28 septembre 2018

IRSEM
INSTITUT DE RECHERCHE STRATÉGIQUE DE L'ÉCOLE MILITAIRE

VULNÉRABILITÉ ET PROTECTION DES RÉSEAUX ÉLECTRIQUES

Approches comparées Union européenne – États-Unis

Angélique PALLE
Chercheur Énergie et matières premières à l'IRSEM

RÉSUMÉ

L'électricité est une composante vitale du mode d'organisation de nos sociétés : l'approvisionnement en eau, la conservation de la nourriture, l'ensemble de l'économie mondialisée et des modes de communication en dépendent. Les sociétés occidentales (on s'intéresse ici au cas de l'Union européenne et des États-Unis) ont fait reposer leur approvisionnement en électricité sur des réseaux d'infrastructures qui assurent la production et la distribution de la ressource. Ces réseaux sont des éléments stratégiques de la défense et de la sécurité nationale qui ont été et redeviennent depuis quelques années des cibles lors de conflits ou d'attaques terroristes.

Cette note de recherche propose un état des lieux des risques qui pèsent sur ces réseaux et une analyse croisée de leur prise en compte par l'Union européenne et par les États-Unis. Elle pose dans un premier temps des éléments de contexte sur leur caractère stratégique avant d'analyser l'évolution des aléas et vulnérabilités qui les affectent. Une comparaison des stratégies européennes et américaines de structuration d'une protection est enfin proposée, ainsi que des différents modèles de gestion de crise et exercices de simulation menés.

SOMMAIRE

NOTE DE RECHERCHE – n° 62

1. LES RÉSEAUX DE TRANSPORT ET DE DISTRIBUTION D'ÉLECTRICITÉ : DES INFRASTRUCTURES STRATÉGIQUES

La notion de risque appliquée aux réseaux électriques

On entend dans cette la note la notion de risque telle qu'elle est utilisée et définie par les géographes et les aménageurs qui travaillent notamment sur les risques naturels, industriels ou sociétaux[1]. Le risque est, dans ce champ, fonction de trois composantes :

- L'aléa qui est la probabilité d'occurrence d'un événement (inondation, incident technique, etc.).

- La vulnérabilité qui est la propension d'un enjeu matériel ou humain considéré à être affecté par cet aléa (présence de digue ou d'architectures spécifiques conçues pour résister à l'aléa).

- La résilience de l'enjeu qui est sa capacité à se régénérer dans un temps donné pour atteindre éventuellement un retour à la situation initiale. En l'occurrence, cet élément, s'il est présent en filigrane dans la dernière partie de cette note dédiée aux exercices de crise, ne fait pas ici l'objet d'un traitement spécifique et les données existantes sur le sujet ont souvent un caractère sensible.

Dans le cas d'un réseau, les aléas qui nous intéressent sont des attaques physiques et/ou cyber. La vulnérabilité du réseau est fonction de l'accessibilité des infrastructures, de leur état, de leur redondance (y a-t-il une seule ou plusieurs voies d'alimentation pour un territoire ?). La résilience est déterminée par la capacité du gestionnaire du réseau à intervenir rapidement, à disposer de matériel de remplacement, à communiquer avec les autres gestionnaires des réseaux voisins – en cas d'interconnexion des réseaux – ainsi qu'avec la police ou l'armée selon les cas.

1. BERSERK BEARS (Allemagne) – Printemps 2018

Le 20 mai 2018, le directeur de l'Office fédéral de protection de la Constitution (le service de renseignement intérieur allemand), après plusieurs alertes de l'Office fédéral pour la sécurité informatique, accuse la Russie de mener une campagne d'infiltration informatique visant le secteur de l'énergie allemand, notamment les fournisseurs d'électricité. Deux mois auparavant, les États-Unis avaient également dénoncé une campagne de cyberattaques visant leur réseau d'électricité et désigné la Russie comme responsable.

Les réseaux électriques, points d'importance vitale

L'approvisionnement en électricité est essentiel au maintien d'un grand nombre de fonctions vitales à la société : en 2003, un *black-out* aux États-Unis avait relevé de façon critique le risque d'épidémie à Détroit en empêchant le nettoyage des conduits du réseau d'approvisionnement en eau. Les réseaux de transport d'électricité sont ainsi classés parmi les infrastructures d'importance vitale (cf. encadré n° 2). En France, il s'agit des infrastructures « dont l'indisponibilité risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la nation[2] ». Le gestionnaire du réseau de transport d'électricité français, RTE, a ainsi été désigné comme opérateur d'importance vitale (OIV) en 2008, dans le cadre de la directive nationale de sécurité « énergie » et comptait en 2012 une cinquantaine de « points d'importance vitale » (PIV)[3].

1. Voir notamment les travaux de Magali Reghezza et Yvette Veyret.
2. Art. L1332 du Code de la défense français.
3. Max Ernoult, Secrétaire général adjoint délégué à la défense et à la sécurité, RTE, Cycle 2012 des rencontres de l'IHEDN, Paris-La Défense, 23 octobre 2012.

2. Infrastructures critiques et points d'importance vitale

La notion « d'infrastructure critique » apparaît dans les textes officiels américains au milieu des années 1990. En 2001, les attentats du 11-Septembre ainsi que la crise énergétique californienne conduisent la Maison-Blanche à définir une stratégie nationale pour leur protection. Cette dernière se traduit notamment par la transformation en 2003 de l'Office de la sécurité intérieure en ministère, dont l'une des directions est chargée particulièrement de la question des infrastructures. Le concept se diffuse en Europe auprès de certains États et des institutions européennes au milieu des années 2000, notamment après les attentats de Londres et de Madrid. Les définitions et les approches varient : certains comme le Canada ou l'Allemagne ont adopté une approche initiale multirisque, d'autres comme le Royaume-Uni ou les États-Unis centrent leur politique de protection sur la menace terroriste.
La France a adopté une position intermédiaire et charge ses ministres ou ses préfets de désigner dans leur secteur de compétence les « opérateurs d'importance vitale » chargés de recenser les « points d'importance vitale » et de mettre en place des « plans de sécurité opérateurs ».

Sources :
Jean-Pierre Galland, « Critique de la notion d'infrastructure critique », *Flux*, n° 81, mars 2010, p. 6-18. DOI : 10.3917/flux.081.0006, https://www.cairn.info/revue-flux1-2010-3-page-6.htm

Textes de référence :
(UE) Commission européenne, 2006, Livre vert sur un Programme européen de protection des infrastructures critiques (EPCIP).
(UE) Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union.
(UE) Directive 2008/114/CE du Conseil du 8 décembre 2008 concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection.
(France) Code de la défense – articles L. 1332-1 à L. 1332-7, L. 2151-1 à L.2151-5 et R. 1332-1 à R. 1332-42.
(France) Instruction générale interministérielle n° 6600 relative à la sécurité des activités d'importance vitale du 7 janvier 2014.
(France) 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, art. 22.
(France) LOI n° 2018-607 du 13 juillet 2018 relative à la programmation militaire pour les années 2019 à 2025 et portant diverses dispositions intéressant la défense, art. 18 à 22.

Objectifs de guerre ou cibles d'attaques physiques et cyber : anciens et nouveaux aléas

Plusieurs évolutions touchent les réseaux européens de transport d'électricité depuis le début des années 2000. Ces réseaux ont été des objectifs de guerre et protégés comme tels pendant la Deuxième Guerre mondiale[4], puis des éléments stratégiques de la reconstruction européenne après le conflit ainsi que pendant la guerre froide[5]. À partir des années 1990, l'accroissement des conflits asymétriques et les modes d'action, notamment terroristes, qui les caractérisent ont renforcé et changé les menaces potentielles pesant sur ces réseaux. Après les attentats du 11 septembre 2001, les États-Unis, l'UE et ses États membres ont progressivement repensé leur approche de la protection des infrastructures critiques dont font partie ces réseaux. Les cyberattaques menées contre le réseau ukrainien à l'hiver 2015 (cf. encadré n° 3) dans un contexte de conflit avec la Russie ont également ravivé l'intérêt des États pour ces infrastructures.

