau	7/2016
CIP-011-2	Protection de l'information	Mettre en place des mesures pour protéger les systèmes informatiques contre le vol ou le piratage de données liées au bon fonctionnement du réseau	7/2016
CIP-014-2	Sécurité physique	Identifier les infrastructures critiques du réseau électrique et mettre en place des mesures pour en assurer la protection contre les attaques physiques	10/2015

Bien que l'UE se soit intéressée à ce sujet à peu près au même moment, les mesures qui y ont été prises n'ont pas le même niveau de précision que la réglementation américaine. Le programme européen de protection des infrastructures critiques (PEPIC) de 2006, ainsi que la directive sur les infrastructures critiques européennes (ICE) de 2008, laisse une grande marge de manœuvre aux États membres et se contente de définir quelques critères imprécis pour protéger les infrastructures. La stratégie de

cybersécurite´ de l'UE, adoptée en février 2013, établit une liste de priorités stratégiques, notamment au niveau des infrastructures critiques, ce qui inclut le secteur de l'énergie. Néanmoins, le document se focalise sur d'autres secteurs principalement en lien avec la cybercriminalité et la politique de sécurité et de défense commune (PSDC), et ne propose pas de mesures concrètes mais simplement des axes stratégiques généraux. En outre, la nouvelle directive sur la sécurité des réseaux et de l'information (SRI), adoptée en juin 2016, pose certaines bases pour le développement de normes européennes en établissant des critères communs pour les « opérateurs de services essentiels » (OSE)[11]. Le paquet sur la cybersécurité, proposé par la Commission européenne en septembre 2017, contient des conseils pratiques pour la mise en application de la directive SRI et pour l'interprétation de certaines de ses clauses[12]. Ces dispositions furent confirmées lors du sommet sur le numérique qui s'est tenu à Tallinn le 29 septembre 2017 sous la présidence estonienne du Conseil de l'UE. Malgré cela, la responsabilité pour définir le détail des normes a été laissée une nouvelle fois aux États membres, qui sont chacun chargés de mettre au point leurs propres stratégies nationales de cybersécurité. Ainsi, la directive SRI risque de ne pas être suffisamment précise car elle se limite à des critères généraux sur ce qui constitue un OSE, ainsi que sur les mesures de sécurité à mettre en place, notamment pour la prévention et la gestion des risques. Jusqu'alors, il en a résulté le développement d'une Europe à plusieurs vitesses, avec des décalages parfois importants au niveau des normes de cybersécurité entre les différents pays européens.

Selon une étude approfondie de la société Software Alliance (BSA), les normes européennes en matière de cybersécurité sont très variables au sein de l'UE. Alors que la plupart des États membres ont mis en place une stratégie nationale de cybersécurité, certains tels que la Bulgarie, la Grèce, le Danemark, l'Irlande et la Suède ne l'ont toujours pas fait. En outre, des pays tels que Croatie, la Lettonie, le Luxembourg et le Portugal n'ont pas développé de plan pour la protection des infrastructures critiques, et d'autres tels que la Belgique, l'Italie et la Slovaquie n'ont pas de législation préconisant au moins un audit annuel de cybersécurité[13]. Cette situation est problématique, car les infrastructures énergétiques européennes sont fortement interconnectées. Les États membres avec les normes de cybersécurité les moins avancées constituent des maillons faibles, où des

11. Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'UE. Disponible sur : http://eur-lex.europa.eu.

12. Commission européenne, *New Cybersecurity Package*, septembre 2017, disponible sur : https://ec.europa.eu.

13. BSA/The Software Alliance, *Tableau de bord de la cybersécurité dans l'UE: Vers un cyberespace europe´en se´curise´*, janvier 2015, disponible sur : http://cybersecurity.bsa.org.

logiciels malveillants peuvent pénétrer et se répandre à l'ensemble du réseau. Par conséquent, il est essentiel de renforcer la directive SRI avec de nouvelles normes plus approfondies, et l'UE pourrait s'inspirer notamment des NERC-CIPs aux États-Unis. Bien qu'il soit évidemment impossible de copier le modèle fédéral américain, l'UE peut tout de même en tirer un certain nombre d'enseignements, notamment au niveau de la mise en place de normes européennes plus précises et exhaustives. En outre, le développement d'une réglementation spécifique et mise à jour de façon régulière pour la sécurité du réseau électrique, et non pour les infrastructures critiques en général comme le fait la directive SRI, permettrait un niveau de détail plus important. L'UE pourrait adopter une nouvelle initiative qui intégrerait ces normes, mais il faudrait le faire cette fois-ci sous la forme d'un règlement. En effet, contrairement à la directive qui doit être transposée dans le droit national, le règlement est directement applicable sans aucune mesure de transcription et s'applique de manière simultanée et uniforme à l'ensemble des États membres, réduisant ainsi le risque de normes différenciées entre les pays européens.

Comparaison entre les normes de cybersécurité aux États-Unis et dans l'UE (par ordre chronologique, en bleu pour l'UE et en blanc pour les États-Unis)

Date de ratification	Nom de la loi ou de la réglementation	Résumé du contenu et clauses principales
08/2005	*US Energy Policy Act*	Donne un mandat à la FERC pour désigner une *Electric Reliability Organization* (ERO) afin de mettre en place des standards de sécurité obligatoires pour le réseau électrique
01/2006	Directive de l'UE sur la sécurité de l'approvisionnement en électricité et les investissements dans les infrastructures	Établit une série de mesures pour sécuriser l'approvisionnement de l'UE en électricité, ainsi que pour le bon fonctionnement du marché interne de l'électricité, sans se référer spécifiquement à la cybersécurité
12/2006	Programme européen de protection des infrastructures critiques (PEPIC)	Établit un cadre général intersectoriel pour la sécurité des infrastructures critiques, qui inclut la cybersécurité, le terrorisme, le crime organisé et les catastrophes naturelles
12/2007	*US Energy Independence and Security Act*	Donne un mandat à la *National Institute of Standards and Technology* (NIST) afin de mettre en place des standards de sécurité pour le *smart grid* (réseau électrique intelligent)

12/2008	Directive de l'UE sur les infrastructures critiques européennes (ICE)	Établit des critères généraux pour identifier et protéger les infrastructures critiques, notamment au niveau de la cybersécurité, qui s'appliquent aux secteurs de l'énergie et du transport
10/2010	Règlement de l'UE sur la sécurité de l'approvisionnement en gaz naturel	Établit une série de mesures pour sécuriser l'approvisionnement de l'UE en gaz naturel. Une mise à jour qui inclut la cybersécurité a été adoptée en avril 2017 et entrera en vigueur prochainement
02/2013	*US Executive Order 13636 "Improving Critical Infrastructure Cybersecurity"*	Astreint la NIST à mettre en place un cadre de cybersécurité pour un développement sécurisé du *smart grid*. Le résultat a été la création du *NIST Framework* qui, même s'il n'est pas obligatoire mais volontaire, a été largement adopté par les entreprises américaines
02/2013	*US Presidential Policy Directive 21 "Critical Infrastructure Security and Resilience"*	Renforce le contrôle des agences fédérales sur la cybersécurité des infrastructures critiques, notamment le secteur de l'énergie
02/2013	Stratégie de cybersécurité de l'Union européenne	Établit une liste de priorités stratégiques pour la cybersécurité dans l'UE, notamment au niveau des infrastructures critiques, ce qui inclut le secteur de l'énergie
12/2015	*Fix America's Surface Transportation Act (FAST Act)*	Bien que cette loi se concentre sur le secteur des transports, elle a aussi augmenté les pouvoirs du secrétaire à l'Énergie concernant les cyberattaques sur le réseau électrique
06/2016	Directive de l'UE sur la sécurité des réseaux et de l'information (SRI)	Pose certaines bases pour le développement de normes européennes de cybersécurité en établissant des critères communs pour les « opérateurs de services essentiels » (OSE), ainsi que sur les mesures à mettre en place, notamment pour la prévention et la gestion des risques
07/2016	*US Presidential Policy Directive 41 "United States Cyber Incident Coordination"*	Renforce la coordination des institutions fédérales chargées de développer des standards nationaux pour la cybersécurité, notamment la FERC, la NERC et le *Department of Energy*
05/2017	*US Executive Order 13800, "Strengthening the Cybersecurity of*	Astreint le secrétaire à l'Énergie, en consultation avec les autres agences fédérales, à étudier la résistance du réseau électrique

	Federal Networks and Critical Infrastructure"	américain face aux cyberattaques afin d'identifier les mises à jour nécessaires
09/2017	Paquet sur la cybersécurité, proposé par la Commission européenne	Contient des conseils pratiques pour la mise en application de la directive SRI. Prévoit le renforcement des compétences de l'ENISA en lui donnant notamment un mandat permanent, ainsi que la création d'un système de certification européen pour développer un marché intérieur de la cybersécurité

Un système efficace pour la mise en application des normes de cybersécurité

Les États-Unis ont aussi développé un système relativement avancé pour la mise en application des normes de cybersécurité, un autre sujet qui pourrait être source d'enseignements pour l'UE. En effet, la NERC dispose de moyens contraignants pour vérifier que les *utilities* (fournisseurs d'électricité) respectent bien les NERC-CIPs. Tout d'abord, elle peut imposer des amendes pouvant atteindre jusqu'à un million de dollars par jour jusqu'à la mise aux normes. La NERC a récemment pris la décision d'augmenter le niveau des amendes pour faire face au non-respect des standards CIPs par certaines entreprises, et a notamment imposé en 2016 deux amendes de 1,1 et 1,7 millions de dollars[14]. Selon l'une des personnes interrogées, il s'agit d'une mesure extrêmement efficace qui a permis de dissuader des fraudeurs potentiels, les *utilities* préférant dans la plupart des cas se conformer aux normes plutôt que d'avoir s'acquitter de montants aussi élevés. La NERC dispose aussi d'équipes d'intervention spécialisées dont la mission est d'inspecter un certain nombre de *utilities* chaque année pour vérifier la mise en application des normes de sécurité.

