Études de l'Ifri

CYBERATTAQUES ET SYSTÈMES ÉNERGÉTIQUES

Faire face au risque

Gabrielle DESARNAUD

Janvier 2017

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.

Avec son antenne de Bruxelles (Ifri-Bruxelles), l'Ifri s'impose comme un des rares *think tanks* français à se positionner au cœur même du débat européen.

ISBN : 978-2-36567-651-9

Comment citer cette publication :
Gabrielle Desarnaud, « Cyberattaques et systèmes énergétiques. Faire face au risque », *Études de l'Ifri*, janvier 2017.

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

Ifri-Bruxelles

Rue Marie-Thérèse, 21 1000 – Bruxelles – BELGIQUE

Tél. : +32 (0)2 238 51 10 – Fax : +32 (0)2 238 51 15

E-mail : bruxelles@ifri.org

Site internet : Ifri.org

Auteur

Gabrielle Desarnaud est chercheur au Centre Énergie de l'Ifri. Ses axes de recherche couvrent la stratégie énergétique et climatique de la Chine et les enjeux de cybersécurité pour les infrastructures énergétiques.

Elle a auparavant travaillé pour Asia Centre à Pékin sur la sécurité énergétique de la Chine, et plus particulièrement sur les défis liés à sa dépendance au charbon. Elle a également traité des sujets tels que la réforme du marché du gaz et la politique de développement des énergies renouvelables en Chine.

Gabrielle Desarnaud est titulaire du master International Energy de l'Institut d'études politiques de Paris et du master Sustainable Development and International Relations de l'université de Pékin.

Avant-propos

Ce papier a été rédigé sur la base d'une revue de la littérature et une vingtaine d'entretiens avec des professionnels de l'énergie et de la sécurité des systèmes d'information. L'auteur souhaite remercier chaleureusement l'ensemble des personnes rencontrées pour le soutien apporté malgré la sensibilité du sujet. Si des représentants de tous les acteurs du secteur n'ont pu être rencontrés pour cette étude, ceux interrogés sont issus d'une variété d'entreprises de l'énergie, de la sécurité, et d'institutions les plus représentatives possible des enjeux actuels. Afin d'assurer toute la confidentialité possible à ceux qui ont souhaité contribuer sans être nommés, aucune des informations issues des entretiens et présentes dans cette étude n'ont été attribuées.

Résumé

La digitalisation de l'industrie énergétique permet de révolutionner les processus de production, de stockage, de transport et de consommation d'énergie. Nos infrastructures énergétiques, conçues il y a plusieurs décennies et prévues pour demeurer fonctionnelles pour de nombreuses années encore, côtoient désormais des équipements numériques avec lesquels elles interagissent au quotidien. Ces évolutions, qui sont aujourd'hui un gage de disponibilité, d'efficacité et de réactivité, ouvrent pourtant la voie à un type de menace qui jusqu'en 2010 avait relativement épargné l'industrie énergétique : les cyberattaques. Le nombre et la technicité des attaques ont augmenté après les dégâts causés par le virus Stuxnet au sein du complexe d'enrichissement nucléaire iranien de Natanz, bien que cette attaque demeure la plus sophistiquée observée à ce jour. Et s'il y a une réelle prise de conscience des enjeux dans le secteur énergétique, les risques persistent. Les politiques de transition énergétique et les efforts d'intégration des énergies renouvelables ne feront que renforcer cette tendance tant que la cybersécurité ne fait pas partie de la réflexion sur l'avenir du système énergétique. La réglementation tente de s'adapter, notamment en France où les autorités collaborent étroitement avec les entreprises de l'énergie pour faire émerger un cadre réglementaire contraignant, et protéger les Opérateurs d'Importance Vitale (OIV). Cette démarche inspire également d'autres pays d'Europe, mais des mesures communes à toute l'Union européenne sont à prendre rapidement afin de garantir la sécurité de nos réseaux énergétiques, fortement interconnectés.

Sommaire

Introduction

L'industrie énergétique amorce, malgré un certain retard vis-à-vis d'autres secteurs, une révolution numérique qui bouleverse les modes de production, de transformation, de stockage, de transport et de consommation de l'énergie. Les technologies de l'information et de la communication (TIC), progressivement déployées au sein des infrastructures énergétiques, ont ce double avantage de permettre l'analyse de données complexes afin d'optimiser la chaîne d'approvisionnement dans son ensemble, tout en proposant au consommateur une gamme de services plus personnalisés.

L'industrie énergétique a particulièrement profité des gains d'efficacité induits par ces technologies : les études sismiques, les forages pétroliers, la gestion de la pression et de la température des oléoducs, le transport d'électricité sur le réseau ou encore les échanges à la bourse européenne de l'électricité sont désormais effectués grâce aux TIC. Certaines activités ont déjà pris le virage du digital depuis plusieurs années, et l'étude de données de production et de fonctionnement des équipements, à toutes les étapes de la chaîne de valeur, améliorera considérablement la prise de décision dans un futur proche.

Certains acteurs de l'industrie énergétique misent ainsi sur l'internet industriel pour en faire une activité à part entière : General Electric a par exemple mis au point une plateforme de collecte et d'analyse de données prélevées par des capteurs présents dans les automates industriels. Il sera alors possible pour les entreprises d'établir des statistiques et créer des profils de production, optimiser le rendement des équipements et maximiser leur disponibilité grâce à la maintenance prédictive. Cette tendance est également accentuée par les politiques de transition énergétique : le déploiement de 35 millions de compteurs communicants en France devrait permettre de rationaliser la consommation d'énergie, créer des profils de consommateurs plus précis afin d'anticiper les courbes de charge et mieux planifier l'investissement en infrastructures lourdes, tout en proposant aux clients la possibilité d'avoir accès à des informations plus détaillées, de mieux gérer leur façon de consommer et donc, de faire des économies. Les « réseaux intelligents » permettront ainsi d'interconnecter les infrastructures industrielles et domestiques, en fournissant une vision holistique de la consommation à différentes échelles d'un territoire.

Cependant, une numérisation accrue de l'industrie énergétique l'expose à des risques auxquels l'informatique de gestion est déjà confrontée depuis de nombreuses années. En 2007, le Laboratoire national de l'Idaho prouvait qu'une cyberattaque pouvait endommager physiquement des composants d'un réseau électrique. L'expérience a démontré qu'à l'aide d'un programme malveillant, il était possible d'actionner les disjoncteurs d'un générateur au diesel afin de le connecter et déconnecter du réseau à répétition, jusqu'à provoquer un début d'incendie[1]. Par la suite, un certain nombre de cyberattaques avérées sur des infrastructures énergétiques ont mis en lumière les dommages potentiels en conditions réelles.

Cette note s'attachera à analyser les risques encourus par le secteur énergétique et particulièrement électrique, notamment au regard des évolutions liées à la transition énergétique. Une revue des moyens déployés en France et à l'échelle européenne aura également pour objectif de déterminer les marges d'action encore à envisager afin de stimuler les progrès.

1. M. Zeller, « Myth or Reality – Does the Aurora Vulnerability Pose a Risk to My Generator? », Schweitzer Engineering Laboratories, 2011, disponible sur : https://selinc.cachefly.net/.

L'industrie énergétique face au risque cyber

Vulnérabilités techniques et humaines

Les systèmes énergétiques ont la particularité d'avoir longtemps gardé une certaine autonomie vis-à-vis des technologies numériques. Celles-ci ont lentement intégré les sites industriels, au gré des évolutions des équipements dont la durée de vie excède pour la plupart une décennie. La longueur des cycles d'investissement caractérisant l'industrie énergétique a retardé l'utilisation de logiciels et de systèmes d'exploitation grand public au sein de ces installations.

Jusqu'à récemment, l'industrie énergétique n'était donc que peu exposée au risque de cyberattaque, car le fonctionnement de ses équipements n'intégrait pas de fonction informatique, ou n'utilisait que des logiciels et protocoles propriétaires spécifiques à chaque activité, voire à chaque installation. Pour les attaquer, il eut fallu être capable de connaître la structure d'un système dans les détails, alors même que le manque de connexions au monde extérieur limitait la possibilité d'espionnage par des moyens informatiques. Même si un système parvenait à être attaqué, il eût été nécessaire de répéter les mêmes étapes de repérage, de création d'un logiciel malveillant et d'infiltration, spécifiques à chaque nouvelle installation visée. Peu éprouvés jusqu'à présent par la communauté informatique, les systèmes énergétiques sont donc aussi restés peu protégés.

Par la suite, trois facteurs ont entraîné une intégration progressive des TIC au sein de l'industrie énergétique :

- le besoin de rationaliser la production avec des outils capables de récolter et de traiter d'importantes masses de données ;
- le besoin d'échanger des données avec des acteurs extérieurs aux sites industriels (opérateurs, entités de gestion…) ;
- la nécessité de faire des économies sur les logiciels employés et de faciliter la communication entre sites de gestion et sites industriels.

Pour répondre à ces besoins, l'industrie énergétique s'est peu à peu tournée vers des logiciels d'exploitation et systèmes de contrôle industriels

(SCI)[2] clés en main, disponibles sur le marché (Annexe 1). Moins onéreux que les systèmes de contrôle propriétaires, mais également mieux connus du grand public, ils sont plus vulnérables aux programmes malveillants qui circulent dans la sphère informatique. En parallèle, les connexions et les échanges de données avec des entités extérieures se sont multipliés : un opérateur électrique doit désormais être capable d'observer l'état du réseau et de la production en temps réel, et de communiquer certaines de ces données à d'autres acteurs. Un prestataire peut aussi requérir une connexion à distance pour effectuer des opérations de maintenance sur certains équipements. Les systèmes de contrôle industriels propriétaires et relativement isolés se sont ainsi transformés en architectures ouvertes, employant des technologies standard interconnectées avec des réseaux d'entreprises et internet.

L'ouverture des réseaux industriels peu protégés n'est pas leur seule faiblesse. Si l'industrie énergétique amorce une phase de digitalisation sans précédent, ses équipements dont la durée de vie excède parfois 30 ans sont toujours en service, et une partie d'entre eux le restera encore pour plusieurs décennies. Ceux-ci ont été conçus à une époque où les balbutiements d'internet ne permettaient pas d'envisager le risque cyber que les systèmes informatiques de gestion convoient, et n'ont pas été pensés pour intégrer des fonctions de sécurité. Ainsi sont-ils programmés pour être précis, stables, prévisibles, résistants, mais non pour utiliser, entre autres, des protocoles de chiffrement ou d'authentification. Les vulnérabilités existantes ne sont d'ailleurs pas nécessairement identifiées puisque les industriels ont une certaine difficulté à connaître précisément tous les automates et composants de leurs installations.

Or les solutions de protection du monde informatique, comme l'application de correctifs de sécurité lorsqu'une faille est découverte dans un logiciel, ne sont pas aisément applicables au monde industriel. En effet, selon l'une des personnes interrogées, mettre en place une « défense active » (comme un antivirus) impliquerait un arrêt net et imprévisible de 10 à 20 % des équipements. À ceux-là s'ajoutent ceux dont le fonctionnement pourrait être altéré. Appliquer une mise à jour logicielle impose d'effectuer des tests longs afin d'assurer la remise en route des installations sans mauvaises interactions. C'est pour cette raison que la

2. Les SCI sont des systèmes informatiques servant à contrôler et automatiser de nombreux processus industriels. Il s'agit d'un terme générique pour plusieurs types de logiciels, dont les Systèmes de contrôle et d'acquisition de données (SCADA). Très utilisés dans l'industrie de l'énergie et réputés vulnérables aux cyberattaques, il s'agit de systèmes de contrôle/commande permettant de superviser et de commander une installation industrielle à distance.

plupart des logiciels dans le monde industriel ne sont que très rarement, voire jamais mis à jour, alors que les failles sont souvent documentées et accessibles sur internet.

Dans le cas d'une centrale nucléaire par exemple, la meilleure marge de manœuvre pour le renouvellement des équipements se situe durant la « visite décennale », c'est-à-dire lors d'un arrêt de tranche de plusieurs mois qui ne s'effectue que tous les dix ans, donnant lieu à des tests et des mises à niveau de grande ampleur[3]. De nombreux opérateurs de transmission d'électricité ou de gaz utilisent encore des logiciels d'exploitation obsolètes pour leurs opérations de gestion des flux[4], en raison de la difficulté que cela représente d'effectuer la migration vers une version plus récente. En 2015, l'organisation en charge d'auditer les dépenses de l'État japonais[5], avait d'ailleurs sommé l'exploitant de la centrale nucléaire de Fukushima (Tokyo Electric Power Company-TEPCO), de migrer ses quelque 48 000 postes informatiques encore sous WindowsXP vers un logiciel d'exploitation plus sécurisé[6]. Alors que Microsoft avait annoncé depuis plusieurs années que les correctifs de sécurité ne seraient plus fournis après juillet 2015, la compagnie TEPCO prévoyait de retarder l'investissement dans un nouveau logiciel[7]. La migration a depuis été effectuée.

Il faut compter avec cela les erreurs humaines courantes : le manque de formation concernant les objets extérieurs connectables (téléphones, ordinateurs portables, clés USB), les mots de passe par défaut qui demeurent inchangés sur les postes ou les automates pour des questions pratiques ou par négligence, le manque de systèmes d'authentification complexes pour les connexions à distance… (Annexe 2)

Jusqu'en 2010, les risques encourus et les mesures de protection à instaurer n'ont pas fait l'objet de réflexions poussées. Le principal élément déclencheur parmi les industriels, et plus particulièrement dans l'industrie énergétique, fut la découverte du virus Stuxnet en 2010 au sein du complexe iranien d'enrichissement d'uranium de Natanz. Cet événement a démontré que l'industrie énergétique pouvait être victime d'attaques tant sur son réseau de gestion (bureaux, entité administrative) comme toute autre entreprise, que sur ses infrastructures. La nature des activités de

3. IRSN, *Visites décennales : Réévaluer la sûreté de la deuxième génération*, 2010, disponible sur : www.irsn.fr/FR.

4. « Windows XP in Utilities Could Mean Big Security Problems », *The Wall Street Journal*, disponible sur : http://blogs.wsj.com.

5. Board of Audit of Japan, disponible sur : www.jbaudit.go.jp.

6. Board of Audit of Japan, Résultat d'audit de Tokyo Electric Power Co., Ltd sur l'indemnisation des dommages nucléaires, p. 100, disponible sur : www.jbaudit.go.jp.

7. TEPCO, Communiqué de presse, 6 juillet 2014, disponible sur : www.tepco.co.jp.

l'industrie énergétique et son rôle vital pour l'économie en font une cible de choix.