4. Henri Morsel, « Industrie électrique et défense en France lors des deux conflits mondiaux. Électricité, armement, défense », *Bulletin d'histoire de l'électricité,* no 23, 1994, p. 7-17.
5. Vincent Lagendijk, *Electrifying Europe: The Power of Europe in the Construction of Electricity Networks*, Amsterdam University Press, 2008.

3. UKRAINE – 2015

Le 23 décembre 2015, un *black-out* en Ukraine touche environ 225 000 consommateurs, il est attribué à une cyberattaque perpétrée contre le réseau de transport d'électricité. L'attaque aurait ciblé les systèmes de contrôle des infrastructures du réseau mais aussi de façon directe sept postes électriques dont les opérateurs du réseau n'ont pas pu reprendre le contrôle et qui ont nécessité l'envoi d'équipes de maintenance pour effectuer des réparations sur les postes touchés. Les lignes de téléphone des opérateurs ont également été brouillées. L'attaque a été attribuée par l'Ukraine à la Russie avec laquelle elle se trouve alors en conflit ouvert depuis plus d'un an. Il s'agit de la première cyberattaque contre un réseau électrique officiellement reconnue comme « réussie ».

Source :
US Department of Homeland Security, Industrial Control Systems Cyber Emergency Response Team, *Alert (IR-ALERT-H-16-056-01) Cyber-Attack Against Ukrainian Critical Infrastructure*, 25 février 2016, https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01.

Deux types de menaces sont envisagés :

Physique : l'attaque en 2013 du poste électrique Metcalf (cf. encadré n° 4) alimentant la Silicon Valley en Californie constitue le point de départ de la prise de conscience, aux États-Unis, d'une vulnérabilité physique spécifique des réseaux électriques que le cadre général de protection des infrastructures du pays ne permettait pas de prendre en compte efficacement.

Cyber : en Europe, la première cyberattaque contre un opérateur de réseau européen et confirmée par celui-ci (50Hertz, gestionnaire de réseau allemand) a eu lieu en 2012[6]. Sans gravité pour la stabilité du réseau et la sécurité d'approvisionnement, elle a néanmoins duré cinq jours avant qu'une solution pour un retour à la normale ne soit trouvée.

La question se pose des effets d'une combinaison de ces deux types de menace. On évoque dans les parties 3 et 4 la différence entre les stratégies de protection européennes et américaines à ce sujet : là où l'UE sépare institutionnellement la gestion de ces deux types de menace, le système américain gère cette double composante de façon intégrée.

4. METCALF (Californie) – 2013

Le 16 avril 2013, vers une heure du matin, le poste électrique californien Metcalf, située au sud-est de San José et qui gère l'alimentation en électricité de la Silicon Valley, est attaqué à l'AK-47. Après avoir coupé les fils du téléphone et de l'Internet, le ou les assaillants mettent hors service, en moins de 20 minutes, 17 transformateurs du poste. Celui-ci n'étant pas particulièrement stratégique pour le réseau, le *black-out* est évité, mais il faudra 27 jours de réparation et 15 millions de dollars pour remettre en état le matériel.
Les transformateurs ont pour fonction d'augmenter ou de diminuer le voltage des lignes, permettant ainsi d'atteindre les hautes tensions que demande le transport de l'électricité sur de longues distances. Longs à fabriquer (parfois plus de deux ans), ils peuvent coûter plusieurs millions d'euros et sont difficilement transportables. Lors de l'attaque du poste Metcalf, les tireurs ont principalement endommagé les structures de refroidissement. Le fonctionnement du poste a été arrêté avant une surchauffe grave du matériel, ce qui a permis d'éviter de plus lourds dégâts. Comme celui de Metcalf, les postes sont la plupart du temps situés dans des zones peu habitées et sont peu protégés, souvent par de simples chaînes métalliques et des caméras. Il s'agit de prévenir le vol de matériel, principal risque encouru par ces infrastructures aujourd'hui. En l'occurrence, les caméras n'ont pas permis d'identifier le ou les tireurs, situés à l'extérieur du périmètre de surveillance. Un an après l'attaque, le même poste faisait, en août 2014, l'objet d'un vol de matériel, sans que les systèmes d'alarme ne réagissent.

Sources :
Shane Harris, « "Military-Style" Raid on California Power Station Spooks U.S. », *Foreign Policy,* 27 décembre 2013.
Joe Jr. Rosato, « Following Attack on PG&E Substation, Bill Requires California Utilities to Beef Up Security », *NBC Bay Area,* 10 mars 2014.
Brian Wingfield, « Rifle-Toting Terrorists Pose Great Threat to Power Grid », *Bloomberg,* 20 novembre 2012.

6. Arthur Nielsen, « European renewable power grid rocked by cyber-attack », *Euractiv.com*, 10 décembre 2012.

2. ÉVOLUTION DE LA VULNÉRABILITÉ DES RÉSEAUX ÉLECTRIQUES

Nouvelles vulnérabilités

Si le caractère asymétrique des conflits actuels et les modes d'action terroristes qu'ils génèrent ont transformé les menaces qui pèsent sur les réseaux d'électricité, le contexte dans lequel s'inscrit la gestion de ces réseaux a également beaucoup évolué depuis le début des années 2000. Dans l'Union européenne (UE) notamment, intégration des réseaux et transition énergétique ont ouvert de nouvelles vulnérabilités.

La politique énergétique de l'UE telle que définie par le traité de Lisbonne[7] promeut une intégration des réseaux d'énergie, à la fois pour permettre la mise en place d'un grand marché commun et pour réaliser des économies d'échelles[8]. Cependant, cette interconnexion accroît aussi les effets de cascade et de propagation en cas d'incident : le dernier grand *black-out* européen (2006) généré par un incident sur une ligne allemande a ainsi touché 15 millions de consommateurs dans 12 pays de l'Union et du voisinage proche. Les effets de cette interconnexion des réseaux européens rendent impossible une approche uniquement nationale de leur protection. Le réseau européen interconnecté rassemble aujourd'hui 42 gestionnaires de réseaux qui doivent interagir pour assurer la sécurité d'approvisionnement de l'espace européen.

À cette vulnérabilité liée à l'interconnexion s'ajoute celle de l'ouverture des réseaux au numérique, dans le cadre notamment de la transition énergétique et de la modernisation des infrastructures. Le but est d'accroître l'efficacité énergétique[9] et l'optimisation technique du réseau en faisant circuler sur celui-ci, outre de l'électricité, de l'information en temps réel dans les deux sens. Cette politique entraîne par exemple, de façon plus ou moins consciente et volontaire, la connexion de certaines infrastructures à Internet, ce qui les rend vulnérables au *hacking*[10].

5. TEST AURORA (USA) – Mars 2007

En mars 2007, les chercheurs de l'Idaho National Lab expérimentent le test Aurora au cours duquel ils réussissent à manipuler à l'aide d'un virus informatique les systèmes de contrôle d'un générateur électrique alimenté au diesel. En jouant sur la vitesse de rotation des pièces, ils arrêtent le fonctionnement du générateur. Ce test est particulièrement concluant parce qu'il démontre alors la possibilité pour une cyberattaque de causer des dommages physiques aux infrastructures du réseau.

Sources :
Aurora test, CNN Video, https://www.youtube.com/watch?v=fJyWngDco3g.
Center for the Study of the Presidency and Congress, *Securing the U.S. Electrical Grid, The honorable Thomas F. McLarty III & the honorable Thomas J. Ridge*, 2014, https://www.thepresidency.org/sites/default/files/Final%20Grid%20Report_0.pdf.