De plus, la NERC a développé un système d'alerte (*NERC Alerts*) qui permet d'informer l'ensemble des *utilities* d'un risque cyber imminent. Ces *NERC Alerts* permettent notamment de vérifier leur coordination et délai de réaction, servant à identifier celles qui ne respectent pas suffisamment les règles, ainsi qu'à installer les mises à jour nécessaires. La NERC a émis 41 alertes depuis 2009, dont deux à un niveau élevé en 2016, la première suite aux cyberattaques en Ukraine et la deuxième en lien avec des logiciels

14. R. Fallon et M. Lazaroff, *NERC Increasing Penalties for Fundamentally Failing to Comply with Cyber Standards*, Cozen O'Connor, novembre 2016, disponible sur : www.lexology.com.

malveillants se servant de « l'Internet des objets » (*Internet of Things*)[15]. En outre, la NERC tient aussi chaque année une grande conférence (*Grid Security Conference* ou GridSecCon) qui rassemble les experts de la cybersécurité issus du secteur public et de l'industrie. La GridSecCon permet à tous les acteurs concernés d'échanger des informations techniques afin que les normes de cybersécurité soient appliquées de manière cohérente. Enfin, la NERC organise tous les deux ans un exercice de grande ampleur qui simule une cyberattaque sur le réseau électrique (*Grid Security and Emergency Response Exercise* ou GridEx) en collaboration avec les institutions fédérales, locales et le secteur privé. Le dernier exercice de ce type (*GridEx IV*) s'est tenu en novembre 2017 avec environ 7 000 participants issus de 450 organisations différentes, permettant de tester en temps réel l'efficacité des pratiques de cybersécurité afin de déterminer les améliorations possibles. Pour mener à bien sa mission, la NERC dispose d'un budget conséquent de 69,6 millions de dollars pour l'année 2017, d'une équipe d'environ 190 salariés à temps plein ainsi que de nombreux sous-traitants et consultants[16].

Les défis institutionnels du système européen de cybersécurité

Au niveau de l'UE, il n'y a aucun équivalent pour la mise en application des normes de cybersécurité. Depuis 2004, il existe une Agence européenne chargée de la sécurité des réseaux et de l'information (*European Network and Information Security Agency*, ENISA) basée à Héraklion en Grèce, dont le mandat a été élargi par l'UE en 2013[17]. Dans le paquet sur la cybersécurité proposé en septembre 2017, la Commission européenne prévoit de réformer l'ENISA en lui attribuant un mandat permanent, ainsi que de renforcer certaines de ses compétences pour lui permettre de mieux soutenir les États membres. Cela inclut notamment la mise en application de la directive SRI, ce qui fut réaffirmé lors du sommet sur le numérique de Tallinn en septembre 2017. Malgré ces avancées, le rôle d'ENISA demeure cependant

15. Suite à cela, la NERC a publié en collaboration avec le E-ISAC un document afin de renforcer la mise en application des normes de cybersécurité pour les *utilities* américaines concernant « l'Internet des objets » (*Internet of Things DDoS White Paper*).

16. Par rapport à l'étendue de son mandat qui couvre une grande partie de l'Amérique du Nord, les effectifs de la NERC en termes de salariés à temps plein peuvent paraître un peu faibles. Cela est dû au fait que la NERC, en tant qu'organisation privée, externalise et sous-traite une part importante de ses activités. Voir : *NERC 2017 Business Plan and Budget, Final Draft, Finance and Audit Committee Meeting*, août 2016, disponible sur : www.nerc.com.

17. Règlement (UE) n° 526/2013 du Parlement européen et du Conseil le 21 mai 2013 concernant l'Agence européenne chargée de la sécurité des réseaux et de l'information. Ce règlement a renouvelé le mandat de l'ENISA pendant sept ans et a élargi ses responsabilités, notamment au niveau de la lutte contre la cybercriminalité.

limité à conseiller les États membres, recueillir et analyser des données, promouvoir des méthodes de gestion des risques, ainsi que favoriser l'échange de bonnes pratiques. Elle ne dispose d'aucun pouvoir coercitif, et ses moyens sont bien moins importants que ceux de la NERC[18]. Par exemple, pour l'année 2017, l'ENISA dispose d'un budget de 11,2 millions d'euros (contre 69,6 millions de dollars pour la NERC) et d'une équipe de 84 salariés à temps plein (contre 190 pour la NERC, avec de nombreux sous-traitants)[19].

En outre, la directive SRI astreint chaque État membre à mettre en place un centre d'alerte national (*Computer Security Incident Response Team* ou CSIRT), dont la mission est notamment de veiller à ce que les « opérateurs de services essentiels » respectent les standards de cybersécurité. La directive prévoit aussi la création d'un réseau composé de tous les CSIRT nationaux, ainsi qu'un « groupe de coopération » impliquant la Commission européenne et les institutions nationales compétentes, afin de faciliter le partage d'informations. Néanmoins, ni le réseau CSIRT ni le « groupe de coopération » n'ont de pouvoirs contraignants pour assurer la mise en application des normes de cybersécurité, cette responsabilité étant laissée aux CSIRT nationaux. Ainsi, ce sont les États membres qui doivent décider quelles compétences attribuer aux CSIRT et comment ils souhaitent organiser la vérification des standards. Même si les dispositions de la directive SRI doivent être adoptées d'ici mai 2018, le résultat sera probablement le développement d'une Europe à plusieurs vitesses, où l'efficacité des CSIRT nationaux risque de varier d'un pays à l'autre. Cette situation sera porteuse de dangers, dans la mesure où les pays qui ne disposeront pas d'un CSIRT suffisamment contraignant deviendront des maillons faibles, fragilisant l'ensemble du réseau européen. Dès à présent, des différences importantes sont apparues entre les États membres au niveau de la mise en application des normes de cybersécurité[20]. Enfin, il y a aussi une dimension économique, dans la mesure où tout retard de l'UE en

18. Une autre différence notable entre l'UE et les États-Unis est que l'ENISA est une institution publique, alors que la NERC est une organisation privée sous la supervision d'une agence fédérale publique (la FERC).

19. ENISA, *Statement of Estimates 2017* (Budget 2017), 2017. ENISA, *Multi-Annual Staff Policy Plan 2016-2018*, octobre 2015. En outre, le paquet sur la cybersécurité proposé par la Commission en septembre 2017 prévoit de renforcer les moyens de l'ENISA, notamment en doublant son budget à 22 millions d'euros et en augmentant les effectifs à 120 personnes d'ici 2021. Bien que ces mesures soient positives, elles demeurent insuffisantes, surtout par rapport aux moyens financiers et logistiques de la NERC américaine, qui continuent d'augmenter de façon régulière.

20. Selon l'étude de la société Software Alliance (BSA), même si la plupart des États membres ont déjà mis en place un CSIRT national, certains tels que Chypre et l'Irlande n'ont toujours pas établi de plateforme pour la centralisation des rapports et des données concernant les incidents de cybersécurité. En outre, une majorité de pays européens, y compris la Belgique, la Finlande, l'Irlande et la Slovénie, n'ont pas réussi, pour l'instant, à développer une structure nationale de gestion des incidents ayant les capacités de répondre aux incidents de cybersécurité. Voir : BSA/The Software Alliance, *Tableau de bord de la cybersécurité dans l'UE : Vers un cyberespace europe´en sécurise´*, janvier 2015.

matière de cybersécurité risque de diminuer la compétitivité des entreprises européennes spécialisées par rapport aux entreprises américaines, avec des pertes potentiellement significatives.

Bien qu'il soit difficile de recréer en Europe une organisation comme la NERC américaine, l'UE peut néanmoins s'en inspirer pour renforcer les institutions actuelles, ou en créer de nouvelles avec plus de compétences. Le principal obstacle a été la réticence d'un certain nombre d'États membres de partager des informations sensibles avec d'autres pays européens. Néanmoins, les récentes cyberattaques en Ukraine, qui se sont propagées à de nombreux États membres et ont causé d'importants dégâts, soulignent le danger majeur que représentent les maillons faibles. Par conséquent, il serait bénéfique soit de créer un CSIRT principal au niveau de l'UE ayant les pouvoirs nécessaires pour coordonner les CSIRT nationaux, soit de renforcer les moyens (budgétaires et humains) et les compétences de l'ENISA. Cela inclurait notamment la possibilité d'imposer des amendes au niveau européen en cas de non-respect des règles, la notification des incidents et un meilleur échange d'informations entre les acteurs publics et privés, ainsi que la mise en place d'inspections régulières dans les États membres (des compétences que l'UE a déjà acquises dans d'autres domaines).