Attaques connues sur des infrastructures énergétiques

Des précédents révélateurs

Les attaques rendues publiques sur le secteur énergétique sont encore peu nombreuses. Certaines sont particulièrement élaborées et supposément soutenues par des moyens étatiques, alors que d'autres ne ciblaient pas nécessairement le secteur énergétique en particulier. Certains incidents techniques illustrent par ailleurs les dégâts qu'une cyberattaque ciblée serait en mesure de causer.

Slammer : un ver simpliste

En janvier 2003, le système de surveillance de sécurité de la centrale nucléaire de Davis-Besse dans l'Ohio s'est arrêté durant plusieurs heures en raison d'une infection par le ver informatique Slammer. Le système d'affichage des paramètres de sûreté collecte les données des systèmes de refroidissement, des capteurs de radiations et autres informations critiques au sein d'une centrale, pour donner des informations en temps réel sur l'état physique des équipements. C'est ce système qui donnerait l'alerte en cas de fusion du réacteur. Il est intéressant de noter que le ver Slammer est un petit code n'ayant d'autre fonction que celle de générer des adresses IP de façon aléatoire, afin de leur envoyer des répliques de lui-même via une connexion internet. La centrale, qui n'était donc pas visée spécifiquement, possédait une connexion non sécurisée vers une entreprise tierce (infectée au hasard par Slammer, comme des milliers d'autres), alors que le reste du réseau était protégé par un pare-feu qui aurait pu empêcher la contamination[8]. De plus, un correctif avait déjà été diffusé par Microsoft six mois avant le début de l'attaque, ce qui illustre les difficultés qu'ont les installations industrielles à appliquer des procédures basiques de sécurité informatique. La centrale était déjà à l'arrêt depuis plus d'un an au moment des faits.

8. B. Kesler, « The Vulnerability of Nuclear Facilities to Cyber Attack », *Strategic Insights*, vol. 10, n° 1, 2011, p. 15-25, disponible sur : http://large.stanford.edu.

Stuxnet : une prise de conscience brutale

Stuxnet est l'attaque la plus avancée à laquelle une infrastructure nucléaire ait été confrontée. Lancé dans sa première version en 2005, ce logiciel malveillant extrêmement sophistiqué, utilisant plusieurs vulnérabilités « zéro jour[9] » a été conçu pour attaquer le complexe d'enrichissement d'uranium de Natanz, en Iran. Celui-ci est probablement passé dans le réseau opérationnel de l'usine par le biais d'une clé USB infectée. La dernière version du programme permettait de modifier la vitesse de rotation des centrifugeuses de manière répétitive : le processus d'enrichissement d'uranium était ainsi compromis et les centrifugeuses elles-mêmes subissaient des avaries matérielles. Environ un millier de centrifugeuses a été endommagé de cette manière sur le complexe de Natanz, jusqu'à la découverte du ver en 2010. Afin de passer inaperçu, Stuxnet enregistrait les mesures des opérations durant les phases opérationnelles normales, et les passait en boucle sur l'interface de contrôle lorsque la vitesse de rotation des centrifugeuses était modifiée. Ce programme aurait été spécifiquement conçu pour attaquer les systèmes iraniens et ne s'activer que s'il rencontrait la configuration très précise du site visé, comme le nombre et la disposition exacts des centrifugeuses. Les attaquants ont donc mené une reconnaissance en profondeur des installations au préalable, et ont sans doute reproduit une partie des équipements à l'identique pour tester le logiciel avant d'infecter l'usine iranienne[10]. S'il est difficile d'attribuer avec certitude[11] l'origine de l'attaque, plusieurs enquêtes ont révélé que sa création aurait été soutenue par les gouvernements américain et israélien[12]. L'intention première aurait été le ralentissement du programme nucléaire iranien, peut-être le temps de mener à bien les négociations sur le terrain diplomatique.

Shamoon : une propagation limitée grâce à une protection adéquate

En août 2012, un malware nommé Shamoon a détruit quelque 30 000 ordinateurs de la compagnie pétrolière Saudi Aramco. Un composant du logiciel était en effet configuré pour détruire la zone

9. Dites des vulnérabilités d'un programme encore inconnues, et pour lesquelles il n'existe pas encore de correctif de sécurité. Ces vulnérabilités peuvent se vendre plusieurs centaines de milliers d'euros (à des entreprises ou des États) et s'échangent également sur le marché noir.
10. D. E. Sanger, « Obama Order Sped Up Wave of Cyberattacks Against Iran », *The New York Times*, juin 2012, disponible sur : www.nytimes.com.
11. Pour plus d'informations sur l'attribution de Stuxnet, voir G. Desarnaud, « Le secteur énergétique exposé à la cyber-menace », *Édito Énergie*, 12 juillet 2016, disponible sur : www.ifri.org.
12. D. E. Sanger, *Confront and Conceal. Obama's Secret Wars and Surprising Use of American Power*, New York, Broadway Books, 2012.

amorce[13] des disques durs, les empêchant de redémarrer. Le but premier de cette attaque semble être le sabotage, avec peut-être la volonté d'interrompre une partie des activités industrielles de l'entreprise. Dans les faits cependant, le programme ne contenait aucune fonctionnalité conçue pour contrôler ou attaquer un système industriel, même s'il aurait pu détruire les ordinateurs en relation avec les opérations de production ou de maintenance. Saudi Aramco avait semble-t-il mis en place des mesures de sécurité assez fiables pour que l'attaque reste cantonnée au réseau de gestion de l'entreprise, et ne puisse se propager dans le réseau opérationnel, séparé et protégé. Selon la compagnie, cet incident n'a eu aucune conséquence sur ses activités pétrolières, bien que les opérations courantes (facturation, règlement des contrats…) aient dû être effectuées manuellement le temps d'installer de nouveaux disques durs[14].

Energetic Bear : l'importance de sécuriser la chaîne logistique

En 2014, quelque 250 entreprises de l'énergie aux États-Unis et en Europe de l'Ouest ont été infectées par un virus similaire à Stuxnet, appelé Energetic Bear. Le logiciel malveillant, probablement en opération depuis 2011, a principalement infecté des producteurs d'électricité, des opérateurs de réseaux de distribution d'électricité et de pétrole ainsi que des équipementiers. Il permettait notamment aux attaquants de prendre le contrôle des équipements industriels. Le groupe à l'origine du virus aurait d'abord infecté trois équipementiers de systèmes de contrôle industriels qui auraient ensuite transmis le virus à leurs clients énergéticiens lors d'opérations de mises à jour[15].

BlackEnergy : les réseaux électriques vulnérables

Enfin, une attaque sur un réseau électrique ukrainien en décembre 2015 a privé quelque 200 000 résidants d'électricité durant plusieurs heures. Une campagne d'hameçonnage aurait permis d'introduire un malware dans le système informatique des opérateurs afin de prendre la main à distance sur les SCI gérant la distribution d'électricité. L'acquisition de mots de passe au préalable a facilité l'accès au réseau interne, permettant aux attaquants d'actionner les disjoncteurs d'une trentaine de postes électriques et couper le courant. Le report d'électricité sur les lignes encore opérationnelles a créé des surcharges sur d'autres parties du réseau. En parallèle, deux des

13. Premier secteur d'un disque dur permettant de charger le système d'exploitation.
14. Symantec, *Targeted Attacks Against the Energy Sector – Security Response*, 2014.
15. Symantec, *Dragonfly: Cyberespionage Attacks Against Energy Suppliers – Symantec Security Response*, 2014.

centres de contrôle étaient eux-mêmes plongés dans le noir car leur système électrique de secours[16] avait été reprogrammé par les attaquants pour ne pas se déclencher en cas de panne de l'alimentation générale. Un module similaire à celui de Shamoon aurait enfin permis d'endommager des disques durs et empêcher le redémarrage des systèmes d'exploitation. Plusieurs semaines après l'incident, un certain nombre de postes électriques devaient toujours être opérés en mode manuel, alors que ces infrastructures sont normalement contrôlées à distance[17].

Attaques et incidents documentés ayant touché des infrastructures énergétiques

Année	Cible	Nom de l'attaque	Conséquences	Objectif	Attaquants
1982	Explosion d'un gazoduc-Sibérie, (Russie)		Logiciel malveillant introduit dans le SCADA de gestion d'un gazoduc, explosion équivalente à 3 tonnes de TNT	Sabotage	Externes
1992	Centrale nucléaire d'Ignalina, (Lituanie)		Un technicien de la centrale nucléaire d'Ignalina a introduit un virus dans un système de contrôle d'un des deux réacteurs RBMK (type Tchernobyl).	Sabotage	Interne
1992	Système d'alerte d'urgence de Chevron, (USA)		Un employé licencié de Chevron a désactivé le système d'alerte d'incident de la firme en piratant les ordinateurs en charge du système. L'intrusion n'a été découverte que lorsqu'une urgence est survenue dans une raffinerie de Chevron dans le Richmond, durant laquelle des milliers de personnes vivant à proximité ont été exposées à des substances toxiques durant une dizaine d'heures.	Sabotage	Interne
1999	Gazprom, (Russie)		Prise de contrôle du tableau de distribution contrôlant les flux de gaz des gazoducs	Sabotage	Interne
1999	Gazoduc à Bellingham (USA)		Incident lié au développement d'une base de données pour le système SCADA opérant les gazoducs de la compagnie Olympic Pipe Line. Incident en partie responsable d'une fuite conséquente de gazole causant 3 morts et 8 blessés.	Incident/ erreur humaine	Interne
2001	Opérateur électrique de Californie, (USA)		Des attaquants ont eu accès à l'un des réseaux internes de l'opérateur California Independent System. L'attaque n'a pu atteindre le réseau d'automates contrôlés par la compagnie avant d'être découvert.	Sabotage	Externes/ Chine ?
2003	Centrale nucléaire de Davis-Besse, (USA)	Slammer	Arrêt du système d'affichage des paramètres de sûreté durant 4 heures en raison d'un ver sans fonctionnalités d'espionnage ou de sabotage	Non visé	Externes

16. Alimentation sans interruption (ASI).
17. SANS-ICS, E.-I., *Analysis of the Cyber Attack on the Ukrainian Power Grid*, 2016.

2008	Centrale Hatch, (USA)		Une mise à jour effectuée sur un ordinateur du système de gestion de l'opérateur a induit en erreur le système de contrôle du réacteur, entraînant un arrêt involontaire de celui-ci pendant 48 heures.	Incident/ erreur humaine	Entreprise tierce
2010	Natanz, (Iran)	Stuxnet	Plusieurs années d'infiltration dans le complexe d'enrichissement d'uranium Natanz, endommagement de plus de 900 centrifugeuses d'enrichissement d'uranium	Sabotage	Externes/ Étatiques/ USA, Israël ?
2011	Industrie pétrolière et gazière	Night Dragon	Extraction d'informations confidentielles relatives à des projets pétroliers et gaziers	Espionnage	Externes
2011	Industries de l'énergie	Duqu	Parties du code presque identiques à Stuxnet, conçu uniquement pour de l'espionnage industriel sans contenir de fonction destructrice	Espionnage	Externes
2011	Areva, (France)		Vol de données, non critiques selon l'entreprise. L'infiltration aurait duré deux ans.	Espionnage	Externes
2012	Entreprises et institutions liées à l'énergie	Flame	Répandu au Moyen-Orient et en Afrique du Nord, a opéré durant au moins deux ans. Conçu pour l'espionnage et l'analyse de données. Découvert après que le Ministère du pétrole iranien et la compagnie nationale pétrolière iranienne aient signalé le vol et l'effacement de certaines données importantes de leurs systèmes	Espionnage /vol de données	Externes
2012	Saudi Aramco, (Arabie Saoudite)	Shamoon	30 000 disques durs détruits à remplacer, réseau opérationnel intouché	Sabotage	Externes
2013	Bowman Avenue Dam, (USA)		Des attaquants ont pris le contrôle à distance d'un petit barrage près de New York, sans conséquences	Reconnaissance	Externes/ Iran ?
2014	Entreprises de l'énergie	Energetic Bear	250 entreprises aux USA et en Europe de l'ouest infectées	Espionnage /possibilité de sabotage	Externes
2014	Stations essence	Operation Petrol	Le groupe d'hacktivistes Anonymous a annoncé son attaque sur des entreprises pétrolières et des stations essence (déni de service, vol de données). Peu d'échos cependant sur ce qui a pu être fait ou non.	Sabotage/ vol de données	Anonymous
2014	Korea Hydro and Nuclear Power (KHNP), (Corée du Sud)		Vol des plans et manuels de deux réacteurs, de circuits électriques, de mesures d'exposition aux radiations de la zone et de données sur 10 000 employés. Suite à des pressions sur le gouvernement pour éteindre trois réacteurs par des activistes.	Chantage	Externe
2015	Opérateurs d'électricité, (Ukraine)	Black Energy	Une trentaine de postes électriques déconnectés du réseau, 8 provinces sans électricité durant plusieurs heures, plus de 200 000 personnes touchées, systèmes de contrôle endommagés physiquement, fonctionnement en mode dégradé plusieurs semaines après l'attaque.	Sabotage	Externe/ Étatique, Russie ?

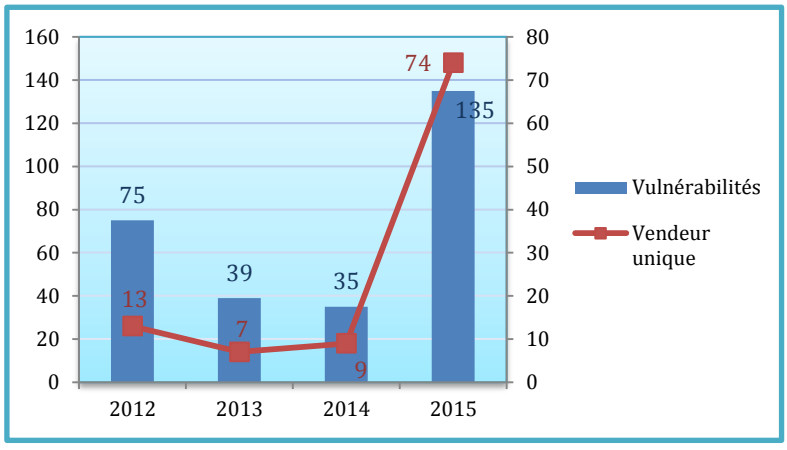
Liste non exhaustive. Source : B. Miller, et D. C. Rowe, Symantec, ICS-CER, NERC.

Le secteur énergétique de plus en plus ciblé

La découverte de Stuxnet en 2010 a créé une onde de choc au sein de l'industrie énergétique. Cette attaque a servi de projecteur sur des vulnérabilités inconnues, et révélé la dimension politique autant que financière, des attaques ciblant l'industrie énergétique.