Vulnérabilité du réseau européen

D'après les entretiens effectués auprès d'eux[11], les gestionnaires de réseaux d'électricité en charge de leur entretien, de leur stabilité et de leur développement perçoivent ces réseaux principalement comme des infrastructures de service, relativement déconnectées des thématiques stratégiques de défense, économique ou industrielle. Ce désintérêt pour la dimension stratégique des réseaux et leur protection est le résultat d'un agenda de priorités fixé au niveau européen ainsi que d'un certain nombre d'obstacles, économiques et liés au consommateur. Les enjeux d'harmoni-

7. Traité de Lisbonne, 2009, art. 194.
8. L'interconnexion de l'Allemagne, de la France et du Benelux permet de diminuer de 2 % la capacité de production nécessaire à leur approvisionnement (RTE, 2015, Schéma décennal de développement du réseau, édition 2014, p. 15).
9. L'efficacité énergétique, utilisée au sens large du terme, désigne l'ensemble des technologies et pratiques qui permettent de diminuer la consommation d'énergie tout en conservant le même service final (définition proposée par la Commission de régulation de l'énergie française).
10. Mc Afee, *Smarter protection for the smart grid*, rapport, 2012, https://www.ccn-cert.cni.es/.../rp-smarter-protection-smart-grid.pdf.
11. Entretiens menés au sein du Réseau européen des gestionnaires de réseau de transport d'électricité européens (ENTSO-E) à Bruxelles de janvier à juillet 2014.

sation des règles européennes et de la coopération, pour permettre la mise en place du grand marché commun de l'énergie souhaité par l'Union européenne, ainsi que la nécessité d'adapter les réseaux aux changements induits par les dynamiques de la transition énergétique, ont jusqu'à très récemment absorbé toutes les forces vives d'un secteur en profonde mutation. L'obstacle est en outre économique. En effet, lorsque la vulnérabilité du réseau à ce type d'aléa est réellement prise en compte, l'obstacle constitué par le coût de la protection vient très vite en considération. Enfin, et dans la mesure où tous les investissements se répercutent *in fine* sur le consommateur, le niveau de protection des réseaux dépend également de la conscience que celui-ci a du risque et du montant qu'il serait prêt à consacrer à sa sécurité d'approvisionnement.

6. SLAMMER – Janvier 2003

Le 25 janvier 2003, le virus Slammer, dérivé du virus Stuxnet connu pour avoir détruit certaines centrales du programme nucléaire iranien, infecte la centrale nucléaire Davis-Besse dans l'Ohio grâce à une connexion (T1) passant à travers le pare-feu de la centrale. Les deux systèmes « Safety Parameter Display System » (Système d'affichage des paramètres de sécurité) et « Plant process computer » (Ordinateur industriel gérant une partie des processus de la centrale) sont désactivés pendant plusieurs heures. La centrale n'étant alors pas en fonctionnement, aucune incidence sur la sécurité des installations ou des populations n'est constatée.

Source :
Congress of the United States, House of Representatives, *Infection of the Davis Besse Nuclear Plant by the "Slammer" Worm Computer Virus – Follow-up Questions*, Paper LTR-03-0695, 22 octobre 2003, https://www.nrc.gov/docs/ML0329/ML032970134.pdf

L'Union européenne soutient dans ce contexte un certain nombre de projets de recherche sur ces questions. Dans le cadre du 7e programme cadre de l'UE pour la recherche et le développement technologique, le projet SESAME (Sécuriser le système électrique européen contre les menaces accidentelles et malveillantes), co-financé par la Commission européenne, est ainsi la traduction en Europe d'une prise de conscience de ces nouveaux risques. Coordonné par le Politecnico di Torino, le consortium de recherche rassemble des acteurs de la recherche et de l'industrie italiens, autrichiens, espagnols, néerlandais, roumains, de l'UE et du Royaume-Uni[12].

Ce programme est issu du constat suivant :

> Les menaces pesant sur l'approvisionnement en électricité ont radicalement changé au cours des dix dernières années […] Tous les réseaux d'énergie sont exposés à des menaces de différents ordres, telles que des attaques physiques frappant des infrastructures clés (comme les postes électriques), des cyberattaques touchant leurs systèmes de contrôle, ainsi que des bombes électromagnétiques désactivant des stations de contrôle stratégiques. De telles attaques peuvent être coordonnées de manière à toucher de larges portions du réseau européen, rendre les réparations difficiles et causer un impact sociétal important. La pression pour garantir la sécurité de ces infrastructures critiques et interconnectées est très forte aux États-Unis […] Jusqu'à présent, la prise de conscience et la préparation de l'industrie européenne ont accusé un retard certain, bien que la reconnaissance du caractère crucial de cette question aille croissant. On considère que l'exposition aux malveillances est en forte croissance, à tel point que certaines sources des services de renseignement estiment aujourd'hui qu'une attaque de nature déstabilisante est plus susceptible de prendre l'Europe que les États-Unis pour cible[13].

Le programme SESAME s'est achevé à l'automne 2014. Il a été possible d'en suivre une partie des évolutions et conclusions, dont sont issues les analyses qui suivent, grâce à des entretiens effectués au sein de la division Sécurité d'approvisionnement de l'Institut de l'énergie et des transports du Centre commun de recherche de l'UE (JRC-IET) en 2013[14] et en prenant part à sa conférence de clôture, le 16 septembre 2014 à Bruxelles. L'intérêt de l'UE pour la recherche dans ce domaine s'est confirmé lors des appels à projets H2020 : un appel sur la cybersécurité des réseaux est en cours pour l'année 2018[15].

12. Site Internet du projet SESAME : www.sesame-project.eu.
13. *Ibid.* (traduction de l'auteur).
14. Entretiens menés au JRC-IET le 21 mai 2013 à Petten (Pays-Bas).
15. Horizon 2020, Cybersecurity in the Electrical Power and Energy System (EPES): an armour against cyber and privacy attacks and data breaches, Pillar: Societal Challenges, H2020-2018-2020, Secure societies – Protecting freedom and security of Europe and its citizens, http://ec.europa.eu/research/participants/data/ref/h2020/wp/2018-2020/main/h2020-wp1820-security_en.pdf ; Call : H2020-SU-DS-2018-2019-2020.

La sécurité des réseaux et du système électrique européen ne relève pas de questions strictement techniques. À l'échelon politique, plusieurs décisions doivent être prises. Il s'agit d'abord de définir ce que l'on entend par sécurité ou sûreté du réseau, qui sont en fonction du niveau d'investissement que la société est prête à consacrer à la protection d'intérêts qui sont à la fois économiques, sociaux et de défense. La protection absolue n'existe pas et un niveau de protection trop élevé par rapport à la probabilité de survenance d'un événement, ou l'ampleur de ses conséquences, constituerait un coût économique et social important. La définition du niveau de vulnérabilité acceptable et la résilience (c'est-à-dire le temps et le coût d'un retour à la normale) attendue du réseau en cas d'incident ne peut alors être laissée à la seule appréciation des gestionnaires du réseau ou des entreprises du secteur électrique. Cela nécessite à la fois une prise de conscience et une prise de responsabilité des pouvoirs politiques, ainsi qu'une sensibilisation des consommateurs.

L'opération de nos marchés d'électricité est en outre de plus en plus centralisée au niveau européen, mais si ce processus de centralisation échoue pour une raison quelconque, nous sommes désormais trop interconnectés pour qu'il y ait possibilité de retour à l'option nationale dans un laps de temps court. Cette interdépendance *de facto* pose donc la question de la coordination et de l'échange d'information à l'échelle européenne pour la sûreté du réseau, et ce alors même que cette interconnexion ne concerne pas uniquement des pays membres de l'UE. La Suisse, la Norvège la Serbie, la Bosnie-Herzégovine, le Kosovo, le Monténégro et la Macédoine sont interconnectés avec les différents réseaux synchrones européens[16] et ne peuvent donc pas être laissés en dehors du champ de la coopération technique et de sécurité, sous peine de fragiliser l'ensemble.