En outre, si les États membres refusaient de transférer ce genre de pouvoir, il serait toujours possible pour l'ENISA ou le réseau CSIRT de développer un système de cyber alerte au niveau de l'UE pour les entreprises et les institutions du secteur de l'énergie, sur le modèle des *NERC Alerts*. Bien que l'UE ait déjà mis en place une institution de ce type (CERT-EU), celle-ci travaille principalement en relation avec les autres institutions et agences européennes. Le CERT-EU ne se focalise pas sur le secteur de l'énergie, et ne possède pas le même type de contact direct et régulier avec l'ensemble des fournisseurs d'électricité et entreprises du secteur comme la NERC américaine. Pour les pays européens, cela n'impliquerait pas de transfert de souveraineté et pourrait contribuer à renforcer l'harmonisation des normes et l'échange d'informations entre les CSIRT nationaux. En outre, même si l'ENISA organise aussi tous les deux ans des exercices de cybersécurité, ceux-ci sont moins développés que le GridEx américain et ne se concentrent pas spécifiquement sur le domaine de l'énergie. Le quatrième et dernier exercice de cybersécurité organisé par l'ENISA, « Cyber Europe 2016 », s'est tenu en avril et en octobre 2016. Il a rassemblé à peu près 1 000 participants (bien moins que les 7 000 participants du GridEx IV) issus de différents secteurs, notamment les opérateurs de télécommunication, les sociétés de TIC et les entreprises de l'énergie[21].

21. ENISA, *Cyber Europe 2016: After Action Report*, juin 2017, disponible sur : www.enisa.europa.eu.

Une possibilité serait que l'UE participe de façon régulière au GridEx afin de bénéficier de l'expérience des méthodes américaines, permettant d'améliorer les exercices de cybersécurité en Europe. De plus, l'ENISA pourrait aussi élargir ses exercices de cybersécurité pour y inclure les pays limitrophes à l'UE membres de la Communauté de l'énergie, notamment l'Ukraine, qui sont reliés au marché intérieur européen de l'énergie[22].

Comparaison de la mise en application des normes de cybersécurité aux États-Unis et dans l'UE (couleur bleu pour l'UE, et blanc pour les États-Unis)

Institution ou compétence	Rôle et objectif
Amendes de la NERC	La NERC peut imposer des amendes pouvant atteindre jusqu'à un million de dollars par jour jusqu'à la mise aux normes.
Équipes d'intervention de la NERC	La NERC envoie des équipes d'intervention pour inspecter un certain nombre de *utilities* chaque année afin de vérifier la mise en application des normes.
NERC Alerts	La NERC a un système d'alerte qui permet d'informer de manière synchronisée l'ensemble des *utilities* d'un risque cyber imminent.
Grid Security Conference	La NERC tient chaque année une conférence qui rassemble les experts de la cybersécurité issus du secteur public et de l'industrie pour l'échange d'informations techniques.
Grid Security and Emergency Response Exercise	La NERC organise tous les deux ans un exercice de grande ampleur qui simule une cyberattaque sur le réseau électrique en collaboration avec les institutions fédérales, locales et le secteur privé.
ENISA	Son rôle est de conseiller les États membres, recueillir et analyser des données, promouvoir des méthodes de gestion des risques, ainsi que favoriser l'échange de bonnes pratiques.

22. Commission européenne, *Energy Community*, disponible sur : https://ec.europa.eu.

CSIRT nationaux	Centre d'alerte pour chaque État membre, dont la mission est de veiller à ce que les « opérateurs de services essentiels » respectent les standards de cybersécurité.
Réseau CSIRT	Sa mission est de développer la confiance entre les États membres afin d'encourager le partage d'informations et la coopération entre les CSIRT nationaux.
Groupe de coopération	Sa fonction est de renforcer la collaboration entre les États membres et la Commission européenne au niveau de la cybersécurité.
Exercice Cyber Europe	L'ENISA organise tous les deux ans des exercices de cybersécurité qui rassemblent des participants issus de différents secteurs, notamment celui de l'énergie.

Le modèle californien de cybersécurité

La Californie est probablement l'État américain le plus avancé en matière de cybersécurité. L'UE pourrait tirer quelques enseignements du modèle californien, surtout en ce qui concerne l'application de la directive SRI, qui prévoit notamment que chaque État membre mette en place un centre d'alerte national pour la cybersécurité (CSIRT). En Californie, le gouverneur Jerry Brown a pris l'initiative en août 2015 de créer la *Cyber Security Integration Center* (Cal-CSIC), qui a la même fonction que les CSIRT européens au niveau de la gestion et de la prévention des incidents de cybersécurité sur les infrastructures critiques. Néanmoins, la Cal-CSIC possède aussi des compétences dans d'autres domaines, traduisant une approche exhaustive de la cybersécurité dont pourraient s'inspirer les CSIRT européens. En effet, le mandat de la Cal-CSIC couvre notamment le développement de nouvelles technologies et systèmes numériques pour renforcer les mécanismes de cyberdéfense. Cela inclut un soutien pour la recherche scientifique et technique, ainsi qu'un partenariat étroit avec le secteur privé pour identifier les meilleures technologies et logiciels informatiques. De plus, la Cal-CSIC est aussi chargée de vérifier la protection de la vie privée et les données à caractère personnel du consommateur en lien avec les nouvelles technologies numériques, notamment les compteurs communicants. Au sein de l'UE, ces fonctions sont réparties entre différents secteurs avec une multitude d'institutions compétentes. Les États membres ont des institutions spécifiques pour veiller à la protection de la vie privée ;

par exemple, la France a mis en place la Commission nationale de l'informatique et des libertés (CNIL). En outre, c'est notamment la Commission européenne qui soutient la recherche scientifique et technique dans ce domaine avec le programme Horizon 2020. Néanmoins, cet émiettement des compétences risque d'empêcher une coordination efficace dans des domaines étroitement interconnectés. Ainsi, l'approche exhaustive de la Cal-CSIC en matière de cybersécurité pourrait inspirer un renforcement de la centralisation des différentes institutions au sein des pays européens, avec par exemple une meilleure collaboration entre la CNIL et le CSIRT dans un pays comme la France.

Un deuxième point sur lequel la Californie pourrait servir de modèle pour l'UE concerne la protection de la vie privée dans le secteur de l'énergie. Le Règlement général sur la protection des données (RGPD), adopté en avril 2016, représente la principale avancée européenne en matière de protection des données à caractère personnel. Le RGPD a une portée générale, donc il s'applique à la plupart des secteurs, notamment celui de l'énergie. La particularité de la Californie est qu'elle dispose de lois conçues pour protéger les données à caractère personnel spécifiquement dans le secteur de l'énergie, y compris au niveau des compteurs communicants. Par exemple, la *Privacy for Customer Electrical or Natural Gas Usage Data Law*[23] est entrée en vigueur en janvier 2014. Cette loi interdit à toute entreprise privée de partager ou de divulguer les informations d'un individu concernant sa consommation d'électricité ou de gaz naturel sans avoir obtenu son consentement explicite[24]. Elle comprend aussi des clauses spécifiques sur les compteurs communicants, et impose des règles strictes pour les entreprises qui gèrent ce type de technologie. Cela inclut l'obligation d'utiliser des procédés de cybersécurité avancés pour protéger les données collectées par les compteurs, notamment le cryptage systématique des données à caractère personnel. En revanche, même si le RGPD européen met en place des mesures concrètes et ambitieuses dans ce domaine, il ne comprend pas de clauses spécifiques pour le secteur de l'énergie. Selon l'une des personnes interrogées, la généralité du RGPD pourrait nuire à sa capacité à protéger les données à caractère personnel en ce qui concerne les compteurs communicants. En effet, la technicité de ces nouvelles technologies numériques et les risques importants qu'elles introduisent en matière de cybersécurité rendent nécessaire une législation qui leur soit propre afin de garantir une protection adéquate de la vie privée des individus.

23. *California Legislative Information*, « AB-1274 Privacy: Customer Electrical or Natural Gas Usage Data », octobre 2013, disponible sur : https://leginfo.legislature.ca.gov.
24. Elle contraint aussi les entreprises de l'énergie à faire connaître au consommateur comment leurs données personnelles sont traitées et à qui elles ont été transmises, les obligeant à mettre en place des mesures pour empêcher le vol ou le piratage des données.

Ce que la France peut apprendre du modèle américain

La France est un pays relativement avancé au niveau de la cybersécurité, même en comparaison avec les États-Unis. Le *Livre blanc sur la défense et la sécurité nationale* de 2008 a permis la mise en place d'une structure autonome pour assurer la cybersécurité des systèmes d'information. Créée en 2009, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) est aujourd'hui parmi les agences les plus développées, avec un budget d'environ 80 millions d'euros (sensiblement supérieur à celui de la NERC qui s'élève à presque 70 millions de dollars[25]). Ses missions ont été définies autour de plusieurs axes stratégiques, notamment la détection des attaques informatiques, la prévention des menaces, le conseil aux administrations et aux opérateurs, ainsi que l'information régulière des entreprises et du public sur les enjeux cyber. Ses compétences ont été renforcées avec la mise en application de la « stratégie de la France en matière de défense et de sécurité des systèmes d'information » de 2011[26]. En outre, le *Livre blanc sur la défense et la sécurité nationale* de 2013 souligne la nécessité de prendre en compte la cybersécurité des opérateurs d'importance vitale (OIV). La Loi de programmation militaire (LPM), adoptée en 2013, a posé les bases juridiques d'une politique de cybersécurité française en fixant des règles strictes pour plus de 200 entités identifiées comme constituant des OIV[27]. Bien que la liste détaillée soit classifiée[28], il s'agit principalement d'entreprises, d'usines, d'opérateurs et d'institutions « pour lesquels l'atteinte à la sécurité ou au fonctionnement risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la survie de la Nation[29] ».

De plus, le décret de 2015 relatif à la sécurité des systèmes d'information des OIV a permis de préciser les règles concernant la détection des incidents cyber, les modalités de déclaration de ces incidents, ainsi que les dispositions de protection nécessaires pour prévenir les menaces[30].