On observe depuis lors une augmentation des attaques sur le secteur énergétique, ainsi que des découvertes de vulnérabilités sur des systèmes industriels. Comme le montre le tableau ci-dessous, ces dernières ont augmenté de 380 % entre 2014 et 2015, bien plus que la découverte de vulnérabilités sur les plug-ins ou les systèmes d'exploitation des téléphones mobiles. Le savoir-faire des pirates informatiques dans ce domaine s'améliore, alors que les experts de la cybersécurité pour les systèmes industriels restent peu nombreux à l'heure actuelle. La découverte de vulnérabilités sur des systèmes de contrôle industriels délivrés par un vendeur unique est également en augmentation, faisant peser des risques à toutes leurs entreprises clientes.

Découvertes de vulnérabilités industrielles dans le monde (2012-2015)



Découvertes de vulnérabilités par type (2014 à 2015)

Vulnérabilités « zéro jour »	+ 125 %
Navigateurs	+ 37 %
Plug-ins	+ 102 %
Internet	+ 2 %
Mobile	+ 214 %
Industrielles	+ 380 %

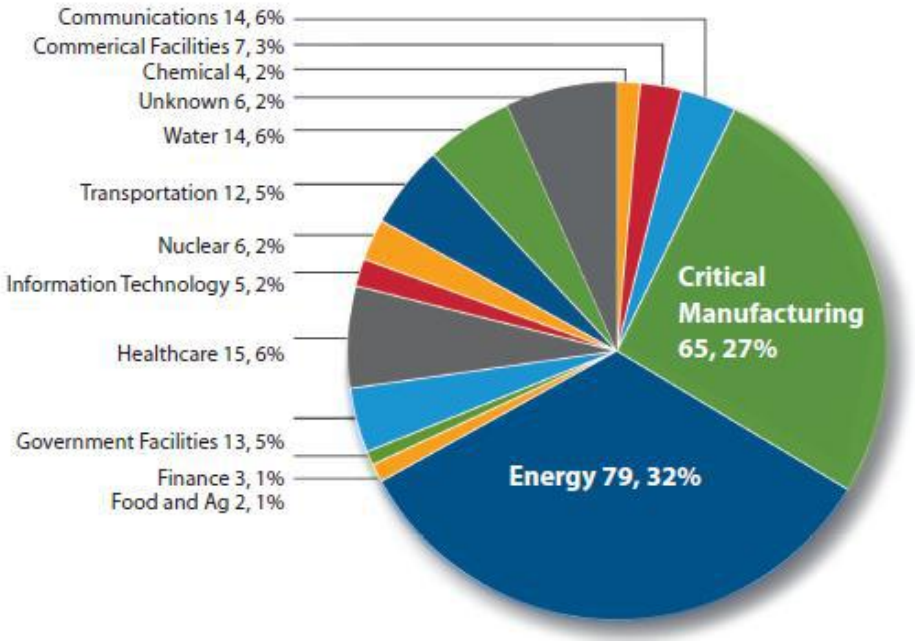
Source : Symantec, Threat Landscape Evolution and Internet Security Threat Report*, 2016.*

Sur l'année 2014[18], les autorités américaines ont été sollicitées pour 245 attaques sur des systèmes industriels aux États-Unis, la plupart ayant eu lieu dans le secteur énergétique, et dont plus de la moitié peut être

18. Année fiscale aux USA, d'octobre 2013 à septembre 2014.

considérée comme des menaces persistantes avancées[19]. Or celles-ci sont en moyenne découvertes plus de 200 jours après qu'elles aient effectivement infiltré un réseau d'entreprise ou d'usine[20].

Incidents rapportés par secteur aux États-Unis, 2014 (Total 245)



"Critical Manufacturing" fait référence aux concepteurs de Systèmes de Contrôle Industriels, dont les équipementiers fournissant le secteur de l'énergie.

Source : US Department of Homeland Security, ICS-CERT Monitor 2014

Les entretiens auprès d'entreprises de l'énergie ont révélé que leurs équipes en charge de la sécurité des réseaux sont quotidiennement confrontées à des attaques informatiques. Les institutions en lien avec l'industrie énergétique ne sont pas épargnées : le Département de l'énergie américain aurait subi 150 attaques « réussies » entre 2010 et 2014, sur des systèmes contenant des informations critiques sur le réseau électrique et certaines centrales nucléaires[21].

19. Advanced Persistant Threat : type d'attaque informatique mettant en œuvre des moyens financiers et techniques conséquents et pouvant durer plusieurs années. La cible est en général définie et étudiée au préalable (US Department of Homeland Security, 2015).
20. Mandiant, *M-Trends Report 2015: A View from the Front Lines. Premier Outlook* (vol. 4). 2014, disponible sur : https://login.proxy.bib.uottawa.ca.
21. « Records: Energy Department Struck by Cyber Attacks », *USA Today*, septembre 2015, disponible sur : www.usatoday.com et https://assets.documentcloud.org.

Des motivations financières et géopolitiques ?

On peut distinguer trois grands types d'attaques à ce jour :

- celles qui visent à interrompre la disponibilité d'un système ou d'un service ;
- les attaques de confidentialité qui ont pour but d'exfiltrer des informations et surveiller une activité, souvent à des fins lucratives ;
- et des attaques sur l'intégrité d'un système visant à altérer des informations ou des processus (supprimer un logiciel critique, modifier le comportement de certains équipements, faire en sorte que le SCADA envoie des commandes erronées…)[22].

Le type d'attaque peut parfois révéler le profil de l'attaquant : les attaques de confidentialité sont par exemple souvent perpétrées par des groupes criminels tirant parti du vol de données sur certains marchés, voire commanditées par des concurrents.

Le risque de sabotage : des facteurs politiques et géopolitiques

Alors que les cyberattaques ont dans le cas le plus fréquent une visée lucrative et d'espionnage, l'industrie énergétique est aussi confrontée à des velléités de sabotage, parfois pour des raisons géopolitiques. Dans les deux cas connus les plus dévastateurs (l'attaque Stuxnet en 2010 et BlackEnergy en 2015), les capacités mises en œuvre et les enquêtes sur le terrain suggèrent qu'il s'agit d'attaques soutenues par des États plutôt que par des groupes d'activistes ou de criminels indépendants.

Dans le cas iranien, outre la reproduction d'une partie de l'installation originale, l'analyse du logiciel en lui-même a surpris les experts par son ingéniosité et sa complexité, comprenant une partie de code développée pour cette installation spécifique, fait rare qui suppose des compétences très développées. Le logiciel BlackEnergy ayant ciblé les opérateurs ukrainiens est également le fruit de plusieurs mois de travail d'une équipe ayant bénéficié de moyens financiers conséquents.

Face à ce type d'attaquants, les experts sont formels : la question n'est pas de savoir si, mais quand les attaques parviendront à pénétrer le système industriel de l'entreprise visée.

22. P. W. Singer et A. Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know*, Oxford, Oxford University Press, 2014.

Au vu des conséquences que l'utilisation de moyens informatiques à l'encontre d'infrastructures énergétiques serait à même d'engendrer, ce type d'attaque pourrait être considéré comme un acte de guerre, et ainsi dissuader un État mal intentionné de passer à l'action. Cependant, la difficulté d'attribution d'une cyberattaque protège également l'exécutant, et peut lui permettre de mener des actions ciblées et dévastatrices sans s'engager ouvertement. L'utilisation de faux drapeaux, très fréquente dans la mesure où les malwares utilisés deviennent progressivement publics et peuvent inspirer d'autres individus, complique le processus d'identification. Cela limite la possibilité d'une riposte ouverte, ou même la formation de coalitions pour dénoncer les actions du commanditaire, mais peut certainement mener à des tensions diplomatiques et un jeu de cyberdissuasion qui rebattrait les cartes de la géopolitique. Les experts de la sécurité des systèmes d'information s'accordent à dire que plusieurs États auraient les moyens de perpétrer une attaque de grande ampleur à l'encontre des systèmes énergétiques européens. Cependant, certains experts estiment que les coûts (sur les plans diplomatique, économique ou commercial) d'une telle action de sabotage seraient supérieurs aux bénéfices que l'État attaquant pourrait en tirer. Il serait toujours possible d'envisager qu'une entité terroriste s'associe à un groupe ayant les compétences pour mener à bien de telles actions. Cependant, un expert de la sécurité informatique interrogé pour ce rapport souligne que rien, à l'heure actuelle, ne laisse supposer qu'une telle manœuvre soit en préparation.

Certains activistes pourraient également représenter une menace bien qu'ils ne semblent pas disposer, à l'heure actuelle, des moyens techniques pour mener des opérations sur des infrastructures critiques. En 2014, Anonymous avait par exemple lancé Operation Petrol visant à attaquer des compagnies pétrolières et dénoncer l'utilisation du dollar dans le commerce d'hydrocarbures. Si l'annonce de l'attaque par le groupe d'« hacktivistes » a fait beaucoup de bruit, elle ne semble pas avoir porté ses fruits. Trois années auparavant, le Département de la sécurité intérieure américain avait démontré que le groupe n'avait pas les capacités de s'attaquer à des systèmes de contrôle industriels[23], ce qui serait, d'après certains experts, *a priori* toujours le cas.

23. Department of Homeland Security Bulletin: *Anonymous Hacktivist Threat to Industrial Control Systems (ICS)*, octobre 2011, https://publicintelligence.net.

Des motivations financières : vol de données et espionnage

Des motivations financières peuvent inciter à une attaque contre le système de contrôle d'une infrastructure énergétique. Plusieurs obstacles rendent néanmoins ce choix peu rentable au regard de ce qui pourrait être fait en visant simplement le réseau de gestion de l'entreprise : les systèmes industriels demeurent assez méconnus des *hackers*, et maîtriser les effets de l'attaque sur les installations nécessite des connaissances techniques précises relevant de l'informatique mais aussi de l'automatique. En comparaison, les logiciels de rançon rapportent des milliards d'euros chaque année par des moyens informatiques classiques, sans avoir besoin de viser une infrastructure critique. C'est d'ailleurs le secteur financier qui est le plus visé par les cyberattaques[24].

Enfin, l'espionnage industriel entre également en ligne de compte, bien qu'il soit complexe de copier des équipements en y introduisant un logiciel d'espionnage. Les moyens à engager seraient particulièrement importants, alors que des documents techniques concernant les équipements visés sont souvent stockés sur le réseau de gestion de l'entreprise, ce dernier étant plus facile à attaquer avec des moyens conventionnels. L'attaque de Korea Hydro Nuclear Power en 2014 illustre bien cette logique. Les attaquants n'avaient pas pour but l'espionnage industriel, mais sont parvenus à se procurer les plans et manuels de deux réacteurs sur le réseau de gestion de l'entreprise. Obtenir la configuration des réacteurs en infiltrant un logiciel espion aurait été beaucoup plus complexe. L'attaque de Natanz démontre cependant qu'un certain niveau de repérage est possible de cette manière, à condition de disposer des moyens appropriés.

Un certain nombre d'attaques documentées à l'encontre d'entreprises de l'énergie illustrent donc les raisons pour lesquelles ce secteur est une cible à visée lucrative, mais aussi géopolitique. Si une partie des incidents n'est jamais rapportée ou découverte, on observe cependant une augmentation des attaques contre des infrastructures énergétiques. Alors que la digitalisation croissante de l'industrie de l'énergie l'expose à de nouvelles vulnérabilités, anticiper les risques devient crucial afin d'élaborer des systèmes de protection robustes.

24. Pwc, *Global Economic Crime Survey 2016*, disponible sur : www.securityweek.com, Symantec, *Internet Security Threat Report 2016*, disponible sur : https://resource.elq.symantec.com.

Vulnérabilité du réseau électrique

Quels risques pour nos systèmes électriques d'aujourd'hui… et de demain ?

Le réseau d'électricité : au cœur des infrastructures énergétiques

C'est sur la chaîne d'approvisionnement en électricité que les conséquences d'une cyberattaque auraient le plus d'implications. Les flux sur le réseau électrique sont instantanés, ce qui exclue toute possibilité de réagir manuellement afin d'endiguer les conséquences d'une attaque à grande échelle. L'intégration des réseaux électriques européens les rend plus résilients, mais expose également chaque pays aux instabilités de ses voisins. C'est de cette manière qu'en 2006[25], la déconnexion sans préavis d'une ligne haute tension en Allemagne a privé 15 millions d'Européens d'électricité durant quelques heures. S'il s'agit là des résultats d'une erreur de communication entre les dispatcheurs et que les réseaux européens ont considérablement évolué depuis 2006, cet événement illustre les implications que pourrait avoir une cyberattaque sur les systèmes électriques européens, dans un scénario similaire à celui de l'Ukraine, mais porté à l'échelle d'un continent.

Les premières conséquences d'une attaque sur le réseau d'électricité seraient financières. En considérant par exemple que pour RTE le coût moyen d'un MWh non délivré avoisine les 26 000 euros[26], la perte d'une poche de consommation de 10 MW durant deux heures atteint le demi-million d'euros de pertes. À l'échelle d'un État, la compagnie d'assurances Lloyd's a simulé les coûts d'une cyberattaque sur plusieurs générateurs d'électricité aux États-Unis dans un rapport en 2015. La mise hors-service

25. Union for the Coordination of Transmission of Electricity UCTE, *Final Report, System Disturbance on 4 November 2006*, disponible sur: www.entsoe.eu.
26. Coût d'une coupure de courant supérieure à 3 minutes : voir la Programmation pluriannuelle de l'énergie, disponible sur : www.developpement-durable.gouv.fr.

du réseau dans 15 États engendrerait un coût total pour l'économie américaine de 243 milliards à un trillion de dollars[27].

Le secteur électrique est un acteur clé à sensibiliser en matière de risque cyber en sa qualité de fournisseur de services essentiels : si l'approvisionnement en électricité était interrompu durant plusieurs jours, d'autres infrastructures critiques (santé, transports, communications) ne pourraient assurer leurs fonctions que jusqu'au terme de leurs réserves de secours en diesel. Les risques d'effondrement d'autres secteurs de l'économie sont multiples : rupture de la chaîne du froid dans les entrepôts alimentaires, télécommunications réduites à leur strict minimum (armée, services gouvernementaux…), services de traitement et de distribution d'eau en danger… Sans compter que l'industrie énergétique elle-même est dépendante de cet approvisionnement en électricité, ne serait-ce que pour maintenir les systèmes de refroidissement des centrales nucléaires, ou assurer l'approvisionnement en essence. En 2011, un rapport officiel de l'Office of Technology Assessment, organisme de recherche dépendant du Bundestag allemand, a analysé les effets d'une coupure de courant, vaste et prolongée, sur le fonctionnement de la société allemande. Les auteurs démontrent qu'en quelques jours, l'approvisionnement en nourriture et en eau ne pourrait plus être assuré, et mettrait plusieurs semaines, voire des mois dans certains cas, à reprendre un cours normal une fois le courant rétabli[28].