Le programme SESAME conclut notamment que les principaux aléas affectant statistiquement ces réseaux sont dus à des défaillances techniques et des erreurs humaines. Il est en revanche très difficile d'estimer les impacts des aléas classés « hors norme », comme les attaques de type terroriste, sur des infrastructures dont les marges de sécurité se sont réduites au cours des dernières décennies et qui opèrent de plus en plus fréquemment dans des situations de tension[17].

Si les impacts socio-économiques sont conséquents et sont estimés en termes de perte de points de PIB, la question de l'impact d'un *black-out* dans des domaines de défense et sécurité nationale se pose également. Infrastructures et systèmes de communication stratégiques sont généralement pourvus de dispositifs électriques de secours. Il est nécessaire d'en assurer la maintenance et la coordination, ce que l'on néglige parfois de faire[18]. Le *black-out* de 2003 dans le Nord-Est des États-Unis avait ainsi affecté certaines prisons et conduit à la révolte de plusieurs centaines de prisonniers (sans toutefois causer de brèche de sécurité majeure). La communication gouvernementale est également pointée du doigt dans un certain nombre de ces événements : le message envoyé aux citoyens est parfois mal maîtrisé, peu clair ou minimaliste, ce qui conduit à des tensions, voire à des réactions de panique au sein des populations[19].

Vulnérabilité du réseau français

Comment le réseau français s'inscrit-il dans ce contexte européen ? Selon les résultats du projet SESAME[20], si sa modernisation demeure une priorité, le risque technique pour le réseau français est considéré comme faible, comparé par exemple au réseau anglais dont les infrastructures comptent parmi les plus vieilles d'Europe. Les risques topographiques, liés aux conditions météorologiques extrêmes, sont également considérés comme faibles. En revanche, le taux élevé de recours au nucléaire, s'il diminue les risques de rupture d'approvisionnement, fait croître la vulnérabilité du système aux attaques terroristes en concentrant des points de productions à risque.

16. Un réseau dit « synchrone » est un réseau où le courant a la même fréquence. Il y a cinq zones synchrones différentes dans l'UE (pour l'utilisateur, changer de zone synchrone implique d'utiliser un adaptateur de prise pour le branchement des appareils).
17. SESAME (Delft University of Technology, Politecnico di Torino, INDRA et Transelectrica), *System Specification of Decision Support System,* Délivrable n° 4.1, 2012.
18. SESAME (Transelectrica, Politecnico di Torino), *Report on the analysis of historic outages,* Délivrable n° D1.1, 2011.
19. *Ibid.*
20. SESAME/Heriot-Watt University, *Assessment of Security of Electricity Supply (SES) Indicators in Europe*, Délivrable n° D3.1, 2014.

Évaluation du risque pour le réseau français par le projet SESAME				
Risques	**Aspects**	**Faible (1-3)**	**Modéré (4-7)**	**Élevé (8-10)**
Économique	Investissement inadéquat, évolution de la demande			8
Technique	Génération décentralisée, nouvelles technologies	3		
Topographique	Météo, catastrophes naturelles	3		
Social	Terrorisme, instabilité politique, manifestations		5	

Source : SESAME/Heriot-Watt University, *Assessment of Security of Electricity Supply (SES) Indicators in Europe*, Délivrable n° D3.1, 2014.

Le réseau français comporte ainsi un certain nombre de points de faiblesse ou de points particulièrement stratégiques identifiés, qui peuvent constituer autant de vulnérabilités en cas de défaillance, d'incident ou de malveillance. En France comme dans le reste de l'UE, les projets des gestionnaires de réseaux tendent, dans la plupart des cas, à la réduction de ces faiblesses ou vulnérabilités. C'est un exercice difficile d'équilibre entre exigences de fiabilité du réseau et de l'approvisionnement, acceptabilité des projets de construction ou de renforcement d'ouvrages par la population, et exigences de moindre coût, pour répondre à la pression politique et économique exercée sur les tarifs de l'électricité. Ceci, alors que les impacts socio-économiques potentiels dépassent largement le simple champ de compétence et de décision des gestionnaires de réseau et appellent un débat plus large et une vision stratégique de long terme.

Le réseau américain

L'objet de cette note qui se concentre sur les réseaux français et européens n'est pas d'analyser en détail les vulnérabilités du réseau américain. On en présente cependant rapidement les principales caractéristiques pour permettre la comparaison, abordée dans la partie suivante, entre la gestion du risque américaine et européenne. La structure et la dynamique des réseaux américains sont de fait différentes de celles qui existent en Europe. Si l'UE a entrepris, depuis la fin des années 1990, une politique d'intégration des réseaux de transport d'électricité de ses pays membres, l'intégration des réseaux des différents États n'a jamais été un objectif pour les États-Unis. La possession et la gestion de ceux-ci sont le fait d'une pluralité d'opérateurs qui jouent un rôle moindre par rapport à celui des gestionnaires de réseaux européens. Inversement, le régulateur nord-américain (NERC) est beaucoup plus influent que l'agence de régulation européenne (ACER, créée en 2011). Ces différences de structuration (cf. annexes 2 et 3) jouent un rôle dans la façon dont l'UE et les États-Unis abordent la protection de leur réseau électrique, de même que l'état du réseau, globalement plus vétuste aux États-Unis que dans l'UE.

3. LA GESTION INSTITUTIONNELLE DU RISQUE, APPROCHES COMPARÉES EURO-AMÉRICAINES

Face à des risques pour partie similaires, on compare dans cette troisième partie la structuration institutionnelle de la gestion du risque (aléa, vulnérabilité, résilience) portant sur les réseaux de transport électriques européens et américains.

États-Unis : la construction d'un lien direct entre le gouvernement fédéral et les instances responsables de la protection du réseau

Le Department of Energy (DOE) américain a commencé à s'intéresser à la coopération entre instances gouvernementales et industrielles pour la protection des infrastructures énergétiques jugées critiques à la fin des années 1990. Il en charge la North American Electricity Reliability Corporation (NERC), autorité de régulation internationale du réseau de transport d'électricité d'Amérique du Nord. L'implication du Department of Homeland Security (DHS) sur le sujet après les attentats du 11 septembre 2001 conduit à la rédaction par celui-ci en 2006 d'un plan national de protection des infrastructures. Il crée l'Electricity Subsector Coordinating Council (ESCC) qui reprend ce rôle de coordination[21]. L'ESCC établit également à partir de 2013 un lien direct entre le gouvernement fédéral et les industriels du secteur responsables de la protection du réseau, à la suite de l'attaque du poste Metcalf (cf. encadré n° 4). Le manque de coordination réelle à l'échelon fédéral pour la protection du réseau ainsi que l'absence de plan national de coordination avaient en effet été pointés par le directeur de l'Agence fédérale de régulation de l'énergie. Aucune agence fédérale n'était officiellement en charge de la sécurité de ces infrastructures, ce vide législatif faisant reposer l'ensemble de la politique de sécurisation du réseau sur les seules initiatives de l'industrie de l'énergie[22].

Les acteurs industriels impliqués dans le fonctionnement des réseaux de transport d'électricité ont parallèlement lancé en 2014 un programme commun de sécurisation du réseau[23]. Courant sur un peu plus de deux ans, il avait alors deux objectifs. Le premier était d'identifier les postes électriques ou les combinaisons de postes stratégiques, soit ceux dont la mise hors service serait critique pour la stabilité du réseau. Le poste Metcalf n'en faisait pas partie, mais d'autres sont des infrastructures plus critiques, notamment celles interconnectant plusieurs lignes à haute tension dont les tensions sont différentes. Le second était d'établir des stratégies possibles de renforcement de la résilience du réseau : utilisation de stations de production plus proches des bassins de consommation (mais plus chères) ou séparation du réseau en plusieurs îlots électriques indépendants en cas de déstabilisation — pour réduire les effets dominos, etc.