25. Cela est dû en partie au fait que la NERC se concentre seulement sur le secteur de l'énergie, alors que l'ANSSI a un mandat beaucoup plus large qui couvre la sécurité de tous les systèmes d'information, ce qui nécessite un budget plus important.
26. ANSSI, « Stratégie de la France : défense et sécurité des systèmes d'information », 2011, disponible sur : www.ssi.gouv.fr.
27. Loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale, disponible sur : www.legifrance.gouv.fr.
28. La liste des OIV avait au préalable été établie par le Décret n° 2006-212 du 23 février 2006, relatif à la sécurité des activités d'importance vitale, disponible sur : www.legifrance.gouv.fr.
29. Article L1332-6-1 du code de la défense.
30. Décret n° 2015-351 du 27 mars 2015 relatif à la sécurité des systèmes d'information des opérateurs d'importance vitale, disponible sur : www.legifrance.gouv.fr.

Ce dispositif ambitieux fut complété par une version révisée de la « stratégie de cybersécurité nationale », présentée par l'ANSSI à l'automne 2015[31]. Par ailleurs, la France a aussi été le premier pays à publier en août 2016 des arrêtés sectoriels pour les OIV, contenant une liste de mesures précises, détaillées et obligatoires pour les entreprises afin de protéger leurs systèmes d'information[32]. Les arrêtés sectoriels comprennent des mesures adaptées au contexte spécifique des différents secteurs, notamment celui de l'énergie, avec des règles strictes pour les OIV concernant les hydrocarbures[33], le gaz[34] et l'électricité[35]. Cela inclut par exemple l'obligation pour les entreprises de fournir sous trois mois à l'ANSSI une liste de leurs systèmes d'information d'importance vitale (SIIV), la mise en place d'une politique de sécurité des systèmes d'information (PSSI), la cartographie des systèmes existants, ainsi que le devoir de planifier toute nouvelle mise à jour d'un logiciel.

Le détail et la précision de ces mesures sont comparables à celles contenues dans les NERC-CIPs américains, ainsi que dans les différents ordres exécutifs et *Presidential Policy Directives*. En outre, l'ANSSI dispose aussi de pouvoirs contraignants comparables à ceux de la NERC américaine afin de vérifier la mise en application des normes de cybersécurité. Cela inclut la possibilité pour l'ANSSI d'imposer aux OIV qui ne respectent pas les règles des amendes pouvant atteindre 150 000 euros pour les personnes physiques et 750 000 euros pour les personnes morales. De plus, l'ANSSI organise aussi des contrôles techniques et des inspections régulières au sein des OIV, et a mis en place un système d'alerte avec l'obligation pour les OIV de notifier l'ANSSI sans délai de tout incident relatif à la cybersécurité. Cependant, contrairement à la France, les États-Unis disposent d'une agence spécialisée pour le secteur de l'énergie, puisque le mandat de la NERC se focalise sur le *Bulk Power System* (entités de production et de transmission électrique[36]). En revanche, la mission de l'ANSSI est bien plus large car elle doit assurer la sécurité de tous les systèmes d'information, notamment ceux du secteur de l'énergie[37].

31. ANSSI, « Stratégie nationale pour la sécurité du numérique », 2015, disponible sur : www.ssi.gouv.fr.
32. ANSSI, « Cybersécurité des OIV : publication d'une nouvelle vague d'arrêtés sectoriels », 2016, disponible sur : www.ssi.gouv.fr.
33. Arrêté du 11 août 2016 fixant les règles de sécurité et les modalités de déclaration des systèmes d'information d'importance vitale et des incidents de sécurité relatives au sous-secteur d'activités d'importance vitale « Approvisionnement en hydrocarbures », 2016, disponible sur : www.legifrance.gouv.fr.
34. *Ibid.*
35. *Ibid.*
36. Une autre différence entre la France et les États-Unis est le fait que l'ANSSI, comme l'ENISA au niveau européen, est une institution publique, alors que la NERC est une organisation privée sous la supervision d'une agence fédérale publique (la FERC).
37. En effet, l'ANSSI dispose d'un responsable pour la coordination sectorielle énergie et nucléaire, mais pas d'une agence spécialisée comme la NERC américaine.

Ainsi, l'avantage du modèle américain est que la NERC peut se concentrer sur la cybersécurité des entreprises de l'énergie, et donc apporter des réponses potentiellement plus adaptées, spécialisées et plus rapides que l'ANSSI. En effet, l'énergie représente un secteur avec un certain nombre de spécificités, méritant des règles et des institutions qui lui soient propres afin de mieux faire face aux cyberattaques. Par conséquent, la France pourrait s'inspirer de la NERC américaine pour mettre en place une nouvelle structure rattachée à l'ANSSI, ou bien une sous-direction à l'intérieur de celle-ci, spécialisée dans le secteur de l'énergie. L'objectif serait de développer un contact direct et régulier avec l'ensemble des fournisseurs d'électricité, les entreprises et autres acteurs du secteur de l'énergie en France, sur le modèle de la NERC américaine. Cela permettrait un échange d'informations approfondi, contribuant à l'introduction de mesures de cybersécurité plus adaptées aux spécificités du secteur de l'énergie. De plus, il serait pertinent de mettre en place un système d'alerte spécialisé pour les fournisseurs d'électricité basé sur les *NERC Alerts* aux États-Unis, permettant une réaction plus rapide et mieux synchronisée des entreprises et acteurs du secteur de l'énergie en cas de cyberattaque.

Regards croisés : ce que les États-Unis peuvent apprendre de l'Europe

La protection du réseau de distribution électrique

Une différence importante entre l'UE et les États-Unis concerne la protection du réseau de distribution électrique. Bien qu'il se présente sous différentes configurations, le réseau électrique traditionnel démarre en règle générale par la production d'électricité, suivi par le transport, et se termine par la distribution à l'échelle du consommateur. Aux États-Unis, même les dernières versions 5 et 6 des NIRC-CIPs, ainsi que les différents ordres exécutifs et *Presidential Policy Directives* sur ce sujet, ne protègent pas le réseau au niveau de la distribution d'électricité, cette responsabilité étant laissée aux États américains. Ces derniers ont été très réticents à toute réglementation fédérale et ont résisté avec succès aux efforts de la NERC d'établir des normes de sécurité à cette échelle. Malgré cela, peu d'États ont pris leurs responsabilités dans ce domaine. Pour l'année 2015 par exemple, seulement cinq États ont passé des lois pour renforcer la cybersécurité du réseau de distribution électrique, avec la Californie une nouvelle fois comme chef de file[38]. Cela représente une faille majeure dans la sécurité du réseau électrique américain. En effet, les millions de compteurs communicants qui vont être installés aux États-Unis dans les années à venir appartiennent au réseau de distribution électrique, et ne sont pas couverts par les NERC-CIPs. En plus des vulnérabilités au niveau de la protection de la vie privée et des données à caractère personnel, les nouveaux compteurs communicants exposent aussi les consommateurs à des risques importants liés aux dégâts physiques et matériels que pourrait causer un logiciel malveillant. Il est donc important de modifier la réglementation américaine, et les États-Unis pourraient notamment s'inspirer de la législation européenne en la matière. En outre, la directive SRI est explicite sur le fait que le réseau de distribution électrique est inclus dans la définition « d'opérateur de services essentiels »

38. Voir D. Shea, « State Efforts to Protect the Electric Grid », *National Conference of State Legislatures*, 2016, disponible sur : www.ncsl.org.

et doit donc être couvert par les mesures de cybersécurité mises en place[39]. Cela comprend un cadre de prévision et de gestion des cybermenaces régi par les CSIRT pour protéger le réseau de distribution électrique.

La cybersécurité des énergies renouvelables et des technologies bas-carbone

Un autre sujet sur lequel les États-Unis peuvent tirer des enseignements de l'UE concerne la cybersécurité des énergies renouvelables et des technologies bas-carbone. Les infrastructures des énergies renouvelables sont particulièrement vulnérables aux cyberattaques, notamment en raison de l'intermittence du solaire ou de l'éolien, nécessitant des technologies numériques avancées pour le pilotage à distance, l'intégration aux réseaux et, de plus en plus, pour le stockage. En 2013, un groupe de hackers dénommé *Dragonfly* a exploité ces vulnérabilités pour introduire des logiciels malveillants au sein de plusieurs entreprises d'énergies renouvelables aux États-Unis et en Europe (notamment en Allemagne), infectant les systèmes de contrôle industriels des infrastructures. Bien que les virus aient été conçus principalement à des fins d'espionnage industriel, les analyses ont permis de démontrer qu'ils avaient aussi la capacité de prendre le contrôle physique des infrastructures, causant potentiellement des dégâts majeurs[40].

Alors que sous la présidence de Barack Obama, le *Clean Power Plan*[41] de 2015 ne prévoyait pas d'inclure de mesures spécifiques pour la cybersécurité, le président Trump a signé le 28 mars 2017 un ordre exécutif pour abroger ce projet de loi, et le climato-scepticisme du parti républicain empêchera vraisemblablement toute législation fédérale sur ce sujet tant qu'il sera au pouvoir. Cependant, même dans les États américains ayant annoncé vouloir continuer à mettre en place leurs politiques climatiques, notamment la Californie et les États de la côte Est, la cybersécurité n'est que rarement intégrée dans les stratégies de transition énergétique. Cela est dû en grande partie à la réticence des entreprises américaines à investir dans ce domaine. En effet, un excès de sécurité a été perçu par nombre de constructeurs comme pouvant mettre à mal l'innovation et l'efficacité des

39. Cela est même précisé dans l'Annexe II de la directive (sous-partie 1 – a), qui mentionne les « gestionnaires de réseau de distribution » comme type d'entité couvert dans le sous-secteur de l'électricité.