Les risques actuels pour le réseau électrique

Points sensibles du réseau de transport d'électricité

Si l'ensemble de la chaîne de valeur électrique est vulnérable, le réseau de transport en constitue l'élément le plus critique. Son bon fonctionnement assure toute la stabilité du réseau électrique, et son infrastructure dispersée est difficile à protéger.

Les conséquences d'une cyberattaque sur le réseau électrique seraient relativement similaires à des événements physiques tels que des intempéries, et auxquels les exploitants se préparent grâce à des plans de reprise d'activité. Mais la particularité d'une cyberattaque réside dans la possibilité de toucher plusieurs points névralgiques du réseau simultanément. Une telle action aurait des conséquences difficiles à

27. Lloyds and University of Cambridge, *Business Blackout – The Insurance Implications of a Cyber-attack on the US Power Grid*, 2015.
28. Office of technology assessment at the German Bundestag, *What Happens during a Black-Out*, technology assessment studies series, disponible sur : www.tab-beim-bundestag.de.

maîtriser et limiterait la possibilité d'intervention physique des équipes de maintenance. Une source a confirmé qu'il serait possible, par une équipe coordonnée, d'attaquer plusieurs postes électriques de la même manière à condition de connaître un certain nombre de paramètres au préalable.

Alors que dans le cas d'un sabotage physique, au moins une personne par site visé serait nécessaire, une cyberattaque pourrait théoriquement utiliser quelques points d'entrée seulement pour répandre un virus au reste des infrastructures du réseau électrique. Une équipe de chercheurs d'OpenSource Security[29] est d'ailleurs parvenue à créer un ver capable de se répliquer d'automate en automate, sans avoir besoin de passer par un ordinateur[30]. Même si ces automates ne sont pas reliés en réseau, il suffirait d'attendre qu'une erreur humaine soit commise, par exemple, l'utilisation d'une clé USB sur plusieurs postes électriques lors d'une opération de maintenance propageant ainsi le virus. Programmer le virus pour déclencher une action simultanée sur tous les automates est également possible. Les créateurs du *PLC Blaster* estiment que ce type de menace se développera fortement dans les années à venir[31].

Les systèmes de contrôle et de commande régionaux ou nationaux[32] des opérateurs du réseau électrique peuvent également être des cibles, et induire des conséquences plus lourdes encore que des attaques de postes électriques. Les SCADA des opérateurs permettent de gérer l'acheminement de l'électricité en fonction des données du réseau, récoltées par une multitude de capteurs. Tant que ces systèmes fonctionnent, il est toujours possible de procéder à des ajustements afin de limiter les coupures en cas de ruptures d'alimentation dans certaines zones, ou de cyberattaques localisées. Cependant, si le système de commande principal d'un gestionnaire de réseau de transport est attaqué, tel qu'en Ukraine, l'opérateur est alors privé d'une vision de l'état du réseau essentielle à la conduite de ses opérations. Sur un court laps de temps, celles-ci peuvent être maintenues relativement normalement, mais le

29. Open Source Security est une entreprise allemande de sécurité des réseaux, effectuant notamment des tests d'intrusion pour les gouvernements et les entreprises. Ses équipes recherchent constamment de nouvelles vulnérabilités qu'elles divulguent avec précaution, une fois qu'un correctif de sécurité a été trouvé. La création de PLC Blaster a été présentée à la conférence Black Hat Asia 2016 à Singapour.

30. R. Spenneberg, M. Brüggemann et H. Schwartke, *PLC-Blaster: A Worm Living Solely in the PLC*, 2016, disponible sur : www.blackhat.com.

31. Securityweek, « PLC Worms Can Pose Serious Threat to Industrial Networks », 2016, www.securityweek.com.

32. Les SCADA peuvent se retrouver au niveau des installations locales (comme au sein des postes électriques) et sont supervisés par le même type de logiciel à plus grande échelle. En France il existe plusieurs SCADA régionaux, mais selon la configuration du réseau électrique et du nombre d'opérateurs un seul SCADA national, prend en charge la totalité des opérations.

risque de faire une erreur aux conséquences importantes pour l'équilibre du réseau augmente sur la durée. Dans un scénario très improbable, mais possible selon plusieurs sources, dans lequel de grandes parties du réseau européen seraient touchées, seules les îles Britanniques pourraient ne subir aucun dégât en raison des liaisons en courant continu qui les isolent des instabilités du système européen.

Une protection totale impossible

En France, de nombreuses mesures de protection physique des installations ont été instaurées, constituant une défense efficace en cas de cyberattaque du réseau électrique.

Dans le cas d'une attaque directement sur les SCADA d'un poste électrique (destruction du système, empêchement de contrôler le poste à distance, exécution de commandes qui n'ont pas lieu d'être), une intervention manuelle peut en endiguer les effets à l'échelle locale. Une partie de ces infrastructures n'est pas indispensable à la stabilité du réseau et peut être déconnectée sans dommages (si ce n'est financiers et « réputationnels »). Les composants des postes électriques qui auraient été dégradés par une prise de contrôle à distance des machines peuvent être remplacés relativement aisément.

En France, les systèmes de commande régionaux qui supervisent le fonctionnement de toutes les infrastructures de terrain sont doublés, ne serait-ce que pour des questions de maintenance d'un autre SCADA localisé sur un autre site. Plus de 70 autres outils de conduite peuvent servir de secours en cas de panne simultanée ou dysfonctionnement d'un SCADA régional et de son doublon.

Les systèmes d'information d'importance vitale (SIIV) du réseau, c'est-à-dire ceux qui sont indispensables au bon fonctionnement des opérations, font l'objet de mesures de sécurité imposées, du moins en France, par la Loi de programmation militaire (LPM) de 2013. Les Points d'importance vitale (PIV), c'est-à-dire les sites particulièrement importants du réseau comme certains postes électriques, font également l'objet d'une politique de protection physique significative depuis 2006[33].

Cependant, même avec ces mesures de protection, la sécurisation totale des installations électriques est impossible, tout comme la prévention d'actes de sabotage physiques par des personnes très motivées. Certaines infrastructures sont difficiles à protéger, comme les postes électriques, répartis sur tout le territoire, souvent en zone isolée. Toute la

33. Décret n° 2006-212 du 23 février 2006 relatif à la sécurité des activités d'importance vitale.

difficulté pour les professionnels de la sécurité est d'envisager le type et l'ampleur des attaques possibles, alors que la digitalisation de l'industrie est en constante progression et que les TIC acquièrent sans cesse de nouvelles fonctionnalités, potentiellement porteuses de nouvelles failles. Le déploiement d'un certain nombre d'objets connectés accompagnant la transition énergétique augmentera le nombre de points d'entrée sur les réseaux et avec eux, la surface d'attaque disponible.

Digitalisation et transition énergétique : anticiper les risques

Vulnérabilités d'un réseau électrique en mutation

Grâce aux politiques de transition énergétique, les technologies renouvelables sont déployées partout dans le monde. Avec elles augmentent les besoins de nouvelles solutions d'intégration, de stockage et de gestion de l'offre et de la demande. Les réseaux intelligents et les compteurs communicants sont des éléments essentiels de ce nouveau système énergétique qui se veut plus efficace, plus résilient et moins polluant.

Les aspects de cybersécurité doivent donc être anticipés dès à présent afin d'assurer la sécurité et la résilience du système énergétique au gré de ses mutations. Pourtant, les projets d'énergies renouvelables n'intègrent pas d'aspect cybersécurité dans leur conception, alors que ces installations sont de plus en plus la cible d'attaques[34]. Mettre hors-service un parc éolien n'aurait, à l'heure actuelle, pas d'impact significatif pour l'équilibre du réseau, et ne présenterait pas de réel danger environnemental ou humain. La déconnexion simultanée de plusieurs installations risque en revanche de poser des problèmes plus importants à l'avenir.

Notre réseau électrique de demain[35] sera composé d'une multitude de producteurs individuels, ainsi que de nouveaux acteurs tels que des agrégateurs. Ces derniers seront l'intermédiaire entre le système électrique et les utilisateurs (particuliers, logements collectifs, industriels…), avec pour rôle d'optimiser le fonctionnement d'un ensemble de producteurs décentralisés. Certains ont déjà la main sur des fonctions importantes telles que des délestages partiels de certains usages électriques des sites dont ils ont la charge, ou encore le démarrage de groupes électrogènes de

34. Plus d'informations sur :www.windpowerengineering.com.
35. Massachusetts Institute of Technology. (2011). *The Future of the Electric Grid*, disponible sur : http://energy.mit.edu.

secours[36]. Afin de piloter ces « centrales électriques virtuelles », les agrégateurs ont également recours à des systèmes de contrôle, comme ceux qui sont actuellement utilisés pour gérer le transport et la distribution d'électricité. Issus du marché car moins onéreux que les systèmes propriétaires, leurs spécificités pourraient donc être accessibles à des personnes mal intentionnées. Au-delà du risque pesant sur la stabilité du réseau, il est important d'anticiper le danger physique pour les producteurs individuels qui posséderont des équipements chez eux (comme des batteries).

Compteurs communicants

Volet important de la transition énergétique, le déploiement des compteurs communicants soulève des questions de sécurité et de protection des données collectées. Lors de la conférence Black Hat Europe 2014, deux professionnels de la sécurité informatique[37] ont en effet démontré qu'il était possible de pirater certains compteurs espagnols[38], dont les communications entrantes et sortantes étaient pourtant chiffrées. En quelques mois, ils ont découvert que la clé de sécurité est identique sur tous les appareils, qu'il est possible d'envoyer des faux rapports de consommation à l'opérateur, ou encore d'utiliser leur fonctionnement en réseau pour modifier le comportement des autres compteurs connectés… Ces actions sur plusieurs milliers de compteurs à la fois sont à même de déstabiliser le réseau de distribution, voire créer des coupures de courant sur des zones importantes.

En France, Enedis porte une attention particulière à la cybersécurité de ses compteurs Linky, dont 35 millions de modèles seront déployés sur le territoire français d'ici 2021. L'accent est particulièrement mis sur la protection des données du consommateur, principal point d'accroc pour leur acceptation. Tout est également mis en œuvre pour qu'ils ne puissent être manipulés : les échanges de données avec un concentrateur sécurisé sont chiffrés et ne passent pas par internet mais directement par le réseau électrique et le réseau de téléphonie. Les données sont envoyées vers les *data centers* d'Enedis, strictement isolés. Le concentrateur qui récupère et renvoie les informations des compteurs vers le *data center* est doté d'un « module de sécurité », c'est-à-dire un composant matériel inviolable qui

36. Commission de Régulation de l'Énergie, disponible sur : www.smartgrids-cre.fr.
37. Javier Vazquez Vidal et Alberto Garcia Illera, connus pour avoir également démontré qu'il était possible de hacker une voiture ou certains systèmes de transports urbains. Pour voir leur intervention à la conférence Black Hat Europe 2014 : « Lights Off! The Darkness of the Smart Meters », disponible sur : www.youtube.com.
38. « Popular Electricity Smart Meters in Spain Can Be Hacked, Researchers Say », *Reuters*, 2014, disponible sur : http://uk.reuters.com.

permet de générer et stocker les clés privées de chiffrement utilisées pour les transferts de données. D'autres mesures ont été mises en place et respectent strictement les référentiels de l'ANSSI en matière de cybersécurité.

Cependant, si la résistance à toute sorte d'intrusions a été testée au préalable, les experts s'accordent à dire que, de la même manière que pour tout autre objet connecté intégrant des fonctions numériques, l'existence de failles ne peut être exclue. Les avis des personnes rencontrées divergent sur l'étendue des risques. Certains affirment qu'à partir d'un certain degré de motivation, de technicité et de moyens financiers, des attaquants parviendront à leurs fins, quel que soit le niveau de protection. La résilience de nos systèmes énergétiques est donc un aspect essentiel de la cybersécurité.

Les réseaux intelligents et les compteurs communicants ont la particularité d'augmenter singulièrement le nombre de points d'entrée sur un réseau où s'échangent des donnés. Dans la mesure où les compteurs sont tous configurés de la même manière et peuvent donc être porteurs des mêmes failles, ils augmentent considérablement la surface d'attaque disponible[39]. Considéré comme un élément clé de la création de villes intelligentes, le développement de « l'internet des objets », qui n'en est qu'à ses balbutiements, accentuera encore cette tendance. L'interaction d'appareils électroniques privés dont l'usage ne peut être contrôlé (téléphones portables, appareils électroménagers) avec des composantes du réseau électrique, rendra les besoins en cybersécurité plus pressants encore.

Pourtant, la cybersécurité des infrastructures énergétiques et son rôle dans la sécurité d'approvisionnement ne font l'objet d'aucune disposition spécifique en France, ni dans la loi de transition énergétique, ni dans le « volet relatif à la sécurité d'approvisionnement, au développement des infrastructures et de la flexibilité du système électrique » du projet de programmation pluriannuelle de l'énergie. Les aspects techniques sont certes traités par l'ANSSI qui soutient l'industrie énergétique dans la sécurisation de ses installations, mais une réflexion stratégique sur l'impact du risque cyber sur la structure du système énergétique de demain n'a pas encore été menée.

39. T. McLarty et T. J. Ridge (Eds), « Securing the U.S. Electric Grid », Washington D.C., The Center for the Study of the Presidency and Congress, 2014, disponible sur : www.thepresidency.org.

Le cas du nucléaire : faut-il être alarmiste ?

L'industrie nucléaire possède une culture de la sûreté développée en raison du niveau de risque physique élevé auquel elle fait face, et donc une habitude de pratiques drastiques pouvant être transposées aux enjeux de cybersécurité. Par ailleurs, de nombreux mécanismes de protection physique instaurés de longue date sont un frein considérable à la perpétration d'une cyberattaque.

Tout d'abord, les équipements et leurs processus de communication sont dupliqués de multiples manières : le réseau Ethernet est doublé, les équipements sont redondés sur site, et les fonctions de sécurité sont également assurées par des équipements supplémentaires déportés sur des sites distants. Les capteurs sur les équipements critiques d'une tranche doivent donc remonter les informations par quatre câbles indépendants. Un système de vote impose d'avoir au moins trois versions concordantes d'une information transmise pour être considérée comme fiable. Les seules informations sortant du réacteur d'une centrale nucléaire à destination d'un acteur tiers concernent les données de tension et de puissance, échangées toutes les cinq secondes avec le réseau de transmission d'électricité, afin d'ajuster la production en fonction de la demande. Aucune autre sorte de communication avec l'extérieur n'est admise par le réseau d'une centrale.