Depuis le début des années 2010, le secteur électrique américain a donc repensé et restructuré la protection de ses réseaux en regard des nouvelles menaces cyber et physiques identifiées. L'annexe 2 en présente l'architecture simplifiée, dont on peut retenir quelques traits majeurs :

- dans un secteur particulièrement complexe sur le plan technique et où les acteurs sont nombreux, l'accent est mis sur le partage d'information et la communication entre les acteurs de différentes natures (politiques, techniques, de défense et sécurité) et à différentes échelles (étatique ou fédérale) ;

- un lien direct entre le gouvernement fédéral et les industriels a été établi ;

- des exercices de simulation d'attaque rassemblant l'ensemble des acteurs ont lieu tous les deux ans pour tester la résilience du réseau et les structures de gestion de crise.

21. Voir l'annexe 2 pour une cartographie des relations entre ces différents acteurs.
22. Michael Martinez, « Sniper attack on Silicon Valley grid spurs security crusade by ex-regulator », *Cable News Network,* 8 février 2014.
23. Norimitsu Onishi, Matthew L. Wald, « Months Later, Sniper Attack at Power Hub Still a Mystery », *The New York Times*, 5 février 2014.

L'Union européenne : tentative d'une gouvernance commune

L'UE a suivi de près l'initiative américaine pour la protection des infrastructures critiques (cf. encadré n° 2 sur la notion d'infrastructure critique). Le premier livre vert de novembre 2005[24] est issu de la volonté de la Commission et du Conseil[25] de lancer un programme européen pour la protection des infrastructures critiques (EPCIP) à la suite des attentats de Madrid en 2004. Cette tentative se heurte rapidement à des problèmes de gouvernance et de coordination ainsi qu'à une divergence de vision des États membres quant à l'évaluation des menaces à prendre en compte[26]. Le livre vert inclut dans la notion d'infrastructure critique 11 secteurs économiques et sociétaux, mais ces ambitions sont réduites aux secteurs de l'énergie et des transports dans la directive qui en est issue[27]. Seules 13 infrastructures critiques européennes sont alors identifiées par les États membres sur l'ensemble de l'Union, selon les obligations posées par la directive. Les réseaux de transport de gaz et d'électricité ne figurent pas dans la liste. La directive aurait ainsi conduit à un renforcement des coopérations bilatérales plutôt qu'à une réelle coopération européenne[28], tandis que la protection de ces infrastructures échoit en dernier ressorts aux États membres[29] et aux propriétaires et opérateurs de ces réseaux. Malgré un fort degré d'interconnexion et d'interdépendance, l'UE n'a pas insufflé de réelle dynamique de coopération concernant la sécurité de ses réseaux électriques.

La menace cyber est traitée spécifiquement dans d'autres programmes ou agences décorrélés (European Union Agency for Network and Information Security) et le personnel institutionnel européen est trop peu nombreux sur ce sujet pour générer, là aussi, une réelle dynamique[30]. Concernant le cas spécifique des réseaux électriques, un groupe thématique sur la protection des infrastructures énergétiques critiques a été créé en 2010 par la DG Énergie et la Commission. Ses rencontres biannuelles laissent cependant peu de place à l'émergence d'une dynamique commune. La Commission, lors d'une évaluation de l'EPCIP en 2013, plaide alors pour une approche plus pratique, intégrant notamment les effets dominos que des infrastructures critiques de différentes natures (communication, énergie, etc.) peuvent avoir les unes sur les autres. Les réseaux de transport d'énergie constituent l'un des quatre secteurs prioritairement identifiés[31].

Faute de réel leadership européen sur le plan institutionnel, les actions de coordination sont menées par les gestionnaires de réseau. Leur association européenne, l'ENTSO-E, a été chargée par la Commission de préparer des « codes de réseau » communs à l'UE, c'est-à-dire un ensemble de règles de fonctionnement communes aux opérateurs de réseaux[32]. Si le projet est plus large que la seule question de la sécurité (il comprend des règles de marché, ou des prérequis techniques pour la connexion au réseau de nouveaux ouvrages), l'un de ces codes, « Emergency and Restoration », est dédié spécifiquement à la question de la gestion commune d'un événement mettant en péril la stabilité du réseau ou l'approvisionnement des consommateurs. Il comporte notamment un plan de défense du système et des procédures synchronisées de remise sous tension du réseau[33].

Outre les codes de réseau, les gestionnaires des réseaux d'électricité européens ont également mis en place (notamment à la suite du *black-out* de 2006) des Coordinateurs régionaux de sécurité (RSC) chargés de surveiller le réseau à une maille régionale supra-étatique (des ensembles de groupes d'États) et d'informer les gestionnaires de réseau nationaux dont le champ de vision s'arrête à leurs frontières et permet peu de coordination et d'optimisation. Si ces initiatives des acteurs européens non étatiques sont nécessaires, elles ne sont cependant pas spécifiquement calibrées pour traiter les menaces cyber et les attaques physiques et elles n'impliquent pas les acteurs gouvernementaux ou

24. Livre vert du 17 novembre 2005 sur un programme européen de protection des infrastructures critiques COM(2005) 576.
25. Commission européenne, COM(2004) 701 du 20 octobre 2004, *Lutte contre le terrorisme : préparation et gestion des conséquences* ; Commission européenne, COM(2004) 698 du 20 octobre 2004, *Attaques terroristes : prévention, préparation et réponse*.
26. Raphaël Bossong, « The European Programme for the protection of critical infrastructures – meta-governing a new security problem? », *European Security*, 23:2, 14 janvier 2014, p. 210-226, DOI : 10.1080/09662839.2013.856307 ; Madelene Lindström, Stefan Olsson, « The European Programme for Critical Infrastructure Protection », *in* Stefan Olsson (dir.), Crisis Management in the European Union, Berlin, Heidelberg, Springer, 2014, DOI : https://doi.org/10.1007/978-3-642-00697-5_3.
27. Directive 2008/114/CE du Conseil du 8 décembre 2008 concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection.
28. Commission européenne, *Commission staff working document on a new approach to the European Programme for Critical Infrastructure Protection Making European Critical Infrastructure more secure*, SWD(2013) 318, 2013.
29. Chaque État désigne un point de contact européen sur la question, le SGDSN est le contact français.
30. Bossong, « The European Programme for the protection of critical infrastructures – meta-governing a new security problem? », *op. cit.*
31. *Ibid.*
32. Règlement (CE) n° 714/2009 du Parlement européen et du Conseil du 13 juillet 2009 sur les conditions d'accès au réseau pour les échanges transfrontaliers d'électricité.
33. ENTSO-E, *Network Code on Emergency and Restoration*, 25 mars 2015.

de la défense, concernés au premier chef en cas d'attaque ciblée sur ces réseaux. Contrairement à l'architecture de réponse à la menace américaine, l'UE n'a pas fait de lien direct entre acteurs industriels et responsables de la défense du territoire. On présente en annexe 3 le même schéma de l'architecture institutionnelle de réponse à la menace pour l'UE qui permet de constater trois éléments :

- les coopérations existantes sont bien plus à l'initiative des industriels, centres de recherches ou gestionnaires de réseaux qu'à l'initiative des institutions ou des gouvernements de l'UE comparativement à la dynamique américaine ;

- il n'existe pas de structures ou d'exercice rassemblant l'ensemble des acteurs impliqués en Europe ;

- il existe une séparation structurelle et institutionnelle entre la gestion de la menace/vulnérabilité cyber et celle de la menace/vulnérabilité physique qui est inexistante dans l'architecture américaine.