40. M. Ruhle et L. Trakimavicius, « Cyberattacks Are the New Challenge for Renewable Energy », Politico, 23 juillet 2017, disponible sur : www.politico.eu.

41. L'objectif de ce projet de loi était d'augmenter la part des énergies renouvelables et les technologies propres dans l'économie américaine à l'horizon 2025.

équipements, ce qui risquerait de réduire les marges de manœuvre et les profits. Selon l'une des personnes interrogées, de nombreux constructeurs de voitures électriques aux États-Unis craignent que des procédures de cybersécurité telles que la réinitialisation régulière des mots de passe ne crée un environnement trop complexe pour les usagers. À l'inverse, l'UE a commencé à intégrer la cybersécurité dans ses politiques de transition énergétique. Le « paquet d'hiver » présenté par la Commission européenne en novembre 2016 et intitulé « Propositions législatives en vue d'une énergie propre pour tous les Européens » fait explicitement référence au domaine de la cybersécurité. Ce « paquet d'hiver » souligne le besoin d'intégrer des dispositions précises pour protéger la transition énergétique en Europe contre les cyberattaques. Cela inclut par exemple l'obligation pour chaque nouvelle technologie verte d'identifier les menaces cyber potentielles, ainsi que la création de règles techniques dont un « code de réseau » sur la cybersécurité afin de protéger les infrastructures de production d'énergies renouvelables. Ce type de mesure est facilement transposable aux États-Unis, et les États américains qui souhaitent poursuivre la transition énergétique pourraient s'en inspirer.

La protection de la vie privée et des données à caractère personnel

La cybersécurité concerne non seulement les logiciels malveillants pouvant causer des dégâts matériels et physiques, mais aussi le vol ou le piratage de données à des fins lucratives ou d'espionnage. La numérisation des systèmes énergétiques expose de plus en plus les consommateurs au vol de leurs données, violant leurs droits fondamentaux liés à la protection de la vie privée. Cette menace risque d'augmenter dans les années à venir en raison du déploiement à grande échelle de millions de compteurs communicants dans l'UE et aux États-Unis. Censés entre autres aider à rationaliser la consommation d'énergie et permettre de faire des économies, ces nouveaux compteurs numériques exposent aussi les consommateurs à un risque accru de piratage de leurs données personnelles[42]. Il est important de faire la distinction entre la protection de la vie privée en amont, qui consiste à empêcher dès le début la collecte excessive de données à caractère personnel, et la protection des données an aval, qui concerne les règles de gestion de ces données une fois qu'elles ont été collectées. Concernant la protection de la vie privée en amont, la législation fédérale américaine n'a pas pour l'instant été en mesure de faire passer de lois dans ce domaine,

42. En raison de leur dépendance à Internet, chaque compteur communicant représente un point d'entrée potentiel pour un logiciel malveillant, qui peut ensuite se répandre à l'ensemble du réseau électrique.

en grande partie à cause de puissants lobbies qui ont réussi à bloquer les efforts du Congrès. Par conséquent, la responsabilité a été laissée aux États américains, mais mis à part la Californie comme chef de file ainsi que quelques autres États, la plupart n'ont pas fait passer de lois en la matière. En ce qui concerne la protection des données à caractère personnel en aval, certaines lois ont été approuvées par le Congrès américain, mais elles ont tendance à avantager les entreprises de l'énergie plutôt que l'individu, ce qui est le cas notamment du *Cybersecurity Information Sharing Act* (CISA), ratifié par le Congrès en 2015[43].

En revanche, l'UE a réussi à mettre en place l'une des législations les plus avancées du monde en matière de protection de la vie privée en amont, tout comme pour la gestion des données à caractère personnel en aval. Adopté en avril 2016[44], le règlement général sur la protection des données (RGPD) contient une série de mesures efficaces pour renforcer les droits des individus. Cela inclut une référence explicite au droit à l'oubli dans le cas où les données personnelles ont été rendues publiques sur le web, ainsi qu'un accès direct aux informations concernant la manière dont les données personnelles ont été traitées. De plus, le RGPD prévoit un droit à la portabilité afin de faciliter la transmission des données entre les opérateurs, un renforcement de la notion explicite du consentement pour le traitement des données, ainsi qu'une augmentation des amendes et des pouvoirs de sanction pour les autorités de régulation compétentes. Enfin, le RGPD impose aussi aux acteurs concernés de mener des analyses régulières concernant l'impact de leurs activités sur la protection des données du consommateur. Par conséquent, la Commission européenne a mis au point un « modèle d'analyse d'impact sur la protection des données des réseaux intelligents et des systèmes intelligents de mesure », en coopération avec le secteur privé[45]. Après une première phase lancée dès 2014, ce cadre permet aux entreprises de planifier leurs investissements dans les réseaux

43. En effet, l'objectif du *Cybersecurity Information Sharing Act* (CISA) est d'assurer la sécurité des données des entreprises qui acceptent d'échanger des informations avec le gouvernement fédéral à travers la création de *safe harbors* qui protègent contre toute procédure judiciaire. Néanmoins, le problème est que ce sont précisément les consommateurs qui sont les plus susceptibles de lancer de telles poursuites contre les entreprises afin de s'assurer de la protection de leurs données personnelles, ce qui ne fait qu'aggraver la violation de la vie privée des individus.

44. Le RGPD remplace la Directive de 1995 sur la protection des données afin d'offrir aux consommateurs plus de contrôle et un meilleur accès à leurs données personnelles, ainsi que des dispositions pour protéger les données des citoyens européens partout dans le monde, y compris en dehors de l'UE. Voir : Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, disponible sur : http://eur-lex.europa.eu.

45. Recommandation de la Commission européenne concernant le modèle d'analyse d'impact sur la protection des données des réseaux intelligents et des systèmes intelligents de mesure, 10 octobre 2014, disponible sur : http://eur-lex.europa.eu.

intelligents en anticipant dès le début les risques liés à la protection des données.

Il n'y a pas d'équivalent à l'échelle nationale aux États-Unis. En raison de la pression des lobbies qui bloquent l'action du Congrès sur ce sujet, il sera probablement difficile de mettre en place une législation fédérale du même type que le RGPD européen, au moins dans un avenir proche. Par conséquent, ce sont les États américains qui devront agir dans ce domaine, puisque les blocages sont moins importants à l'échelle locale. Les États qui ont déjà mis en place certaines règles en la matière, ainsi que ceux qui souhaiteraient le faire, pourraient donc s'inspirer de la législation européenne pour développer la protection de la vie privée du consommateur. En outre, depuis le 12 juillet 2016, un bouclier de protection des données UE-États-Unis (*EU-US Privacy Shield*) a été mis en place afin de renforcer la protection des données personnelles dans les échanges commerciaux transatlantiques. Ce dispositif contient une série de mesures pour que les entreprises des deux côtés de l'Atlantique respectent la législation européenne en matière de protection des données personnelles lors des transactions commerciales. Bien que les entreprises américaines n'aient pas l'obligation d'adhérer au bouclier de protection des données, une fois qu'elles ont officiellement fait ce choix, elles doivent rendre des comptes devant la justice américaine[46]. De plus, les entreprises européennes ont tendance à passer des accords commerciaux en priorité avec les entreprises américaines qui font partie du bouclier de protection des données. Cela signifie que les entreprises américaines sont sous pression de se conformer aux règles européennes en matière de protection des données si elles veulent avoir accès au marché européen. Étant donné que l'UE est le premier partenaire commercial des États-Unis, le bouclier de protection des données représente un outil efficace pour que les normes européennes concernant la protection des données personnelles puissent se répandre sur le sol américain, malgré l'absence d'une législation fédérale. Cela a un impact direct sur le secteur de l'énergie, compte tenu de la numérisation croissante du réseau électrique, avec de nombreux échanges commerciaux concernant l'installation des compteurs communicants en Europe comme aux États-Unis dans les années à venir.

46. US Department of Commerce, *Overview of the EU-US Privacy Shield*, 12 juillet 2016, disponible sur : www.commerce.gov.

Ce que les États-Unis peuvent apprendre du modèle français

Un sujet important où la France est relativement avancée par rapport aux États-Unis concerne la protection de la vie privée et des données à caractère personnel. En effet, la France possède ses propres institutions nationales compétentes dans ce domaine, avec notamment la Commission nationale de l'informatique et des libertés (CNIL). Créée en 1978, cette institution est chargée d'assurer que les technologies de l'informatique soient au service du citoyen afin de ne pas nuire aux droits de l'homme, à l'identité humaine, ainsi qu'à la protection de la vie privée et des libertés individuelles ou publiques. Le mandat de la CNIL est défini par la loi du 6 janvier 1978, modifiée le 6 août 2004, relative à l'informatique, aux fichiers et aux libertés. Bien qu'il existe d'autres institutions similaires en Europe, la CNIL est considérée comme l'une des plus actives, et il n'y a surtout aucun équivalent aux États-Unis. En effet, la seule institution fédérale américaine dans ce domaine est le *Privacy Office of the U.S. Department of Homeland Security*, créé en 2002, censé avoir un mandat pour agir au niveau de la protection des données à caractère personnel. Néanmoins, le problème est que ce *Privacy Office* est subordonné aux exigences du *Department of Homeland Security,* dont la priorité est avant tout d'assurer la sécurité nationale. De plus, l'absence d'une législation fédérale américaine pour la protection de la vie privée en amont, ainsi que l'insuffisance des mesures concernant les données à caractère personnel en aval, limite considérablement la marge d'action possible du *Privacy Office*.