Dans le cas d'une cyberattaque qui parviendrait à couper l'alimentation en électricité d'une centrale (nécessaire au fonctionnement des systèmes de sécurité), l'ilotage, c'est-à-dire la réduction de puissance de production pour que la centrale puisse s'alimenter elle-même en électricité, fonctionne dans 80 % des cas. En solution alternative, chaque tranche dispose de plusieurs générateurs indépendants, et d'un générateur de secours qui peut être affecté aux différentes tranches. Il est donc également très difficile d'attaquer les systèmes d'alimentation d'urgence. Cet aspect a été particulièrement renforcé depuis la catastrophe de Fukushima. En effet, à la suite de cet événement la Commission européenne a lancé, entre 2011 et 2012, une campagne sans précédent de tests de résistance sur tous les sites nucléaires européens à l'issue de laquelle un rapport a été émis afin de renforcer la sécurité de certains sites[40].

40. Commission européenne, *Technical Summary on the Implementation of Comprehensive Risk and Safety Assessments of Nuclear Power Plants in the European Union*, Corrigendum du document SWD (2012) 287 (2012), Bruxelles, , 22 août 2013, disponible sur : http://eur-lex.europa.eu.

Celui-ci montre bien que toutes les centrales nucléaires françaises (et la plupart en Europe) étaient équipées d'une salle de commande de secours avant 2012. Dans le cas où le système de contrôle commande serait atteint, un second, lui-même localisé hors site et configuré différemment est disponible. L'accès aux sites est également particulièrement contrôlé, notamment par des procédures de « condamnations administratives ». De plus, la plus grande partie du parc nucléaire français (les réacteurs 900 MW et 1 300 MW), a été construite avant l'apparition du numérique dans le secteur énergétique, et fonctionne donc encore en analogique (hors quelques fonctions de supervision), ce qui rend beaucoup plus difficile leur corruption par un logiciel malveillant. Le programme Grand Carénage qui prévoit un investissement de 51 milliards d'euros jusqu'en 2025[41] afin de moderniser cette partie du parc, ne vise pas à passer les fonctions critiques en numérique.

Ces mesures, pensées à l'origine pour permettre de garder le contrôle sur les opérations en cas d'incendie, de radiations ou tout autre incident physique, limitent non seulement la possibilité d'introduire un programme malveillant dans les parties les plus critiques des centrales, mais également les marges d'action d'une attaque.

La numérisation progressive du secteur nucléaire soulève malgré tout certaines questions. Seuls quatre réacteurs en France (les N4) et les EPR intègrent ces systèmes de contrôle modernes[42]. Cependant, leur conception a incité EDF à revoir certains équipements, à la centrale de Chooz notamment[43]. En 2009, les autorités de sûreté nucléaire de la France, du Royaume-Uni et de la Finlande ont publié une position commune exprimant leurs réserves quant au système de commande numérique des EPR, soulignant que celui-ci « n'est pas conforme [au] principe d'indépendance dans la mesure où il y a beaucoup d'interconnexions complexes entre les systèmes de contrôle et de sûreté[44] ». L'Institut de Radioprotection et de Sûreté Nucléaire estimait la même année que « cette évolution vers davantage de complexité soulève des problèmes de fond et

41. EDF, grand Carénage : chiffres clés disponibles sur : www.edf.fr.
42. Ces systèmes servent de solution de regroupement des moyens de surveillance et d'action. Le système informatisé permet de remonter en temps réel les informations des quelque 12 000 capteurs qui contrôlent l'état des équipements en permanence.
43. V. Nouyrigat, « EPR – Les 4 erreurs de la filière française », *Science & Vie*, n° 1113, juin 2010, p. 94.
44. *Déclaration commune sur le réacteur EPR*, Autorité de Sureté Nucléaire (ASN), 2009, disponible sur : www.asn.fr.

que de futures conceptions ne devraient pas continuer à évoluer dans ce sens[45] ».

Le système de contrôle de l'EPR d'Olkiluoto, en Norvège, a finalement été doublé d'un système annexe et indépendant de toute informatique[46]. L'Angleterre a poussé plus loin sa requête pour le projet Hinkley Point et dupliqué toutes sortes de processus, en surcroît des fonctions vitales des deux tranches. Certains experts estiment que ces mesures sont certes compréhensibles, mais risquent d'augmenter la complexité du système sans forcément en accroître la résilience. L'architecture du contrôle commande de l'EPR de Flamanville a également été revue pour renforcer l'indépendance des processus de sûreté vis-à-vis de l'informatique[47].

La numérisation touche donc également le secteur nucléaire, et questionne en partie son modèle de sûreté. Des procédures de sécurité drastiques rendent cependant très complexe la possibilité de menacer les équipements physiquement pas le biais d'une cyberattaque. L'industrie nucléaire demeure très contrôlée avec une bonne connaissance des enjeux, du moins en France, et s'adapte facilement aux réglementations qui se mettent en place.

45. Institut de radioprotection et de sûreté nucléaire (IRSN), *Synthèse du rapport de l'IRSN portant sur l'architecture du contrôle-commande du réacteur EPR de Flamanville 3 et les plateformes associées*, 2009, disponible sur : www.irsn.fr.
46. Non Computerised Safety System (NCSS).
47. Autorité de sûreté nucléaire (ASN), « L'ASN lève ses réserves sur le contrôle commande de l'EPR Flamanville 3 », 2012, disponible sur : www.asn.fr.

Cybersécurité des systèmes énergétiques : structurer les réponses française et européenne

De nombreux moyens existent pour protéger les systèmes énergétiques des cyberattaques. Les attaques Stuxnet et BlackEnergy démontrent en effet qu'un certain nombre de mesures auraient pu permettre de les détecter durant leur préparation.

La « défense en profondeur[48] » est le principe qui assure au mieux la protection des parties critiques d'un système, l'objectif étant de superposer des défenses variées, pour que l'attaquant se heurte à une nouvelle strate de sécurité après chaque obstacle surmonté. Assurer des principes de sécurité de base, tels que séparer les réseaux de gestion et opérationnels de l'entreprise, installer des pare-feu, changer des mots de passe par défaut des automates et objets connectés lorsque cela est possible et imposer des procédures « d'hygiène » drastiques (interdiction pour les employés de connecter des objets non vérifiés, faire tester tous les nouveaux équipements avant de les installer…), pourrait significativement réduire les risques. La cybersécurité en milieu industriel « c'est 80 % d'organisation, et 20 % de technique », rappelle une personne interrogée. C'est aussi la garantie de dissuader à moindre coût les attaquants les moins performants.

La formation des employés est également cruciale : les attaquants comptent la plupart du temps sur l'erreur humaine pour entrer dans un système. Une personne travaillant dans la sécurité industrielle a en effet déclaré lors d'un entretien que la manière la plus aisée d'introduire un logiciel malveillant au sein d'une installation industrielle serait de disperser des clés USB infectées sur le parking de l'entreprise. Il suffirait ensuite d'attendre qu'un employé s'en serve sur le site.

Ces mesures sont à la portée des entreprises qui pourtant peinent parfois à identifier les actions prioritaires à mener. C'est pourquoi la

48. ANSSI, *Maîtriser la SSI pour les systèmes industriels*, 2012, disponible sur : www.ssi.gouv.fr.

France et certains de ses voisins ont choisi la voie de la réglementation pour les accompagner dans leur mise à niveau.

Une vision française : le choix de la réglementation

Une approche novatrice

Dès 2009, l'Agence nationale de la sécurité des systèmes d'information (ANSSI), qui compte aujourd'hui parmi les agences les plus développées d'Europe (environ 500 personnes), était créée afin de donner au pays les moyens de lutter contre le risque cyber. Ses pouvoirs ont été étendus en 2011 alors que la Stratégie nationale de cybersécurité voyait le jour[49]. La Loi de programmation militaire (LPM[50]) adoptée en 2013 posait les premiers jalons juridiques d'une politique de cybersécurité pour la France. Celle-ci fixe notamment les règles pour les quelque 200 opérateurs d'importance vitale (OIV) identifiés par le décret[51] relatif à la sécurité des activités d'importance vitale de 2006, c'est-à-dire des entreprises, usines, opérateurs et 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 capacité de survie de la Nation[52] ». Ces opérateurs font l'objet d'obligations strictes en matière de sécurité des systèmes d'information, sous peine d'amende (150 000 euros).

En août 2016, la France était le premier pays[53] à publier des arrêtés sectoriels pour ses OIV (hydrocarbures[54], gaz[55], électricité[56] pour le secteur énergétique) comprenant une liste de mesures à mettre en place par les entreprises pour protéger leurs systèmes d'information, dont :

49. Stratégie nationale pour la sécurité du numérique, 2011, disponible sur : www.ssi.gouv.fr.
50. 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 (2013). Voir article « Chapitre IV : Dispositions relatives à la protection des infrastructures vitales contre la cyber-menace », article 22, disponible sur : www.legifrance.gouv.fr.
51. Décret n° 2006-212 du 23 février 2006, relatif à la sécurité des activités d'importance vitale, disponible sur : www.legifrance.gouv.fr;
55. Article L1332-6-1 du code de la défense.
53. ANSSI, « Cybersécurité des OIV : publication d'une nouvelle vague d'arrêtés sectoriels », 2016, disponible sur : www.ssi.gouv.fr.
54. 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.
55. *Ibid.*
56. *Ibid.*

- Fournir sous trois mois à l'ANSSI une liste de leurs systèmes d'information d'importance vitale (SIIV).
- Mettre en place une politique de sécurité des systèmes d'information (PSSI) décrivant les moyens mis en œuvre afin de protéger les SIIV. Cette politique doit inclure une procédure d'homologation du système d'information tous les trois ans.
- Cartographier les systèmes existants : un certain nombre d'installations sont en place depuis plusieurs décennies et la position, la configuration de chaque équipement ou réseau sur le site industriel ne sont souvent pas connues parfaitement des opérateurs. Une entreprise telle que RTE disposant de 2500 postes électriques[57] répartis sur tout le territoire doit avoir une vision très précise de ses systèmes déployés. Si RTE a de longue date effectué le recensement de son patrimoine, ce n'est pas le cas de nombreuses entreprises. Les résultats doivent également être transmis à l'ANSSI.
- Notifier l'ANSSI sans délais de tout incident de cybersécurité dans le but notamment de créer une accidentologie qui permettra de mieux anticiper les prochaines attaques.
- D'autres pratiques sont désormais imposées, comme l'obligation de planifier l'installation d'une nouvelle version d'un logiciel, programme ou mise à jour afin d'éviter la conservation de versions obsolètes.

Les arrêtés prévoient des clauses d'exception afin de tenir compte des équipements existants, sur lesquels les mises à jour ou l'application de correctifs de sécurité sont impossibles[58]. Celles-ci seront réévaluées par l'ANSSI en coopération avec l'industrie, afin de les adapter aux évolutions technologiques et inciter l'investissement dans du matériel plus sécurisé.

Un système de certification est également mis en place par l'ANSSI, afin de donner un label à des équipements testés par l'agence[59], et permettant ainsi aux industries de l'énergie de disposer d'une offre adaptée à leurs activités. Siemens, dont une faille dans l'un de ses automates avait été révélée par Stuxnet, a restructuré une partie de son activité depuis lors, afin de proposer des produits intégrant la sécurité « en natif », et fait

57. RTE, *Memo 2014*, disponible sur : www.rte-france.com.
58. « Lorsque des raisons techniques ou opérationnelles le justifient, l'opérateur peut décider [...] de ne pas installer une version supportée par le fournisseur ou le fabricant de la ressource concernée ou de ne pas installer une mesure correctrice de sécurité. Dans ce cas, l'opérateur met en œuvre des mesures techniques ou organisationnelles prévues par cette procédure pour réduire les risques. »
59. ANSSI, Certification de sécurité de premier niveau des produits des technologies de l'information, 2014, disponible sur : www.ssi.gouv.fr.

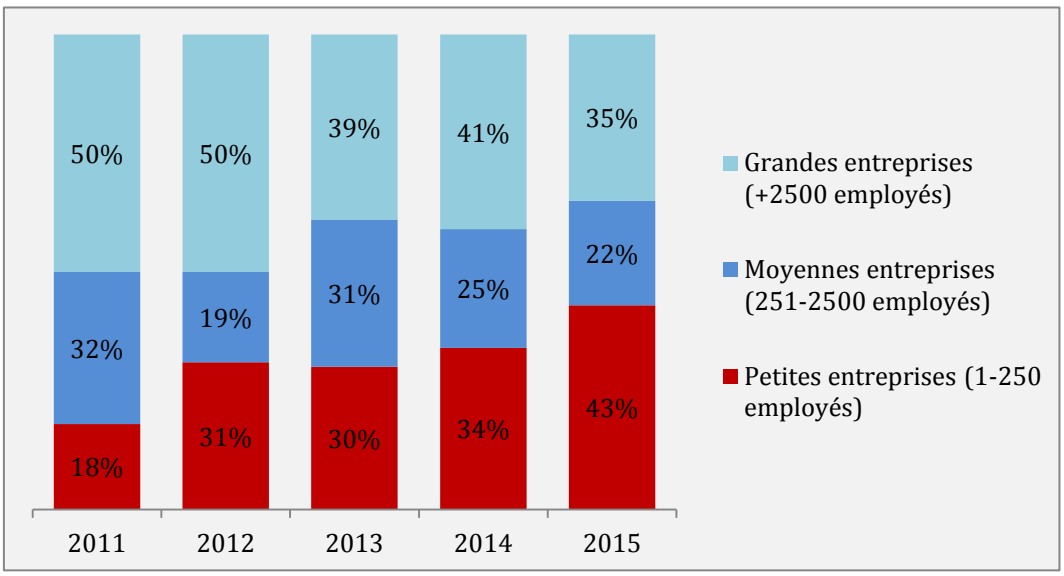
désormais partie des premiers équipementiers à avoir fait certifier un de ses automates. Schneider Electric tente également de faire de la cybersécurité un axe de compétitivité, et la réglementation française lui permet justement d'espérer voir un marché dynamique de la cybersécurité industrielle se développer.

L'approche française implique fortement les entreprises de l'énergie (comme les autres OIV pour la réglementation qui les concerne) dans le processus d'élaboration de ces arrêtés afin d'apporter des réponses adaptées à leurs besoins spécifiques. Une manière de faire qui permet de gagner la confiance de ces acteurs, qui loin d'être réticents à l'idée d'une réglementation reconnaissent l'intérêt de se référer à des mesures claires.