La différence d'approche entre UE et États-Unis qui existe sur le plan institutionnel a des effets sur la préparation concrète des acteurs du secteur à des situations de crise. La dernière partie aborde ainsi la question des exercices de simulation mis ou non en œuvre pour former les acteurs à la gestion du risque.

4. PRÉPARATION ET EXERCICES DE CRISE

Le modèle nord-américain GridEx

Si le caractère terroriste ou non de l'attaque du poste Metcalf en Californie (cf. encadré n° 4) n'a pas été tranché[34], l'événement a conduit le Department of Homeland Security à demander l'actualisation du rapport du National Research Council, *Terrorisme et système de distribution d'électricité,* rédigé en 2007 à sa demande et déclassifié en 2012[35]. Ce rapport se concentre sur la vulnérabilité du réseau ainsi que les moyens d'en accroître la protection et la résilience.

La réactivité des acteurs et la résilience du réseau en cas d'attaque ont été testées par des exercices de simulation d'attaques (GridEx[36]), en 2011, 2013, 2015 et 2017, qui intègrent ces réflexions. Si le premier GridEx a été mené à une échelle régionale, les suivants sont d'une ampleur beaucoup plus grande et combinent des attaques cyber et physiques. GridEx II, mené en 2013 à l'échelle du continent (le Canada et le Mexique y ont également participé), sur 48 heures, a ainsi plongé virtuellement dix millions d'Américains dans le noir et occasionné la mort fictive d'une centaine de membres des forces de l'ordre, ou de personnels des entreprises impliquées dans l'exercice. Les résultats de ces deux premiers exercices montrent, selon les rapports, une bonne coordination horizontale des industriels à l'échelle locale ou régionale, qui se détériore lorsqu'il est question de communiquer verticalement, avec les instances de régulation ou les agences fédérales pour gérer la crise[37].

Selon les rapports, ce manque de communication s'explique à la fois par des questions de protocole internes, une absence de culture de la coopération avec les acteurs fédéraux, ainsi qu'un manque de confiance des industriels à leur égard. À la suite de ce constat, les deux GridEx suivants (2015 et 2017) ont été largement centrés sur l'amélioration de la communication et de la coordination entre les différents acteurs impliqués (l'exercice concerne autour de 5 000 personnes). Des canaux de communication spécifiques, un système de partage d'information sur l'état du réseau, de coordination des messages envoyés à la population ont été mis en place et testés[38].

34. Michael Martinez, « Sniper attack on Silicon Valley grid spurs security crusade by ex-regulator », *Cable News Network*, 8 février 2014.
35. National Research Council, *Terrorism and the Electric Power Delivery System*, Washington, DC, The National Academies Press, 2012, https://doi.org/10.17226/12050.
36. Pour Grid Exercise : exercice sur le réseau.
37. NERC, *2011 NERC Grid Security Exercise, After action report,* Washington, 2012 ; NERC, *Grid Security Exercise (GridEx II), After action report*, Washington, 2014.
38. NERC, Gridex III Public Report, 2015 ; NERC, GridEx IV Public Report, 2017. Les rapports sont disponibles en ligne : https://www.nerc.com/pa/CI/CIPOutreach/Pages/GridEX.aspx.

Absence d'exercice européen et morcellement des coopérations

Contrairement aux États-Unis qui organisent des exercices à échelle fédérale, l'UE n'a pas mis en place d'exercice intégré à l'échelle communautaire. Les canaux de communication entre industriels, gestionnaires du réseau, gouvernements nationaux et structures européennes sont plus faibles. Il existe cependant au sein de l'UE des velléités de coordination comme le European Energy – Information Sharing & Analysis Centre[39]. Cependant ces initiatives n'ont jamais une dimension réellement européenne et elles n'impliquent pas les gouvernements. Surtout, l'approche européenne décorrèle en amont la sécurité physique du réseau des questions cyber, traitées à part, alors que l'approche nord-américaine part de l'aval, du réseau, pour se poser dans un second temps la question de la nature des menaces et des réponses possibles. Cette même approche décorrélée est employée dans les structures de l'OTAN, dont les centres d'excellence sur l'énergie et la coopération cyber (ENSEC COE et CCDCOE) sont alternativement présents dans des structures différentes sans afficher de vision intégrée sur le sujet.

Les acteurs français n'ont pas participé officiellement aux différentes initiatives de coordination à l'échelle européenne citées ci-dessus (SESAME ou EE-ISAC par exemple). Le réseau électrique français est pourtant l'un des plus performants d'Europe et RTE, son gestionnaire, est un acteur majeur et influent dans le paysage électrique européen. À l'échelle nationale, PIRANET, le plan gouvernemental consacré à l'intervention de l'État en cas de crise majeure d'origine informatique préparé et maintenu par l'ANSSI et le SGDSN, a intégré tardivement le réseau de transport d'électricité. Si PIRANET 2012 a associé des opérateurs d'importance vitale des secteurs de la santé, des transports et des communications, ce n'est qu'en 2016 que RTE, le gestionnaire du réseau d'électricité français, évoque dans son bilan de sûreté une participation à l'exercice ayant permis de « mettre en situation les compétences SI internes de RTE en matière de sécurité et de tisser des liens avec les services de l'État ».

CONCLUSION

La comparaison des stratégies de protection des réseaux de transport d'électricité américaine et européenne montre ainsi une double différence d'approche. Cette différence est scalaire. Les États-Unis ont construit une architecture institutionnelle intégrée fondée sur une interaction et une communication fluide entre les échelles. À l'inverse, le paysage européen est caractérisé par une pluralité d'initiatives à des échelles diverses sans que ne se dégage de réel leadership ou de vision intégrée du problème. Si ces constructions semblent *a priori* logiques dans la mesure où les États-Unis sont un État-nation alors que l'Union européenne est une organisation internationale avec une faible intégration politique, deux éléments viennent nuancer cette vision.

Premièrement, les États-Unis ont construit leur stratégie de réponse au risque à une échelle continentale et non à une échelle nationale, en intégrant le Canada et le Mexique dans leurs exercices de crise et en mettant en place une autorité de régulation internationale (la North American Electric Reliability Corporation) dès 1968. Inversement, l'UE, dont on attendrait des actions sur ce plan de la coopération internationale, en est paradoxalement bien plus absente : elle ne coordonne pas d'exercices à l'échelle de l'Union.

Deuxièmement, sur un plan technique, la politique d'intégration de l'UE a conduit à la mise en place progressive d'un réseau aujourd'hui très interconnecté et interdépendant à l'échelle européenne, ce qui le rend particulièrement sensible aux effets de cascade. Inversement, les États-Unis n'ont pas mené de politique d'intégration à l'échelle fédérale et les réseaux américains sont beaucoup moins interconnectés et interdépendants. Il y a donc une forme de paradoxe entre, d'une part, la nature de ces deux entités et, d'autre part, les politiques qu'elles mènent sur le plan technique des infrastructures et sur le plan de l'organisation de leur protection.

La même différence apparaît sur le plan sectoriel : la vision américaine intègre la gestion des vulnérabilités et des menaces physiques et cyber dans un seul plan de réponse centré sur le réseau, quand l'UE a séparé en amont les questions cyber et physiques qu'elle gère par des canaux différents. L'efficacité opérationnelle de cette approche européenne est questionnable dans un contexte d'évolution de la vulnérabilité de ces réseaux, marqués par une inter-

39. Le EE-ISAC cherche une amélioration de la cybersécurité et de la résilience des réseaux électriques via les partages d'informations et de données. Il est une initiative conjointe de quatre grands fournisseurs de services énergétiques européens (EDP, Enel, PSE, Alliander), d'organismes gouvernementaux et universitaires ainsi que de fournisseurs de technologies.

connexion et une ouverture au numérique croissantes, partiellement liée à la politique de transition énergétique. La question de la gestion des interdépendances issues de la politique énergétique de l'UE se pose alors du point de vue de la sécurité d'infrastructures essentielles au fonctionnement des sociétés européennes. La France s'inscrit dans ce contexte : si son réseau est l'un des plus performants d'Europe, il reste soumis aux mêmes types de vulnérabilité.