À l'inverse, la CNIL constitue une autorité administrative indépendante de tout organisme public ou privé, dont la neutralité est garantie par sa composition et son organisation. Le président de la CNIL est élu librement parmi ses membres et ne reçoit d'instruction d'aucune autorité, aucun ministre ou chef d'entreprise ne pouvant s'opposer à son action[47]. En outre, la CNIL peut aussi s'appuyer sur une législation européenne et française très étendue au niveau de la protection de la vie privée, ce qui lui confère une base juridique solide pour pouvoir mener à bien sa mission. Par conséquent, la CNIL possède un mandat bien plus étendu que son homologue américain, ce qui inclut notamment un travail pour informer, protéger, accompagner et conseiller les entités à la fois publiques et privées, ainsi que le pouvoir de contrôler et sanctionner si besoin toute violation des libertés. La CNIL est aussi chargée d'anticiper les risques liés aux nouvelles technologies numériques, disposant notamment d'un laboratoire pour expérimenter des

47. La CNIL en France – *Le fonctionnement*, disponible sur : www.cnil.fr.

produits ou des applications innovantes[48]. Même si les États-Unis sont sujets à des blocages au niveau fédéral dans ce domaine en raison de la pression exercée par de puissants lobbies, ils pourraient tout de même tirer quelques enseignements du fonctionnement de la CNIL. En outre, le niveau local est moins contraint par ce type de blocages. Ainsi, les États américains qui ont déjà mis en place certaines règles en la matière, ainsi que ceux qui souhaiteraient le faire, pourraient s'inspirer de la CNIL à propos de la protection de la vie privée et des données à caractère personnel.

48. La CNIL en France - *Les missions*, disponible sur : www.cnil.fr.

Renforcer la coopération transatlantique pour développer des standards communs

L'UE et les États-Unis ont des approches très différentes en ce qui concerne la cybersécurité des infrastructures énergétiques. D'un côté, la stratégie américaine privilégie la sécurité en profondeur avec des réglementations strictes et détaillées dans des secteurs précis, avec des institutions ayant des pouvoirs contraignants pour les appliquer. De l'autre côté, la stratégie européenne est plus souple et générale, privilégiant la protection d'une large panoplie de différents secteurs tels que le réseau de distribution électrique, les technologies bas-carbone et les données à caractère personnel. Ainsi, il apparaît que les approches européennes et américaines sont complémentaires, avec un fort potentiel de collaboration. Par conséquent, il serait avantageux de développer une coopération transatlantique plus approfondie au niveau de la cybersécurité, permettant à chacun d'apprendre du modèle de l'autre en renforçant le dialogue et l'échange d'informations. À la suite de l'élection de Donald Trump, les relations transatlantiques sont entrées dans une période d'incertitude[49]. Néanmoins, le président Trump a démontré un intérêt notable pour les questions de cybersécurité en renforçant les mesures prises par son prédécesseur en la matière.

De ce fait, malgré des désaccords sur de nombreux sujets, la cybersécurité représente un domaine où il existe une réelle opportunité pour approfondir la coopération transatlantique au cours des prochaines années. Cela serait bénéfique pour les deux parties, étant donné la complémentarité de leurs approches respectives. Par ailleurs, un partenariat transatlantique renforcé permettrait de construire des standards internationaux communs pour la cybersécurité parmi les plus avancés au monde, pouvant servir d'exemple pour des pays moins avancés en la matière. En raison de la mondialisation des technologies numériques, une cyberattaque dans un pays apparemment éloigné peut se répandre et affecter les réseaux en Europe et aux États-Unis. C'est précisément ce qui s'est passé récemment

49. T. Gomart (dir.), « Trump, un an après. Un monde à l'état de nature ? », *Études de l'Ifri*, Ifri, novembre 2017, disponible sur : www.ifri.org.

avec le virus *NotPetya*, qui s'est propagé à beaucoup d'entreprises occidentales entretenant des relations commerciales avec l'Ukraine, notamment par le biais de leurs filiales dispersées dans de nombreux pays. Par conséquent, une meilleure coopération transatlantique permettant le développement de normes internationales rigoureuses pourrait contribuer à réduire les risques de contagion.

La coopération transatlantique bilatérale

La coopération transatlantique bilatérale entre gouvernements représente le moyen le plus direct et l'un des plus efficaces pour le développement de standards communs. Un sommet annuel UE/États-Unis est organisé depuis 1991 afin d'approfondir la coopération dans de nombreux domaines. Au cours des dernières années, les enjeux liés au secteur énergétique et à la cybersécurité sont devenus plus importants, et plusieurs plateformes de haut niveau ont été créées spécifiquement dans ces domaines. Cela inclut le Conseil de l'énergie UE/États-Unis depuis 2009, le dialogue UE/États-Unis sur le cyberespace depuis 2014, le groupe de travail UE/États-Unis sur la cybersécurité et la cybercriminalité depuis 2010, ainsi que le *Information Society Dialogue* depuis 2002. Néanmoins, bien que ces quatre plateformes permettent aux États-Unis et à l'UE de collaborer de façon concrète, aucune ne se focalise spécifiquement sur la cybersécurité dans les infrastructures énergétiques, même si elles travaillent sur d'autres sujets qui sont analogues. Par conséquent, une solution serait de créer une nouvelle plateforme transatlantique dédiée spécifiquement à ce sujet, qui pourrait prendre la forme d'un sommet annuel au niveau ministériel afin d'encourager le développement de normes communes. Une autre solution plus facilement réalisable serait de créer de nouveaux groupes de travail au sein des quatre plateformes déjà existantes, qui se concentreraient de manière spécifique sur la cybersécurité dans les infrastructures énergétiques. L'objectif serait d'encourager ces différents groupes de travail à collaborer en instaurant un dialogue et un partage d'informations régulier.

Par exemple, lors du septième Conseil de l'énergie UE/États-Unis de mai 2016, une déclaration commune a fait état de la volonté des deux partenaires de renforcer leur coopération concernant les nouvelles technologies numériques. Cela comprend notamment les compteurs communicants, un domaine où la cybersécurité joue un rôle essentiel[50].

50. De plus, il existe déjà un partenariat entre la FERC américaine et la Direction générale de l'énergie de la Commission européenne dans le cadre du Conseil de l'énergie UE/États-Unis. Bien que celui-ci se concentre sur la régulation des marchés de l'énergie, son mandat pourrait être étendu pour couvrir les enjeux de cybersécurité, qui ont un impact direct sur les marchés énergétiques. Voir : 7th US-EU Energy

De façon similaire, pendant la troisième réunion du dialogue UE/États-Unis sur le cyberespace en décembre 2016, les deux partenaires ont exprimé le souhait de renforcer leur coopération concernant la cybersécurité des infrastructures critiques[51], avec une forte probabilité d'y inclure le secteur de l'énergie. En outre, le groupe de travail sur la cybersécurité et la cybercriminalité a mis en place de façon régulière un « mois de sensibilisation à la cybersécurité » synchronisé en Europe et aux États-Unis. Celui-ci s'étant jusqu'ici concentré sur les systèmes de contrôle industriels, il y aurait la possibilité d'intégrer les enjeux énergétiques durant les prochains cycles de sensibilisations. Enfin, à l'occasion du quatorzième sommet du *Information Society Dialogue* (ISD) de juin 2016, l'UE et les États-Unis ont affirmé vouloir renforcer leur collaboration au niveau de la protection de la vie privée dans le développement des nouvelles technologies numériques[52]. L'impact des compteurs communicants par rapport à la protection des données dans le réseau électrique mériterait d'occuper une place plus importante lors des prochains sommets de l'ISD. Néanmoins, un certain doute plane actuellement sur le maintien de ces quatre plateformes de coopération transatlantique, en raison de la politique étrangère du président Donald Trump. Il est impératif que l'UE fasse tout son possible pour convaincre l'administration Trump des bénéfices majeurs que peuvent apporter ces structures de dialogue. Des deux côtés de l'Atlantique, les gouvernements font face aux mêmes défis grandissants, qui ne pourront être surmontés qu'en renforçant leur collaboration.

La collaboration transatlantique dans un cadre multilatéral

La coopération transatlantique au niveau bilatéral mérite d'être renforcée par un cadre institutionnel multilatéral. En effet, l'objectif serait que les standards transatlantiques de cybersécurité puissent être partagés afin de devenir des normes internationales rigoureuses. Il existe plusieurs institutions multilatérales dans lesquelles l'UE et les États-Unis collaborent avec d'autres pays sur le sujet de la cybersécurité, notamment l'OTAN[53]. En effet, l'OTAN possède plus d'une décennie d'expérience en la matière, avec le sommet de Prague en 2002 instaurant pour la première fois la

Council, *Joint Statement*, Service européen pour l'action extérieure, mai 2016, disponible sur : https://eeas.europa.eu.

51. *Third meeting of the EU-US Cyber Dialogue*, Service européen pour l'action extérieure, décembre 2016, disponible sur : https://eeas.europa.eu.

52. *Joint Statement of the 14th EU-US Information Society Dialogue*, Commission européenne – Marché unique numérique, juin 2016, disponible sur : https://ec.europa.eu.