Des obstacles à surmonter

La législation ambitieuse adoptée en France pose cependant certaines difficultés. La plupart des petits acteurs, même parmi les OIV, n'ont pas forcément les ressources pour désigner un référent de sécurité des systèmes industriels, mener les audits et construire une PSSI ambitieuse. Or les dernières analyses des entreprises de la sécurité informatique démontrent que les PME sont depuis quelques années les cibles croissantes d'attaques.

Attaques par hameçonnage par taille d'entreprise dans le monde (2011-2015)



Source : D'après Symantec.

Si le risque cyber est désormais bien identifié au sein de l'industrie énergétique, il ne fait pas toujours partie des priorités budgétaires. En 2015, un rapport de Chatham House évoquait par ailleurs le manque de sensibilité au problème de la cybersécurité de la part des opérateurs d'infrastructures critiques en Europe[60].

Les solutions de sécurité industrielle sont, selon une personne interrogée, particulièrement onéreuses, dans un contexte où le marché est encore peu consolidé et l'offre rare. Les automates certifiés proposés par les équipementiers sont encore peu nombreux, et nécessitent un remplacement des équipements existants, ce qui représente un coût considérable.

Les arrêtés sectoriels précisent par ailleurs que l'opérateur devra installer un système de « sondes d'analyse de fichiers et de protocoles[61] » afin d'améliorer la détection des événements susceptibles d'affecter la sécurité. Si cette étape est indispensable afin d'analyser les flux suspects sur un réseau, à l'instar des flux générés par l'attaque des opérateurs ukrainiens durant la phase de repérage, elle soulève des questions parmi les industriels. Cela implique en effet de disperser dans des infrastructures anciennes des objets totalement électroniques, dont la durée de vie est bien inférieure aux équipements à surveiller. Ces objets seront donc sujets à des remplacements plus fréquents dans un environnement où limiter les allées et venues fait partie intégrante de la sécurité.

En dépit d'une évolution certaine dans la compréhension des enjeux et des standards de sécurité adoptés, l'industrie énergétique devra consentir à d'importants efforts pour s'adapter à la législation. Le cadre réglementaire français laisse espérer l'émergence de solutions certifiées pour les OIV, qui pour l'heure doivent composer avec des équipements existants difficiles à protéger. Cette protection ne sera pourtant pas optimale tant que toute la chaîne de valeur n'y est pas soumise, au moins à l'échelle européenne.

60. C. Baylon, R. Brunt et D. Livingstone, « Cyber Security at Civil Nuclear Facilities », *Chatham House Report*, 2015.

61. Les sondes sont des systèmes de détection d'intrusions visant à automatiser la surveillance d'événements survenant dans un réseau ou sur une machine. Elles signalent à l'administrateur système toute trace d'activité anormale sur ce dernier ou sur la machine surveillée.

L'Union européenne, échelon indispensable

Une mise à niveau nécessaire

Sur le plan européen, la législation intègre peu à peu les exigences de cybersécurité. Le Paquet d'hiver[62] publié par la Commission européenne à l'automne 2016, introduit pour la première fois dans la réglementation européenne des obligations concernant la cybersécurité en matière d'énergie. Le projet de Règlement sur la préparation des risques dans le secteur électrique[63] indique que les États membres ont des pratiques de gestion des risques différentes, non coordonnées et essentiellement tournées vers le contexte national, sans se préoccuper de la situation transfrontalière. Le projet de Règlement sur le marché intérieur électrique stipule donc que les mesures pour assurer la protection des données et la cybersécurité devront être dictées par un code de réseau élaboré au niveau européen[64]. La version préliminaire du code de réseau rédigée par Entso-e sur la sécurité opérationnelle[65], validée par les États membres et en attente d'approbation par le Parlement européen et le Conseil avant son entrée en vigueur, oblige par ailleurs les opérateurs de transmission d'électricité à établir des scénarios de cyberattaques et évaluer les moyens de s'en prémunir. Ces nouvelles réglementations viennent ainsi compléter la principale avancée juridique en matière de cybersécurité en Europe : la directive sur la sécurité des réseaux et de l'information (SRI), adoptée le 6 juin 2016[66], qui impose désormais à tous les membres de l'UE de désigner une autorité nationale en charge des questions de cybersécurité. Le projet de directive a créé un effet de mise à niveau lors de sa publication en 2013, alors que plus de la moitié des pays européens ne disposaient d'aucune institution compétente en la matière. Depuis 2013, presque tous les pays ont mis en place des mesures pour remplir les conditions de la

62. Le paquet « Énergie propre pour tous les Européens », est un ensemble de mesures législatives (directives, règlements et leurs annexes techniques) présenté par la Commission européenne le 30 novembre 2016, ayant pour but de maintenir l'Union européenne compétitive sur les marchés de l'énergie et en tant qu'acteur de la transition énergétique. Plus d'informations sur : http://ec.europa.eu.

63. Commission européenne, « Proposal for a Regulation of the European Parliament and of the Council on Risk-preparedness in the Electricity Sector and Repealing », Directive 2005/89/EC, disponible sur : https://ec.europa.eu.

64. Article 55, « Proposal for a Regulation of the European Parliament and of the Council on the Internal Market for Electricity », 2016/0379 (COD), disponible sur : http://eur-lex.europa.eu.

65. Article 26, « Network Code on Operational Security, Commission Regulation, Establishing a Guideline on Electricity Transmission System Operation », disponible sur : www.entsoe.eu.

66. Proposition de directive du Parlement européen et du Conseil concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et de l'information dans l'Union, NIS Directive, disponible sur : http://eur-lex.europa.eu.

directive. Des décalages importants persistent cependant entre les règles de cybersécurité, les instruments juridiques et les capacités opérationnelles des États membres (Annexe 4). Cette situation fragilise l'ensemble des infrastructures européennes, étroitement interconnectées.

La directive SRI pose donc des bases communes de sécurité pour les systèmes d'information, permettant ainsi d'éviter la création de maillons faibles qui mettraient à mal toutes les mesures prises par les pays les plus matures sur la question. La directive met également l'accent sur les « opérateurs de services essentiels », qui au niveau européen regroupent les acteurs dont les activités s'étendent à plusieurs pays membres tels que :

- les fournisseurs d'électricité et de gaz ;
- les gestionnaires de transmission d'électricité et de gaz ;
- les raffineries et usines de traitement ;
- les producteurs de gaz et de pétrole ;
- les opérateurs des marchés d'électricité et de gaz ;
- les opérateurs de gazoducs/oléoducs et de stockage (dont GNL).

Jusqu'à présent, les États membres pouvaient volontairement fournir aux institutions européennes une liste des opérateurs jugés essentiels présents sur leur territoire, mais cette démarche n'avait donné lieu qu'à un nombre infime de déclarations.

La directive impose de plus la mise en place d'une stratégie nationale de cybersécurité. En 2015, seuls 19 États avaient développé un tel plan d'action, parfois incomplet et souvent statique, alors que la rapidité des changements dans ce domaine supposerait une adaptation constante[67]. Elle astreint également chaque État à la création d'un centre d'alerte national (CERT[68]) et la notification des incidents aux autorités nationales par les opérateurs critiques. Les États membres ont 21 mois pour se conformer à ces obligations.

La Commission européenne soutient la mise à niveau des États les moins avancés sur ces questions par le programme de financement pour l'interopérabilité des infrastructures et services numériques (CEF[69]). Doté de 60 millions d'euros sur sept ans, il est destiné à l'achat d'équipements, la mise en place de formations et l'aide au renforcement des capacités

67. BSA, Tableau de bord de la sécurité dans l'UE, 2015, disponible sur : http://cybersecurity.bsa.org. À cet égard, la France a révisé sa propre stratégie en 2015.
68. Computer Emergency Response Team-CERT.
69. Connecting Europe Facility : instrument de financement des infrastructures transeuropéennes pour la période 2014-2020. Plus d'informations sur : https://ec.europa.eu.

institutionnelles. Un partenariat public-privé a également été établi en juillet 2016 entre la Commission européenne et l'association de cybersécurité européenne (European Cyber Security Organisation), dont l'objectif est de stimuler les efforts de recherche appliquée en cybersécurité. L'UE soutiendra cette initiative à hauteur de 450 millions d'euros, et espère un investissement complémentaire en provenance du secteur privé d'un milliard d'euros[70].

L'UE entend aussi renforcer la coopération entre les États membres, en instaurant deux réseaux d'échange : un réseau constitué de tous les CERT nationaux afin de partager des détails techniques[71], ainsi qu'un réseau impliquant la Commission européenne et les institutions nationales. L'objectif de ces mesures est de motiver la diffusion d'informations pour créer une culture commune de la cybersécurité. Celle-ci cependant n'est pas toujours aisée à développer.

Une harmonisation difficile

Un certain nombre de pays, dont la France, ont milité pour assouplir le degré de contrainte de la directive par rapport à la proposition initiale de la Commission européenne[72], en particulier sur le partage d'informations sensibles avec d'autres pays de l'UE. La France et l'Allemagne collaborent presque quotidiennement et mettent en place un cadre similaire, mais le principe du partage d'informations contraignant et systématique avec l'ensemble des pays membres n'a pas été inclus dans le fonctionnement des réseaux d'échange.

De même, des systèmes de certification naissent dans les pays dont les législations sont les plus matures comme en France et en Allemagne, mais soulèvent des questions d'harmonisation auxquelles la Commission européenne espère pouvoir répondre par un référentiel commun. À plus long terme, un système de certification identique à tous les pays membres imposerait également de créer une agence de certification européenne, requérant l'emploi de 30 000 à 60 000 personnes pour assurer tous les besoins en certification, solution difficilement envisageable. L'alternative serait donc de faire certifier les produits par des instances nationales, ce qui soulève des questions diplomatiques au sein même de l'UE. Certains

70. Commission européenne, *Commission Signs Agreement with Industry on Cybersecurity and Steps Up Efforts to Tackle Cyber-Threats*, 5 juillet 2016, disponible sur : http://europa.eu.
71. Animé par l'ENISA : European Union Agency for Network and Information Security.
72. Commission européenne, « Directive of the European Parliament and of the Council Concerning Measures to Ensure a High Common Level of Network and Information Security Across the Union », 2013.

pays n'auront en effet pas les moyens d'accomplir ces tâches et devront faire appel à des laboratoires européens de taille plus importante (probablement allemands comme le BSI, ou français) qui devront être audités en retour par les autres pays membres. Or les compétences en matière de cybersécurité de ces laboratoires reposent en partie sur leurs activités dans la recherche militaire, ce qui rend l'audit par d'autres instances étatiques délicat.

L'harmonisation des normes est également une question cruciale au niveau européen, et à plus long terme au niveau mondial.

L'adoption de normes communes et d'un cadre de reconnaissance de certification permettrait de stimuler une mise à niveau régulière des cadres réglementaires au sein de l'UE, et ainsi empêcher qu'ils ne restent statiques une fois adoptés. C'est aussi le moyen d'assurer que toutes les installations énergétiques européennes soient protégées par un standard minimum de sécurité, même au sein des pays les moins matures sur la question. À ce titre, l'accord du Senior Officials Group Information Systems Security (SOG-IS), rassemblant les autorités nationales de la sécurité des systèmes d'information de dix pays et dont le but est de coordonner la normalisation de profils de protection, peut servir de cadre de base[73]. Développer un système de normes au niveau international sera plus aisé si l'UE est déjà en accord sur un référentiel commun. Sur les questions de standards internationaux, la Commission européenne a constitué un groupe de travail qui collabore avec les États-Unis (dont les normes en matière de cybersécurité au sein de l'industrie électrique et nucléaire sont parmi les plus élaborées[74]) afin d'analyser les bonnes pratiques et standards à généraliser. L'élaboration de normes internationales et d'équivalences reconnues de tous est ardemment défendue par l'industrie, qui redoute d'avoir à exposer la confection de ses équipements à des organismes de certification étrangers. Des discussions bi-annuelles entre l'Europe et la Chine portent d'ailleurs sur ce point, mais l'idée de voir émerger des normes européennes n'est pas très bien accueillie par le pays, de peur qu'elles ne constituent une barrière à l'importation de ses produits. De telles normes sont encore loin de voir le jour en Europe, malgré l'implication de l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA)[75].

73. Senior Officials Group Information Systems Security, disponible sur : www.sogis.org.
74. De la North-American Electrical Reliability Corporation (NERC) pour le nucléaire, NIST très appliqué dans le secteur électrique.
75. Créée en 2004, l'ENISA ou AERSI, soutient les États membres dans le renforcement de leurs capacités techniques, élabore des guides pratiques de référence et participe à la résolution de

Une étude du Parlement européen souligne que si de nombreux progrès ont été effectués sur les questions de cybersécurité en Europe, les efforts manquent de coordination, ce qui risque d'aboutir en une variété de mesures qui laisseraient des failles dans les protections mises en place. Selon ce rapport, l'une des mesures à instaurer en priorité serait la création d'une institution de cybersécurité sectorielle comme référent principal de l'industrie énergétique en Europe, mais cela suppose que les États membres acceptent le principe du partage d'information régulier et obligatoire[76].

Similitudes et divergences des approches

Allemagne

La Stratégie de cybersécurité allemande a été adoptée en 2011, quelques jours après celle de la France, et mettait également l'accent sur la nécessité de protéger en priorité les infrastructures vitales nationales[77]. La loi allemande en matière de cybersécurité (IT Security Act) a finalement été adoptée en 2015 et coïncide fortement avec les obligations de la directive européenne SRI. Cette loi impose comme en France aux opérateurs d'infrastructures critiques d'assurer la protection de leurs systèmes d'information, d'effectuer un audit de sécurité tous les deux ans, de notifier des incidents à l'Office fédéral de la sécurité des technologies de l'information[78] (BSI) ainsi que la nomination d'un point de contact avec le BSI au sein de chaque entreprise critique. Là également, le non-respect de la loi peut se traduire par une amende[79]. L'ordonnance adoptée en avril 2016 précise les critères qui permettent de déterminer quelles sont les infrastructures considérées comme vitales[80]. Le nombre d'opérateurs jugés vitaux serait plus élevé qu'en France (2000), bien que la liste complète demeure confidentielle. L'approche allemande n'introduit pas de distinction entre les opérateurs critiques des différents secteurs.

problèmes rencontrés par les Etats membres en matière de sécurité des réseaux et des systèmes d'information.

76. European Parliament, Directorate General for Internal Policies, Cyber Security Strategy for the Energy Sector, 2016, disponible sur : www.europarl.europa.eu.

77. *Cyber Security Strategy for Germany*, Ministère fédéral de l'Intérieur, 2011, www.bsi.bund.de.

78. Bundesamt für Sicherheit in der Informationstechnik.

79. « Gesetz zur Erhöhung der Sicherheit informationstechnischer Système (IT-Sicherheitsgesetz) », *German Federal Law Gazette*, 2015, n° 31, p. 1324, disponible sur : www.bgbl.de.