BIBLIOGRAPHIE

Articles et ouvrages scientifiques

BOSSONG Raphaël, « The European Programme for the protection of critical infrastructures – meta-governing a new security problem? », *European Security*, 23:2, 14 janvier 2014, p. 210-226, DOI : http://doi.org/10.1080/09662839.2013.856307.

GALLAND Jean-Pierre, « Critique de la notion d'infrastructure critique », *Flux,* mars 2010 (n° 81), p. 6-18. DOI : http://doi.org/10.3917/flux.081.0006, https://www.cairn.info/revue-flux1-2010-3-page-6.htm.

LAGENDIJK Vincent, *Electrifying Europe: The Power of Europe in the Construction of Electricity Networks*, Amsterdam University Press, 2008.

MORSEL Henri, « Industrie électrique et défense en France lors des deux conflits mondiaux. Électricité, armement, défense », *Bulletin d'histoire de l'électricité*, n° 23, 1994, p. 7-17.

LINDSTRÖM Madelene, OLSSON Stefan, « The European Programme for Critical Infrastructure Protection », *in* OLSSON, Stefan (dir.), *Crisis Management in the European Union*, Springer, Berlin, Heidelberg, 2014, DOI : https://doi.org/10.1007/978-3-642-00697-5_3.

REGHEZZA Magali, VEYRET Yvette, « Aléas et risques dans l'analyse géographique », *Annales des mines*, octobre 2003.

–, « Vulnérabilité et risques, l'approche récente de la vulnérabilité », *Responsabilité et environnement*, n° 43, juillet 2006.

Sources techniques

Center for the Study of the Presidency and Congress, *Securing the U.S. Electrical Grid, The honorable Thomas F. McLarty III & the honorable Thomas J. Ridge*, 2014, https://www.thepresidency.org/sites/default/files/Final%20Grid%20Report_0.pdf.

Congress of the United States, House of Representatives, *Infection of the Davis Besse Nuclear Plant by the "Slammer" Worm Computer Virus – Follow-up Questions*, Paper LTR-03-0695, 22 octobre 2003, https://www.nrc.gov/docs/ML0329/ML032970134.pdf.

ENTSO-E, *Network Code on Emergency and Restoration*, 25 mars 2015.

Mc Afee, *Smarter protection for the smart grid*, rapport, 2012, https://www.ccn-cert.cni.es/.../rp-smarter-protection-smart-grid.pdf.

National Research Council, *Terrorism and the Electric Power Delivery System,* Washington, DC, The National Academies Press, 2012, https://doi.org/10.17226/12050.

NERC, *2011 NERC Grid Security Exercise, After action report*, 2012, Washington.

NERC, *Grid Security Exercise (GridEx II), After action report*, 2014, Washington.

NERC, *Gridex III Public Report*, 2015.

NERC, *GridEx IV Public Report*, 2017.

RTE, *Schéma décennal de développement du réseau*, 2015.

SESAME (Delft University of Technology, Politecnico di Torino, INDRA et Transelectrica), *System Specification of Decision Support System,* Délivrable n° 4.1, 2012.

SESAME (Transelectrica, Politecnico di Torino), *Report on the analysis of historic outages,* Délivrable n° D1.1, 2011.

SESAME (Heriot-Watt University), *Assessment of Security of Electricity Supply (SES) Indicators in Europe*, Délivrable n° D3.1, 2014.

US Department of Homeland Security, Industrial Control Systems Cyber Emergency Response Team, *Alert (IR-ALERT-H-16-056-01) Cyber-Attack Against Ukrainian Critical Infrastructure*, 25 février 2016, https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01.

Entretiens

Entretiens menés au sein du Réseau européen des gestionnaires de réseau de transport d'électricité européens (ENTSO-E) à Bruxelles de janvier à juillet 2014.

Entretiens menés au JRC-IET le 21 mai 2013 à Petten (Pays-Bas).

Textes de référence

Union européenne

Traité de Lisbonne, 2009, art. 194.

Commission européenne, COM(2004) 701 du 20 octobre 2004, *Lutte contre le terrorisme : préparation et gestion des conséquences*.

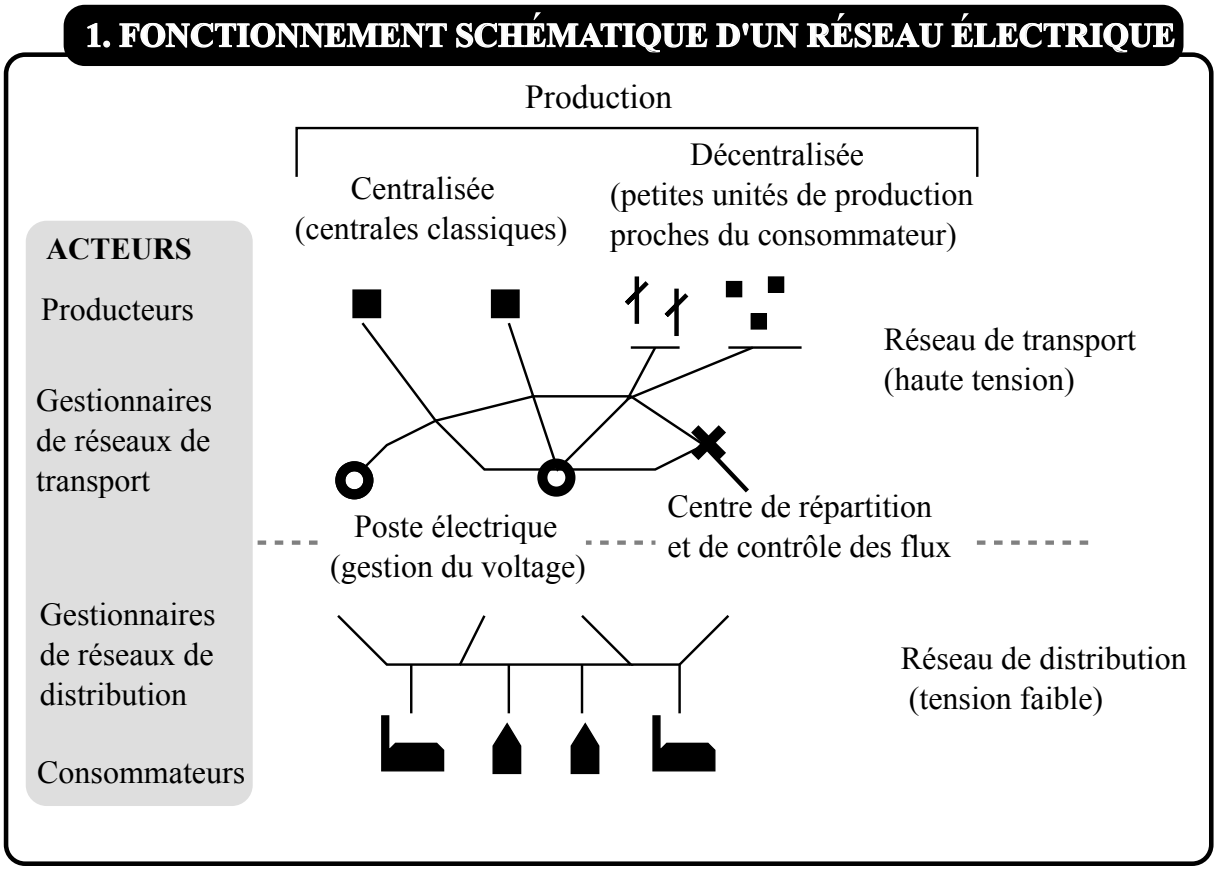
Commission européenne, COM(2004) 698 du 20 octobre 2004, *Attaques terroristes : prévention, préparation et réponse.*

Commission européenne, COM(2005) 576, *Livre vert du 17 novembre 2005 sur un Programme européen de protection des infrastructures critiques (EPCIP)*.
Directive 2008/114/CE du Conseil du 8 décembre 2008 concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection.
Règlement (CE) n° 714/2009 du Parlement européen et du Conseil du 13 juillet 2009 sur les conditions d'accès au réseau pour les échanges transfrontaliers d'électricité.
Commission européenne, *Commission staff working document on a new approach to the European Programme for Critical Infrastructure Protection Making European Critical Infrastructure more secure*, SWD(2013) 318, 2013.
Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union.