53. Malgré des critiques pendant la campagne présidentielle, Trump a depuis réaffirmé son soutien à l'OTAN, soulignant les possibilités de coopération transatlantique au sein de cette institution.

cybersécurité dans l'agenda politique de l'Alliance. En juillet 2016, les Alliés ont reconnu le cyberespace comme constituant une priorité et un secteur d'opérations pour lequel l'OTAN doit se donner les moyens de se défendre aussi efficacement que sur terre, sur mer et dans le domaine aérien. L'OTAN organise chaque année depuis 2010 un exercice de cybersécurité de grande ampleur (*Locked Shield Cyber Exercise*) impliquant de nombreux pays membres qui simulent une cyberattaque massive sur les réseaux informatiques. Le *Locked Shield Cyber Exercise* de 2017 a simulé une cyberattaque sur le réseau électrique, ce qui est encourageant pour la cybersécurité des infrastructures énergétiques à l'avenir[54]. Il est essentiel que ce type d'exercice se répète de façon régulière, car une cyberattaque importante sur le secteur de l'énergie pourrait avoir des conséquences majeures sur le potentiel militaire de l'OTAN. De plus, lors du sommet de Varsovie en 2016, les Alliés ont affirmé que l'amélioration de la cybersécurité des infrastructures critiques devait être une priorité, ce qui inclut par extension le secteur énergétique. En outre, l'OTAN et l'UE ont déjà signé en février 2016 un arrangement technique de coopération en matière de cyberdéfense, concernant notamment l'échange d'informations et des exercices en commun. Cet arrangement pourrait servir de base pour inciter l'OTAN à renforcer ses moyens d'action pour la cybersécurité des infrastructures énergétiques. Par exemple, il serait bénéfique de systématiquement inclure le réseau électrique lors des *Locked Shield Cyber Exercises,* et peut-être aussi intégrer les centrales nucléaires durant les simulations en raison de leur importance stratégique.

Le G7 est une autre institution multilatérale essentielle où l'Europe et les États-Unis collaborent étroitement avec les autres grandes puissances, notamment sur les thématiques de l'énergie et de la cybersécurité. Sur ce point, le sommet du G7 qui s'est tenu au Japon en mai 2016 a débouché sur de nombreuses avancées majeures dans ces domaines. En effet, les chefs d'État et de gouvernement se sont mis d'accord sur une feuille de route développant des standards internationaux communs pour la cybersécurité, notamment au niveau des infrastructures critiques (« Principes et actions du G7 sur le Cyber[55] »). Ils ont aussi créé un nouveau groupe de travail permanent spécialisé sur les questions de cybersécurité (*Ise-Shima Cyber Group*), qui devra travailler en collaboration avec l'autre groupe de travail déjà existant (*G7 Cyber Expert Group*). Ce sommet du G7 au Japon a aussi permis d'organiser une réunion entre les ministres de l'énergie des pays participants, qui se sont mis d'accord sur une série de mesures dans

54. En effet, la priorité de l'OTAN en matière de cybersécurité est pour l'instant de protéger ses propres réseaux, surtout au niveau militaire. Voir : OTAN, *La cyberdéfense*, août 2017, disponible sur : www.nato.int.

55. *G7 Principles and Actions on Cyber,* mai 2016, disponible sur : www.mofa.go.jp.

plusieurs domaines, notamment la cybersécurité (*Initiative on Energy Security for Global Growth*[56]). Cela comprend le secteur du gaz et le réseau électrique, pour lesquels des standards internationaux pour la cybersécurité ont été formulés. Ces avancées furent confirmées lors du sommet du G7 de 2017 en Italie, notamment avec le travail du *Ise-Shima Cyber Group* spécialisé sur la cybersécurité, ainsi que lors de la réunion des ministres de l'Énergie des pays participants à Rome.

Néanmoins, l'une des faiblesses des travaux du G7 est que les déclarations communes sont d'ordre général et ne rentrent pas suffisamment dans le détail, ce qui fait que les standards internationaux risquent de devenir de simples déclarations d'intention. De plus, les responsabilités entre les différents groupes de travail et les réunions ministérielles[57] n'ont pas été clairement délimitées, ce qui créé parfois des redondances et confusions. Enfin, les travaux du G7 pour la cybersécurité se sont focalisés avant tout sur le système financier, avec l'élaboration d'une stratégie commune lors du sommet de 2016[58], qui fut approfondie et renforcée lors du sommet de 2017[59]. Bien que la cybersécurité des infrastructures énergétiques soit abordée lors des réunions du G7 réunissant les ministres de l'énergie des pays participants, elle ne figure pas pour l'instant au rang de priorité. Ainsi, il est essentiel que le G7 assigne une place plus importante à ce sujet, ce qui pourrait prendre la forme d'un nouveau groupe de travail spécialisé sur le sujet, travaillant en collaboration avec les réunions ministérielles de l'énergie. Cela permettrait aussi de clarifier les compétences des différents groupes de travail et d'apporter plus de précisions lors des déclarations communes.

Des partenariats transatlantiques entre les entreprises et les groupes industriels

En Europe comme aux États-Unis, les entreprises privées et les groupes industriels jouent un rôle essentiel dans le développement de standards et de bonnes pratiques en matière de cybersécurité, en collaboration avec le secteur public. Par exemple, un certain nombre de pays européens ont

56. G7 Energy Ministerial Meeting, *Kitakyushu Initiative on Energy Security for Global Growth*, mai 2016, disponible sur : www.g8.utoronto.ca.
57. En effet, les derniers sommets du G7 ont aussi réuni les ministres travaillant sur les thématiques liées aux technologies de l'information et de la communication, permettant de mettre au point une stratégie avec des standards internationaux communs (*G7 ICT Strategy*), notamment au niveau de la protection de la vie privée dans le développement des nouvelles technologies numériques.
58. *G7 Fundamental Elements of Cybersecurity for the Financial Sector*, mai 2016, disponible sur : www.treasury.gov.
59. *G7 Fundamental Elements for Effective Assessment of Cybersecurity in the Financial Sector*, octobre 2017, disponible sur : www.g8.utoronto.ca.

développé des partenariats public-privé officiels pour soutenir la cybersécurité, où les différentes industries nationales sont elles-mêmes organisées avec des conseils de cybersécurité composés de représentants d'entreprises[60]. Au niveau de l'UE, un partenariat public-privé contractuel (PPPc) a été mis en place en juillet 2016 avec la Commission européenne et l'Organisation européenne pour la cybersécurité (regroupant les acteurs publics et privés, partenaires de la Commission dans le cadre du PPPc[61]). L'objectif de ce partenariat est de renforcer la coopération avec le secteur privé en amont du processus de cyberdéfense pour les infrastructures critiques, notamment le secteur de l'énergie[62]. En outre, le paquet sur la cybersécurité proposé par la Commission européenne en septembre 2017 prévoit la mise en place d'un système de certification européen régi par l'ENISA[63]. Le but est de faciliter le développement d'un marché intérieur pour la cybersécurité dans l'UE et de renforcer la coopération public-privé dans ce domaine. Le sommet sur le numérique de Tallinn a permis de préciser certaines des mesures prévues à ce sujet.

Aux États-Unis, le *Cybersecurity Risk Information Sharing Program* (CRISP) représente l'un des principaux partenariats entre l'industrie de l'énergie, le *Department of Energy* (DOE), ainsi que le *DOE Office of Electricity Delivery and Energy Reliability* (DOE-OE). Le CRISP permet aux différents acteurs d'échanger des informations de façon régulière et structurée sur la cybersécurité. Ce partenariat a bien fonctionné, avec une majorité d'entreprises du secteur de l'énergie ayant accepté d'y participer, représentant 75 % des consommateurs américains. En outre, depuis 1998, les opérateurs industriels collaborent avec le gouvernement américain pour identifier les cybermenaces et développer des standards de protection par le biais d'institutions appelées *Information Sharing and Analysis Centers* (ISACs). En 2015, Barack Obama avait créé les *Information Sharing Analysis Organizations* (ISAOs) afin d'encourager les entreprises n'ayant pas eu la possibilité de rejoindre les ISACs à collaborer quand même avec le gouvernement américain, notamment en matière de partage d'informations. Il existe aussi un ISAC spécialisé pour le secteur de l'électricité (E-ISAC), servant comme principal intermédiaire pour l'échange d'informations

60. Cela inclut notamment l'Allemagne, l'Autriche, l'Espagne et les Pays-Bas. Voir : BSA/The Software Alliance, *Tableau de bord de la cybersécurité dans l'UE*, *op. cit.*

61. L'Organisation européenne pour la cybersécurité (*European Cyber Security Organisation*, ECSO) est une organisation autofinancée à but non lucratif régie par la loi belge, établie en juin 2016. Elle regroupe tous les acteurs concernés issus des secteurs public et privé participant au PPPc en relation avec la Commission européenne. Voir : ECSO, *Mission & Objectives*, disponible sur : https://ecs-org.eu.

62. L'UE entend soutenir le PPPc à hauteur de 450 millions d'euros, avec un investissement supplémentaire espéré d'un milliard d'euros en provenance du secteur privé. Voir Commission européenne, *Commission Signs Agreement with Industry on Cybersecurity and Steps Up Efforts to Tackle Cyber-Threats*, 5 juillet 2017, disponible sur : http://europa.eu.

63. Commission européenne, *New Cybersecurity Package*, septembre 2017.

techniques et la coordination entre le *Department of Energy* et les fournisseurs d'électricité (*utilities*).