80. Règlement déterminant les infrastructures critiques après la loi BSI – Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSIGesetz (BSI-Kritisverordnung – BSI-KritisV), 22 avril 2016, disponible sur : www.gesetze-im-internet.de.

La loi, discutée au Bundestag depuis 2013, a été fortement critiquée par l'industrie allemande, la jugeant à la fois vague et stricte au point de risquer d'affaiblir sa compétitivité[81]. En revanche, deux partenariats public-privé sont à l'œuvre en Allemagne et bien établis : UP KRITIS rassemble les opérateurs d'infrastructures critiques, les associations des industries et des institutions publiques dans le but de développer des structures communes de réponse aux incidents et partager l'analyse des risques. L'Alliance pour la cybersécurité a été établie en partenariat entre le BSI et Bitkom, l'association de l'industrie numérique allemande, afin de créer une plateforme d'échange d'informations à laquelle plus de 1 200 institutions participent[82].

Ainsi, la législation en Allemagne est très similaire aux orientations prises par la France en matière de cybersécurité des infrastructures critiques, bien qu'elle n'impose pas de mesures spécifiques à l'industrie énergétique[83] comme peuvent le faire les arrêtés sectoriels français. Des réticences plus fortes qu'en France se font sentir au sein de l'industrie, cependant la collaboration entre les secteurs privé et public s'effectue aisément par le biais de partenariats bien établis, nourris par la stratégie « Industrie 4.0 » du gouvernement[84].

Royaume-Uni

Le Royaume-Uni s'est également doté en 2011 d'une stratégie de cybersécurité identifiant le risque de cyberattaque comme faisant partie des priorités[85]. La même année, le gouvernement lançait le National Cyber Security Programme doté de 860 millions de livres afin d'atteindre les objectifs de la Stratégie de cybersécurité. La révision de la stratégie pour les années 2016-2021 parue fin 2016, met notamment l'accent sur la création d'un programme de formation visant à augmenter le nombre d'experts de la cybersécurité dans les années à venir, en plus d'engager le gouvernement à hauteur de 1,9 milliard de livres sur cinq ans[86].

81. Council on Foreign Relations, Germany's Cybersecurity Law: Mostly Harmless, But Heavily Contested, 2015, http://blogs.cfr.org.
82.ENISA, CIIP Governance in the European, janvier 2016, Union Member States, disponible sur : www.enisa.europa.eu.
83. Des standards de sécurité informatique spécifiques aux opérateurs de centrales nucléaires préexistaient l'adoption de l'IT Security Act.
84. D. Kohler et J.-D. Weisz, *Industrie 4.0 : Les défis de la transformation numérique du modèle industriel allemand*, Paris, La Documentation française, 2016.
85. The UK Cyber Security Strategy, novembre 2011, disponible sur : www.gov.uk.
86. *UK Cyber Security Strategy: Statement on the Final Annual Report*, 14 avril 2016, disponible sur : www.gov.uk.

Cependant, l'approche britannique emploie assez peu la réglementation comme moyen de faire progresser la sécurité des systèmes d'information, même en ce qui concerne les infrastructures critiques. Ces dernières sont certes considérées comme des infrastructures à protéger en priorité par la Stratégie de cybersécurité, mais elles ne font l'objet d'aucune législation particulière en la matière. Selon un chercheur de Chatham House, le fait qu'une part importante des opérateurs d'infrastructures vitales soient privés inciterait l'État à privilégier les partenariats avec les entreprises concernées pour stimuler les bonnes pratiques[87]. Cette tendance s'observe dans la structure institutionnelle en charge des questions de cybersécurité : une multitude de bureaux et d'institutions[88] se partagent les pouvoirs, ce qui tend à limiter la visibilité sur leurs actions, alors que les moyens engagés financièrement sont importants[89]. Le CERT national n'a été établi qu'en 2014 et lors de l'adoption de la directive européenne SRI, aucune autorité nationale ne pouvait être identifiée comme point de contact unique avec la Commission européenne et l'ENISA. Le National Cyber Security Centre (NCSC), fondé à l'automne 2016, a pour but de « gérer la réponse opérationnelle aux incidents de cybersécurité[90] », et sera le point de contact unique pour les secteurs public et privé. La Stratégie de cybersécurité 2016-2021 du Royaume-Uni fait du NCSC l'institution nationale de référence dont la création est imposée par la directive SRI, une décision tardive compte tenu du niveau de maturité des pays d'Europe de l'Ouest sur les questions de cybersécurité[91]. Le Cyber Security Information Sharing Partnership (CiSP) créé en 2013, rassemble plus de 750 organisations et sert également de plateforme d'échanges d'informations critiques sur des attaques, sur un modèle similaire à l'Alliance pour la cybersécurité allemande. Cependant, Alex Dewdney, directeur de la cybersécurité au CESG, aurait signalé lors d'une conférence internationale en mars 2016 que la ligne de conduite du gouvernement n'a pas porté ses fruits, et qu'il serait question d'envisager une méthode plus interventionniste à l'avenir[92].

87. M. Carr, « Public–private Partnerships in National Cyber-Security Strategies », *International Affairs*, vol. 92, n° 1, 2016, p. 43-62, disponible sur : www.chathamhouse.org.
88. Le Government Communications Headquarters (GCHQ) concentre la plupart des pouvoirs et des fonds, la National Crime Agency, National Cyber Crime Unit (NCCU) ou encore l'agence Cyber Security Operation Centre (CSOC) hébergée par le GCHQ, travaillant aux côtés du Communications Electronics Security Group (CESG).
89. K. Stoddart, « UK Cyber Security and Critical National Infrastructure Protection », *International Affairs*, vol. 92, n° 5, 2016, p. 1079-1105.
90. *National Security Strategy and Strategic Defense and Security Review 2015*, HM Government, 2015, p. 41.
91. UK National Cyber Security Strategy 2016-2021, www.gov.uk
92. « UK government to change tack on cyber security », Computer weekly, RSAC16, mars 2016, disponible sur : www.computerweekly.com.

Les institutions françaises en charge de la cybersécurité coopèrent continuellement avec leurs homologues allemands et britanniques, ce qui explique en partie les similitudes dans les institutions de partage de l'information entre les secteurs privé et public, et dans l'approche réglementaire de la France et de l'Allemagne. La directive SRI permettra de réduire les écarts entre les politiques nationales, même s'il est peu probable que certains pays puissent se doter de capacités similaires à celles des pays les plus matures sur la question. Quelques pays comme la Suède ou la Grèce ne se sont pas encore dotés de stratégie nationale de cybersécurité, malgré l'existence d'initiatives de protection des infrastructures énergétiques[93]. Dans ce cadre, la France peut s'appuyer sur ses partenaires européens et son expérience législative significative pour promouvoir un cadre de cybersécurité cohérent et influent en Europe et dans le monde.

93. Pour suivre l'état d'avancement des stratégies nationales de cybersécurité en Europe : www.enisa.europa.eu.

Conclusion

Nos systèmes énergétiques connaissent des évolutions digitales cruciales dont il est difficile d'imaginer précisément les débouchés. Aux infrastructures lourdes, pérennes, s'ajoutent toutes sortes de composants éphémères et interconnectés qui révolutionnent les métiers de l'énergie, mais qui apportent leur lot de risques avec lesquels l'environnement industriel actuel permet difficilement de composer. Alors que l'industrie énergétique commence depuis à peine cinq ans à intégrer la cybersécurité dans son mode de fonctionnement quotidien, la rapidité de la digitalisation et l'impossibilité d'anticiper la nature des nouvelles technologies qui iront se greffer sur les anciennes infrastructures, promettent de défier constamment les efforts consentis. Les experts s'accordent à dire que les risques existent, qu'ils peuvent être endigués, mais que se prémunir contre toutes les cyberattaques est impossible. Ceci est lié à la nature des technologies numériques qui sont par essence plus vulnérables que les systèmes industriels analogiques et mécaniques, mais aussi à leurs évolutions permanentes qui ouvrent toujours de nouvelles faiblesses à détecter, analyser et corriger. Un certain courant de l'industrie énergétique estime d'ailleurs que maintenir l'analogique pour assurer les processus les plus critiques serait indispensable.

Les évolutions réglementaires permettront peut-être d'accomplir cette révolution digitale sans compromettre la sécurité des infrastructures énergétiques. Les mesures prises par la France, l'Allemagne, le Royaume-Uni et suivies par l'UE laissent espérer une meilleure prise de conscience, des actions mieux coordonnées et des investissements ciblés vers des équipements plus fiables. C'est aussi un moyen, en France, de stimuler la recherche et l'innovation dans le domaine de la cybersécurité et motiver l'adoption de normes communes qui feront la force de l'industrie énergétique européenne. Sur ce point, la France a la chance de disposer d'un secteur énergétique relativement mature concernant les enjeux de cybersécurité, enclin à coopérer avec les autorités nationales et organisé en une communauté d'intérêt de l'énergie, qui en fait probablement un excellent moteur pour porter la cybersécurité industrielle à la française.

Bibliographie

Agence Nationale de la Sécurité des Systèmes d'Information, (ANSSI), Stratégie de la France, 2011.

ANSSI. *Maîtriser la SSI pour les systèmes industriels*, 2012. www.ssi.gouv.fr.

ANSSI, Certification de sécurité de premier niveau des produits des technologies de l'information, 2014, www.ssi.gouv.fr.

Baylon C., Brunt R., et Livingstone, D., « Cyber Security at Civil Nuclear Facilities », *Chatham House Report*, 2015.

Connecting Europe Facility, instrument de financement des infrastructures transeuropéennes pour la période 2014-2020 : https://ec.europa.eu.

Council of the European Union, Report of the Ad Hoc Group on Nuclear Security, www.consilium.europa.eu.

ENISA, Incident reporting and security regulation, www.enisa.europa.eu.

ENISA, Smart Grid Security www.enisa.europa.eu.

ENISA, Good Practice Guide for Incident Management, 2010, www.enisa.europa.eu.

European Commission, Proposal for a new regulation on risk preparedness in the electricity sector, 2016, http://ec.europa.eu.

European Commission, Technical summary on the implementation of comprehensive risk and safety assessments of nuclear power plants in the European Union Accompanying the document Communication From The Commission To The Council And The European Parliament on the comprehensive risk and safety assessments ("stress tests") of nuclear power plants in the European Union and related activities : http://eur-lex.europa.eu.

European Parliament, Directorate General for Internal Policies, Cyber Security Strategy for the Energy Sector, 2016, www.europarl.europa.eu.

Gluschke, G., Cyber Security Challenges in the Energy Context, (2016).

Hausermann, L., « SENTRYO – Cybersécurité industrielle, que doit-on craindre ? », www.cxp.fr.

Industrial Ethernet Book, Using ANSI/ISA-99 standards to improve control system security, www.iebmedia.com.

Introducing The Activities Of Control System Security Center (Cssc): www.css-center.or.jp.

Kesler, B., « The Vulnerability of Nuclear Facilities to Cyber Attack », *Strategic Insights*, *10*(1), 2011, p. 15-25, http://large.stanford.edu.

Miller, B., A Survey of SCADA and Critical Infrastructure Incidents., 2012, http://citeseerx.ist.psu.edu.

MIT, The Future of the Electric Grid, 2011, http://energy.mit.edu.

National Cybersecurity and Communications Intergration Center – US Department of Homeland Security, 2015 ICS-CERT Monitor.

Nicolas, M. et Machado, C., « Cyber Security Governance: Securing the European Union's Cyber Domain », 2015.

Nouyrigat, V., « EPR – Les 4 erreurs de la filière française », *Science&Vie*, juin 2010, p. 94.

Office of technology assessment at the German Bundestag, « What Happens During a Black-out », *Technology Assessment Studies Series*, www.tab-beim-bundestag.de.

Programmation Pluriannuelle de l'Énergie, www.developpement-durable.gouv.fr.

Rid, T. et Buchanan, B., « Attributing Cyber Attacks », *Journal of Strategic Studies*, 2014.

Sanger, E. D., *Confront and Conceal*, New York, Broadway Books, 2012.

SANS-ICS, E.-I., *Analysis of the Cyber Attack on the Ukrainian Power Grid*, 2016.

Singer, P.W. et Friedman, A., *Cybersecurity and Cyberwar: What Everyone Needs to Know*, Oxford, Oxford University Press, 2014.

Trend Micro, « Who's Really Attacking your ICS Equipments? », 2013, www.trendmicro.com.

Union for the Coordination of Transmission of Electricity UCTE, *Final report, System Disturbance on 4 November 2006*, www.entsoe.eu.

Wired. Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid, www.wired.com.

Liste des entreprises et institutions rencontrées

Agence Nationale pour la Sécurité des Systèmes d'Information (ANSSI)

Commission Européenne : DG-CNECT

DG-ENER

DG-HOME

Club des experts de la sécurité de l'information et du numérique (CESIN)

EDF

Enedis

European Union Agency for Network and Information Security (ENISA)

Nokia

Organisation du Traité de l'Atlantique Nord (OTAN)

Réseau de Transport d'Électricité (RTE)

Schneider Electric

Sentryo

Siemens

Symantec

Trend Micro

Commission de Régulation de l'Énergie (CRE)

D'autres n'ont pas souhaité être identifiées dans cette étude.