France
Code de la défense – articles L. 1332-1 à L. 1332-7, L. 2151-1 à L.2151-5 et R. 1332-1 à R. 1332-42.
Instruction générale interministérielle n° 6 600 relative à la sécurité des activités d'importance vitale du 7 janvier 2014.
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, art. 22.
LOI n° 2018-607 du 13 juillet 2018 relative à la programmation militaire pour les années 2019 à 2025 et portant diverses dispositions intéressant la défense, art. 18 à 22.

ANNEXES

1. Généralités techniques sur la structure et le fonctionnement d'un réseau électrique
2. Schéma de l'architecture institutionnelle de la protection du système de transport d'électricité américain
3. Schéma de l'architecture institutionnelle de la protection du système de transport d'électricité européen



Points techniques particuliers du fonctionnement d'un réseau

Un courant électrique alternatif est caractérisé par sa fréquence, il est produit par la rotation d'un alternateur. La fréquence du réseau doit être maintenue à chaque instant pour assurer l'approvisionnement.

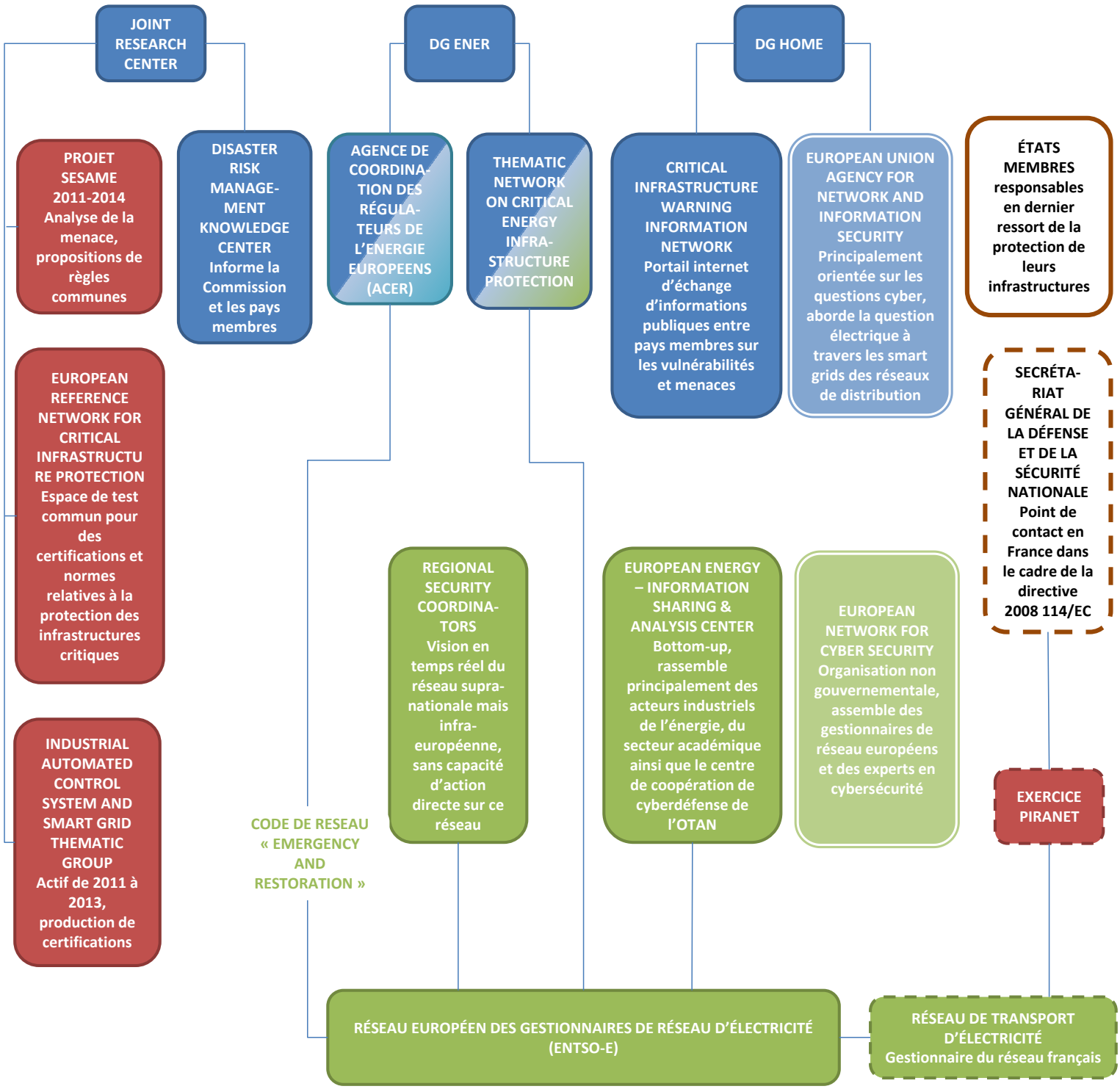
Un réseau dit « synchrone » est un réseau où le courant a la même fréquence, il y a cinq zones synchrones différentes dans l'UE (pour l'utilisateur, changer de zone synchrone implique d'utiliser un adaptateur de prise pour le branchement des appareils).

Il n'est pas possible de prévoir le trajet de l'électricité sur le réseau.

2. SCHÉMA DE L'ARCHITECTURE INSTITUTIONNELLE DE LA PROTECTION DU SYSTÈME DE TRANSPORT D'ÉLECTRICITÉ AMÉRICAIN

Réalisation : A. Palle, 2018

3. SCHÉMA DE L'ARCHITECTURE INSTITUTIONNELLE DE LA PROTECTION DU SYSTÈME DE TRANSPORT D'ÉLECTRICITÉ EUROPÉEN



ÉCHELON EUROPÉEN | RÉGULATION | GESTION-NAIRES DE RÉSEAU | ACTEURS FRANÇAIS | PROGRAM-MES DE RECHERCHE, EXERCICES | ACTEURS NATIONAUX | ACTEURS DE LA PROTECTION CYBER POUR QUI LES RÉSEAUX SONT UN ÉLÉMENT SECONDAIRE

Réalisation : A. Palle, 2018

Angélique Palle est docteur en géographie de l'Université Paris 1 Panthéon-Sorbonne, où elle a travaillé au cours de sa thèse sur les questions d'approvisionnement et de transition énergétique, ainsi que sur les dynamiques d'intégration régionale. Ses travaux ont notamment été publiés dans *La Revue internationale et stratégique, Flux* ou à l'Oxford Institute for Energy Studies. Depuis octobre 2017, elle est chercheur à l'IRSEM au sein du domaine « Armement et économie de défense » et traite en particulier des questions d'approvisionnement en énergie et matériaux stratégiques, de protection des réseaux d'infrastructures d'énergie et sur les liens entre le développement durable et la Défense.

Contact : angelique.palle@irsem.fr