Néanmoins, malgré les progrès réalisés, plusieurs des personnes interrogées sont d'accord sur le fait que le partage d'informations entre les secteurs privés et publics est insuffisant en Europe comme aux États-Unis. Cela est notamment dû au fait que les entreprises sont souvent réticentes à notifier les agences gouvernementales en cas de cyberattaque par peur des dégâts causés à leur image. Ainsi, soutenir la coopération transatlantique dans ce domaine pourrait contribuer à renforcer les partenariats public-privé des deux côtés de l'Atlantique. L'objectif serait de faire collaborer les partenariats européens et américains afin qu'ils puissent développer des normes communes. Bien qu'il existe plusieurs plateformes encourageant la collaboration transatlantique entre les entreprises sur des sujets analogues, aucune ne travaille de manière approfondie sur la cybersécurité des infrastructures énergétiques. Par conséquent, une solution serait de créer une nouvelle institution transatlantique spécifiquement dédiée aux enjeux de cybersécurité pour les entreprises de l'énergie, qui ferait travailler ensemble les partenariats public-privé au travers de réunions régulières pour l'échange d'informations. Une autre possibilité serait de faire participer ces partenariats au sein de structures déjà existantes pour les échanges commerciaux transatlantiques. Par exemple, le *Transatlantic Business Council* organise régulièrement depuis 2002 le *Digital Economy Workshop* (DEW), l'un des principaux évènements du *Information Society Dialogue*, qui travaille notamment sur le développement de standards de sécurité pour les nouvelles TIC. En outre, il existe aussi le *EU-US Innovation and Investment in the Digital Economy Dialogue* (IIDED), dont la première réunion s'est tenue à Boston en mars 2016 pour traiter des enjeux liés aux nouvelles technologies digitales. Dans les deux cas, le DEW et le IIDED travaillent sur des sujets qui sont en lien direct avec les partenariats public-privé de cybersécurité pour le secteur de l'énergie en Europe et aux États-Unis. Il serait donc bénéfique que ces derniers y participent de façon régulière afin de développer des standards transatlantiques communs.

Conclusion

Les États-Unis et l'UE ont des approches différentes en matière de cybersécurité pour les infrastructures énergétiques. La stratégie américaine a été de privilégier la sécurité en profondeur avec des réglementations strictes et détaillées dans des secteurs précis, appliquées par des institutions fédérales aux pouvoirs coercitifs. Au contraire, l'UE a préféré adopter une stratégie plus flexible et générale, couvrant un large éventail de différents domaines et laissant une marge de manœuvre importante aux États membres dans la mise en application des règles. Néanmoins, ces approches sont complémentaires dans la mesure où elles représentent les deux faces de la même médaille. En effet, les forces du système américain peuvent servir de modèle pour améliorer certaines faiblesses dans l'approche européenne, et *vice versa*, car l'UE dispose aussi d'un certain nombre d'atouts. Par exemple, les États-Unis sont en avance concernant le développement de normes précises et détaillées pour la cybersécurité, ainsi que dans la mise en application de ces normes, où l'UE pourrait s'inspirer du modèle américain. En revanche, les États-Unis peuvent aussi apprendre de l'UE sur les sujets de la protection de la vie privée et des données à caractère personnel, la cybersécurité des technologies bas-carbone, ainsi que la protection du réseau de distribution d'électricité. En outre, la Californie et la France sont des exemples d'État américain et de pays membre de l'UE qui présentent un certain nombre de spécificités pertinentes en la matière.

Ainsi, il existe une véritable opportunité pour développer une coopération transatlantique plus approfondie en matière de cybersécurité, permettant à l'UE et aux États-Unis de pouvoir chacun apprendre du modèle de l'autre. Cela mériterait de se faire à plusieurs échelles, notamment avec un renforcement de la collaboration bilatérale entre les gouvernements, mais aussi au sein de structures multilatérales telles que l'OTAN et le G7, et enfin au niveau des partenariats public-privé. L'objectif serait de mettre en place des standards transatlantiques communs de cybersécurité, qui pourraient ensuite devenir des normes internationales rigoureuses. En raison de la mondialisation des technologies numériques, une cyberattaque même dans un pays éloigné peut se répandre à l'ensemble du réseau, comme ce fut le cas récemment avec l'Ukraine. Par conséquent, si l'UE et les États-Unis parviennent à renforcer les normes internationales de cybersécurité, cela pourrait permettre de réduire les risques de propagation. Avec l'accélération de la digitalisation des infrastructures critiques, le sujet

de la cybersécurité dans le secteur de l'énergie va devenir encore plus crucial dans les années à venir. Cela est lié notamment à l'augmentation de l'espionnage industriel et à la cybercriminalité, où des logiciels malveillants sont de plus en plus utilisés pour le piratage de données à des fins lucratives. En outre, en raison de l'instabilité du contexte géopolitique, l'augmentation des risques de cyberattaques est aussi liée à la montée des tensions entre les grandes puissances. C'est pour ces raisons que l'UE et les États-Unis ont une responsabilité particulière, car leur collaboration au niveau de la cybersécurité est essentielle. Malgré des divergences avec l'UE sur de nombreux sujets, le président Trump a démontré un intérêt notable pour les questions de cybersécurité. Il y a donc dans ce domaine une réelle opportunité pour renforcer la coopération transatlantique dans les années à venir.

Références

AIEA, « Computer Security at Nuclear Facilities », *Security Series No. 17: Technical Guidance Reference Manual*, 2011.

ANSSI, *Maîtriser la SSI pour les systèmes industriels*, 2012.

ANSSI, « Stratégie de la France : défense et sécurité des systèmes d'information », 2011.

ANSSI, « Stratégie nationale pour la sécurité du numérique », 2015.

BSA/The Software Alliance, *Tableau de bord de la cybersécurité dans l'UE : Vers un cyberespace europe´en sécurise´*, 2015.

California Legislative Information, « AB-1274 Privacy: Customer Electrical or Natural Gas Usage Data », octobre 2013.

Commission européenne, *Commission Signs Agreement with Industry on Cybersecurity and Steps up Efforts to Tackle Cyber-Threats*, 5 juillet 2017.

Commission européenne, *New Cybersecurity Package*, septembre 2017.

Cruciani M., « Le paysage des énergies renouvelables en Europe en 2030 », *Études de l'Ifri*, Ifri, juin 2017.

Desarnaud G., « Cyberattaques et systèmes énergétiques : faire face au risque », *Études de l'Ifri*, Ifri, janvier 2017.

Ebinger C. et Massy K., « Software and Hard Targets: Enhancing Smart Grid Cyber Security in the Age of Information Warfare », *Energy Security Initiative at Brookings*, 2011.

EECSP, *Cyber Security in the Energy Sector: Recommendations for the European Commission on a European Strategic Framework and Potential Future Legislative Acts for the Energy Sector*, 2017.

ENISA, *Cybersecurity Cooperation: Defending the Digital Frontline*, 2013.

ENISA, *Cyber Europe 2016: After Action Report*, juin 2017.

ENISA, *Good Practice Guide for Incident Management*, 2010.

ENISA, *Multi-Annual Staff Policy Plan 2016-2018*, octobre 2015.

ENISA, *Report on Cybersecurity Information Sharing in the Energy Sector*, 2016.

ENISA, *Statement of Estimates 2017* (Budget 2017), 2017.

EU-US Cyber Dialogue – Third meeting, décembre 2016, https://eeas.europa.eu.

EU-US Energy Council, *Joint Statement*, 2016.

EU-US 14th Information Society Dialogue, *Joint Statement*, 2016.

Fallon R. et Lazaroff M., *NERC Increasing Penalties for Fundamentally Failing to Comply with Cyber Standards*, Cozen O'Connor, novembre 2016.

Global Cybersecurity Summit 2017, qui s'est tenu à Kiev en Ukraine du 14 au 15 juin 2017, https://gcs17.com/.

Gomart T. (dir.), « Trump, un an après. Un monde à l'état de nature ? », *Études de l'Ifri*, Ifri, novembre 2017.

Guiton A., « Enquête : les cobayes de la cyberguerre », *Libération*, 28 juillet 2017.

G7 Principles and Actions on Cyber, 2016.

G7 Fundamental Elements of Cybersecurity for the Financial Sector, 2016.

G7 Fundamental Elements for Effective Assessment of Cybersecurity in the Financial Sector, 2017.

G7 Kitakyushu Initiative on Energy Security for Global Growth, 2016.

Lindsay J. R., « Tipping the Scales: The Attribution Problem and the Feasibility of Deterrence against Cyberattack », *Journal of Cybersecurity*, vol. 1, n° 1, 1er septembre 2015.

NERC 2017 Business Plan and Budget Final Draft, Finance and Audit Committee Meeting, août 2016.

O'Keefe E. et Nakashima E., « Cybersecurity Bill Fails in Senate », *The Washington Post*, 2 août 2012.

OTAN, *La cyberdéfense*, août 2017, www.nato.int.

Parlement européen, Direction générale des politiques internes de l'Union, *Cyber Security Strategy for the Energy Sector – Study for the Industry, Research and Energy Committee*, octobre 2016.

Ruhle M. et Trakimavicius L., « Cyberattacks Are the New Challenge for Renewable Energy », POLITICO, 23 juillet 2017.

SANS et E-ISAC, *Analysis of the Cyber Attack on the Ukrainian Power Grid: Defense Use Case*, 2016.

Shea D., « State Efforts to Protect the Electric Grid », *National Conference of State Legislatures*, 2016.

US Chamber of Commerce, *Transatlantic Cybersecurity: Forging a United Response to Universal Threats*, 2017.

US Department of Commerce, *Overview of the EU-US Privacy Shield*, 12 juillet 2016.

World Energy Council, « The Road to Resilience: Managing Cyber Risks », *World Energy Perspectives*, 2016.

ifri
institut français
des relations
internationales