Annexes

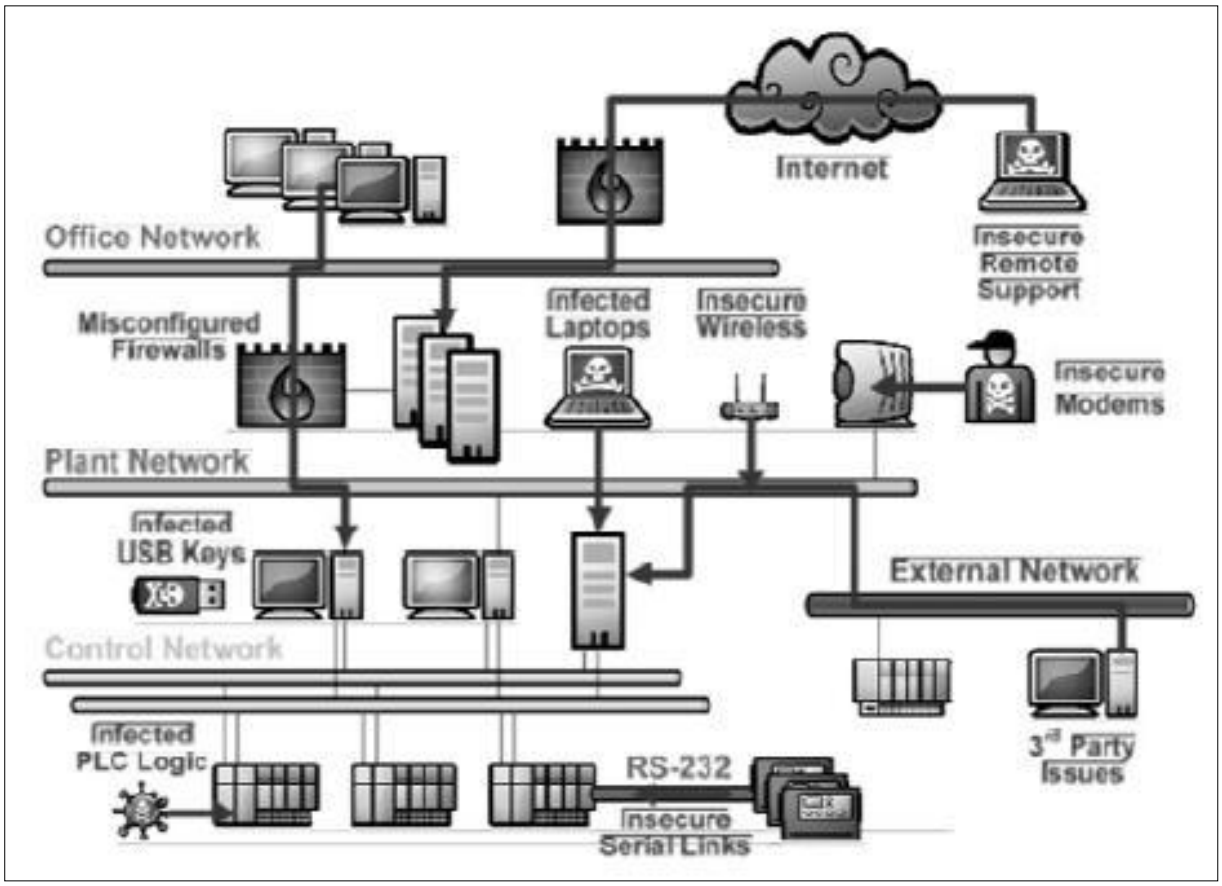
Annexe 1 : Le Système d'information industriel

Le Système d'information industriel (SII) est un système « numérique » permettant d'effectuer des actions sur des installations physiques. Il est souvent désigné par l'acronyme ICS (Industrial Control System) ou SCI (Système de contrôle industriel). Les SII sont constitués de quatre grandes catégories de composants :

- Ceux assurant l'interaction avec le monde physique : capteurs (température, ouverture, humidité, lumière…) et actionneurs (pompes, vérins, moteurs, voyants…), reliés entre eux par un réseau spécifique.
- Ceux réalisant le pilotage des actionneurs en fonction des informations remontées les capteurs. Ils peuvent être distribués (DCS : Distributed Control System) ou autonomes, sous la forme d'automates adaptés à un déploiement soit local (PLC (Programmable Logical Controler) ou API (Automate Programmable Industriel) en français), soit déporté (RTU : Remote Terminal Unit). Aujourd'hui ces distinctions ont tendance à s'estomper. Les composants de nouvelle génération (PAC : Programmable Automation Controler) disposent d'une plus grande palette de fonctionnalités que les composants traditionnels et sont reliés en IP au réseau informatique de pilotage de la production.
- Les composants de supervision et de contrôle permettent la visualisation de l'ensemble du processus, et son pilotage grâce à une interface homme-machine (IHM). On parle souvent de SCADA (Supervisory Control And Data Acquisition). Ils sont reliés aux systèmes de gestion de production de l'entreprise dont ils reçoivent les ordres. Ils sont composés d'éléments issus de l'informatique de gestion tels que des serveurs ou des postes de travail fonctionnant avec des systèmes d'exploitation grand public (Windows et Linux principalement).
- De façon croissante, les systèmes industriels sont informatisés et interconnectés au système de gestion (SIG) de l'entreprise.

Source : D'après Clusif 2014, Cybersécurité des systèmes industriels.

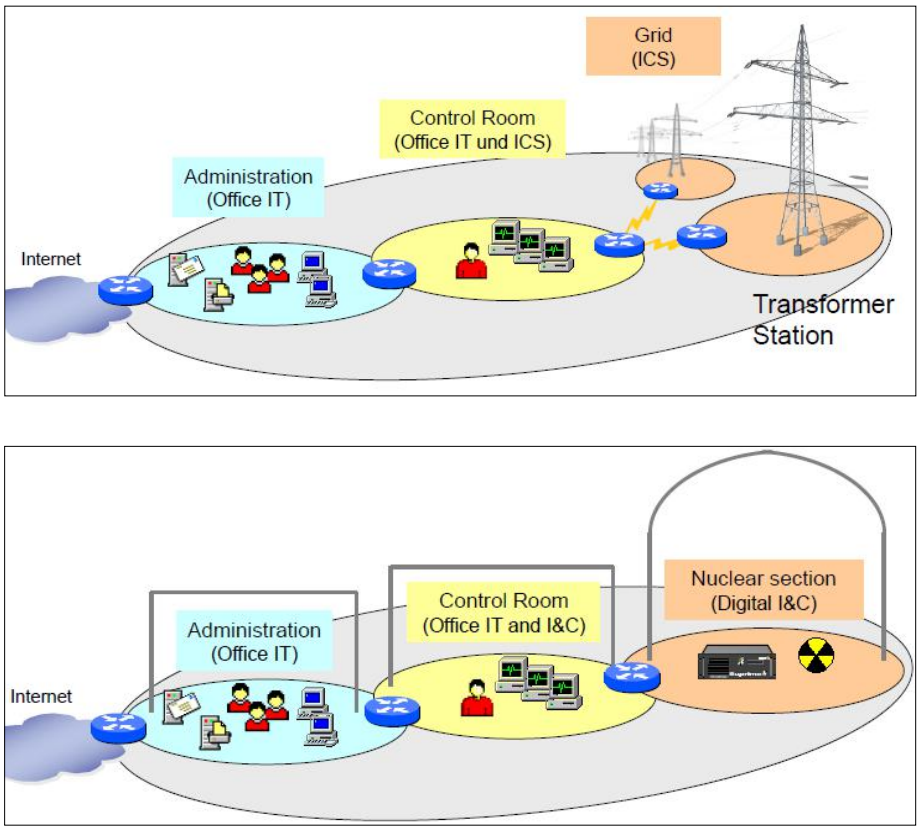
Annexe 2 : Vulnérabilités et points d'entrée sur les systèmes de contrôle industriels



Source : Nokia

Annexe 3 : Architecture réseau d'infrastructures énergétiques

Architecture du réseau électrique et d'une centrale nucléaire



Source : Institute for Security and Safety (ISS) at the Brandenburg University of Applied Sciences, NISS / NATO ENSE CoE.

Annexe 4 : Tableau de bord de la cybersécurité dans l'UE, 2015

(Source : BSA | The Software Alliance)

✔ Oui ✖ Non ◑ Partiellement

# QUESTION	Allemagne	Autriche	Belgique	Bulgarie	Chypre	Croatie	Danemark	Espagne	Estonie	Finlande	France	Grèce	Hongrie	Irlande	Italie	Lettonie	Lituanie	Luxembourg	Malte	Pays-Bas	Pologne	Portugal	République tchèque	Roumanie	Royaume-Uni	Slovaquie	Slovénie	Suède
BASES LÉGALES																												
1. Existe-t-il une stratégie nationale de cybersécurité ?	✔	✔	✔	✖	✔	✖	✖	✔	✔	✔	✔	✖	✔	✖	✔	✔	✔	✔	✖	✔	✔	Draft	✔	✔	✔	✔	✖	✖
2. En quelle année la stratégie nationale de cybersécurité a-t-elle été adoptée ?	2011	2013	2012	–	2013	–	–	2013	2014	2013	2011	–	2013	–	2014	2014	2011	2013	–	2013	2013	–	2011	2013	2011	2008	–	–
3. Existe-t-il une stratégie ou un plan de protection d'infrastructures critiques ?	✔	✔	◑	◑	✖	✖	✖	✔	✔	✔	✖	✔	◑	✖	✔	✖	◑	✖	◑	✔	✔	✖	✔	✔	✔	✔	✔	✔
4. Existe-t-il une législation ou une règle qui oblige à établir un plan écrit de sécurité de l'information ?	✖	✖	✖	✖	✖	✖	◑	✖	✔	◑	✖	◑	✔	✖	✖	✖	✖	✖	◑	◑	✖	✖	✔	✖	◑	◑	✖	✔
5. Existe-t-il une législation ou une règle qui oblige à dresser un inventaire des « systèmes » et une classification des données ?	✔	✔	✔	✔	◑	✔	✔	✔	✔	✔	✔	✔	✔	✖	✔	✔	✔	◑	◑	✔	✔	✔	✔	✔	✔	✔	✔	✔
6. Existe-t-il une législation ou une règle qui impose des pratiques ou des obligations de sécurité en fonction du niveau de risque ?	✔	✔	✔	✔	✖	✔	✔	✔	✔	✔	✔	✖	✔	✖	✔	✔	✔	✖	✖	✔	✔	✔	✔	✔	✔	✔	✔	✔
7. Existe-t-il une législation ou une règle qui préconise (au moins) un audit annuel de cybersécurité ?	En cours	✔	✖	✖	✖	✖	✖	◑	✔	✔	✖	✖	✖	✖	✖	✔	◑	◑	◑	◑	✖	◑	◑	✖	✖	✖	◑	✖
8. Existe-t-il une législation ou une règle qui oblige à publier un état des lieux des capacités de cybersécurité à la disposition de l'Etat ?	En cours	◑	✖	✖	✖	◑	✖	✖	✔	✔	✖	✖	✔	✖	✔	✖	◑	✖	✖	✔	✖	◑	✔	✖	◑	◑	✖	✖
9. Existe-t-il une législation ou une règle qui oblige chaque agence à se doter d'un directeur des services informatiques (DSI) ou de la sécurité ?	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✔	✖	✖	✖	✖	✔	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✔
10. Existe-t-il une législation ou une règle qui oblige à déclarer les incidents de cybersécurité ?	✔	✖	◑	✖	✔	✖	✖	✖	✔	✖	✖	✖	✖	✖	✖	✔	✔	✖	✔	✖	✔	✖	✔	◑	✖	✖	✔	✖
11. Existe-t-il dans la législation ou les règles une définition appropriée de la « protection des infrastructures critiques » ?	✔	✔	✔	✔	✖	✖	✔	✔	✔	✔	✖	✔	✔	✖	✔	✔	✔	✔	✔	✔	✔	✖	✔	✔	✔	✔	✔	✔
12. Les achats de solutions de cybersécurité dans le public et le privé sont-ils encadrés par les systèmes d'accréditation ou de certification internationaux, sans exigences locales spécifiques ?	✔	✔	◑	N/A	N/A	N/A	✔	✔	✔	✔	◑	✔	✔	N/A	✔	◑	◑	◑	N/A	✔	◑	N/A	◑	◑	◑	✖	N/A	✔
ENTITÉS OPÉRATIONNELLES																												
1. Existe-t-il un centre national d'alerte et de réaction aux attaques informatiques, CERT (computer emergency response team) ou CSIRT (computer security incident response team) ?	✔	✔	✔	✔	✖	✔	✔	✔	✔	✔	✔	✔	✔	◑	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
2. En quelle année le CERT (computer emergency response team) a-t-il été établi ?	2012	2008	2008	2008	–	2009	2009	2008	2008	2014	2008	2009	2013	–	2014	2006	2006	2011	2002	2012	2008	2008	2011	2011	2014	2009	2010	2003
3. Existe-t-il une autorité nationale compétente en charge de la sécurité informatique et des réseaux ?	✔	◑	✔	✔	◑	✔	✔	✔	✔	✔	✔	✔	✔	✖	✔	✔	✔	◑	✔	◑	◑	✔	✔	✔	✔	✔	✔	✔
4. Existe-t-il une plate-forme de centralisation des rapports et données concernant les incidents et cybersécurité ?	✔	✔	✔	✔	✖	✔	✔	✔	✔	✔	✔	✔	✔	✖	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
5. Des exercices nationaux de cybersécurité sont-ils organisés ?	✔	✔	✔	✔	◑	◑	✔	◑	✔	✔	✔	✔	◑	✔	✔	✔	◑	◑	◑	✔	◑	◑	◑	◑	✔	✔	◑	✔
6. Existe-t-il une structure nationale de gestion des incidents ayant les capacités de répondre aux incidents de cybersécurité ?	✖	✔	✖	◑	✖	✖	◑	✔	◑	✖	✖	✖	✔	✖	✔	✔	◑	◑	✖	✔	✔	◑	✔	◑	✔	✖	✖	◑
PARTENARIATS PUBLIC-PRIVÉ																												
1. Existe-t-il un partenariat public-privé officiel en faveur de la cybersécurité ?	✔	✔	◑	◑	◑	◑	✖	✔	◑	◑	✖	✖	◑	✖	◑	✖	✖	✖	◑	✔	✖	◑	✖	✖	✔	✖	✖	◑
2. L'industrie est-elle organisée (conseils de cybersécurité de représentants d'entreprises ou de l'industrie) ?	✔	✔	✔	◑	✖	✖	✔	✔	◑	✔	✖	✖	◑	✔	◑	✖	◑	✖	✖	✔	◑	✖	✖	◑	✔	◑	◑	◑
3. Y a-t-il de nouveaux partenariats public-privé en cours ou en projet (si oui, de quelle spécialité) ?	✔	✔	–	✖	✖	✖	✖	–	✖	✖	◑	✖	✖	✖	◑	◑	◑	◑	✖	–	✖	✖	◑	✔	–	✖	✖	✖
PLANS DE CYBERSÉCURITÉ SECTORIELS																												
1. Existe-t-il un plan commun aux secteurs public et privé qui traite de la cybersécurité ?	✖	✔	✖	✖	◑	◑	✖	✔	✖	◑	✔	✖	◑	✖	✖	✖	✖	✖	✖	✔	✖	✖	✖	✖	✔	✖	✖	✖
2. Des priorités de sécurité par secteur ont-elles été définies ?	✖	✖	✖	✖	✖	✖	✖	◑	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	◑	✖	✖	✖
3. Des évaluations des risques pour la cybersécurité ont-elles été réalisées par secteur ?	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✔	✖	✖	✖	✖	✖
ÉDUCATION																												
1. Existe-t-il une stratégie d'éducation pour informer et sensibiliser davantage le jeune public aux risques de cybersécurité ?	◑	✔	◑	◑	✖	✖	✖	✔	✔	✔	✔	✖	✔	◑	✔	✔	✔	✔	✖	✔	✔	✖	✔	✔	✔	✔	✖	✖

ifri
institut français
des relations
internationales