Sécuriser le réseau électrique européen : un défi de gouvernance pour l'Union européenne

Margaux Grellety
Association Werra
Août 2021

C’est en intégrant Sciences Po Paris en Bachelor sur son campus euro-latino-américain de Poitiers que **Margaux Grellety** découvre et s’intéresse à la zone Amérique latine et Caraïbes. Après un an d’échange au Mexique, elle se concentre sur les enjeux de défense et de sécurité et intègre le Master International Security de l’école d’affaires internationales de Sciences Po, dont elle est diplômée en 2020. Passionnée de géopolitique, elle cherche à se spécialiser dans la gestion de crise et rejoint pour l’année 2021-2022 l’IRIS Sup’ en tant qu’étudiante alternante dans le Master 2 « défense, sécurité et gestion de crise ».

INTRODUCTION

En mars 2019 au Venezuela, une panne d'électricité plonge 80% de la population dans le noir. Les hôpitaux déplorent des décès à cause de l'arrêt des dialyses, la capitale est paralysée par la suspension des transports en commun tandis que les supermarchés ferment leurs portes, faute de pouvoir maintenir les produits au frais et les terminaux de paiement opérationnels. Pour le gouvernement de Nicolás Maduro, le black-out est dû à une attaque cybernétique tandis que pour le chef de l'opposition, Juan Guaidó, celui-ci est la conséquence du manque d'investissement dans les infrastructures[1]. Dans les deux cas, le black-out illustre à quel point l'électricité est une composante vitale de nos sociétés, permettant non seulement l'approvisionnement en biens de première nécessité, mais se trouvant également au cœur de l'économie nationale et mondiale ainsi que des moyens de communication. Sa production et sa distribution sur l'ensemble des territoires reposent sur un réseau d'infrastructures qui sont vulnérables aux aléas naturels et des cibles stratégiques potentielles.

Pour l'Union européenne (UE), l'énergie est un élément central de sa construction. En 1951, la Communauté européenne du charbon et de l'acier (CECA) met en avant la nécessité pour les États de s'entendre sur la production et la distribution de l'énergie. Cet intérêt s'explique par le caractère stratégique des infrastructures énergétiques pour les Européens et ce, dès la Seconde Guerre mondiale. Durant cette période, les futurs pays fondateurs de ce qui deviendra l'UE intègrent les réseaux électriques et leur contrôle dans l'effort de guerre en tant qu'infrastructures de sécurité nationale, à la fois pour renforcer les lignes en cas d'attaques et pour soutenir l'effort de guerre économique. En France par exemple, une police spéciale est formée pour garder et protéger les infrastructures électriques qui font l'objet d'opérations de sabotage de la part de la Résistance[2]. À partir de la guerre froide, la guerre asymétrique, qui repose sur une faiblesse de moyens d'une des parties au conflit par rapport à l'impact des dommages obtenus sur l'adversaire visé, se généralise. Les attentats du 11 septembre 2001 aux États-Unis en seront un exemple caractéristique et avec eux, la prise de conscience d'une nouvelle vulnérabilité. Le secteur de l'énergie s'inscrit dans cette tendance. Les infrastructures réseaux sont ainsi endommagées pour servir une stratégie d'affaiblissement des moyens de

[1] François-Xavier Gomez, « Au Venezuela, le black-out s'installe, la crise perdure », *Libération*, 10 mars 2019, consulté le 7 juillet 2021 : https://www.liberation.fr/planete/2019/03/10/au-venezuela-le-black-out-s-installe-la-crise-perdure_1714250/
[2] Angélique Palle, « Power networks as targets : hazards, vulnerabilities and protection of electricity networks from the Second World War to 21th Century asymmetric conflicts », *Flux*, 2019/4 n°118, pp. 46-58, Université Gustave Eiffel

l'adversaire et avec l'apparition de nouvelles technologies, le risque d'une attaque physique est accru par celui naissant des attaques cyber.

Pour l'UE, l'enjeu lié à l'énergie et ses infrastructures a donc changé de dimension. Il est passé d'un besoin de contrôler la production des autres États pour prévenir un potentiel conflit interétatique, à celui de coopérer pour se protéger de nouvelles menaces. L'énergie électrique fait en effet partie d'un secteur en pleine mutation, soumis à des impératifs économiques de rationalisation des coûts et d'efficacité de production et à l'injonction politique de devenir plus durable, en prenant en compte son impact environnemental. Dès lors, le développement du réseau électrique européen repose de plus en plus sur ces nouvelles technologies qui, si elles sont un outil pour répondre à ces demandes, comportent de nouveaux risques. En 2015, l'attaque cyber d'un réseau de transport d'électricité ukrainien qui touche environ 225 000 consommateurs, attribuée à la Russie, est la première d'une telle ampleur à mettre en avant ces nouveaux enjeux[3].

En 2014, Raphaël Bossong publie un article sur le défi de « métagouvernance » de l'UE dans le domaine de la protection des infrastructures critiques. Il la définit comme la capacité à « stimuler et maintenir des efforts de gouvernance entre plusieurs acteurs sectoriels et politiques sur des sujets complexes »[4]. La protection des infrastructures électriques représente en effet un enjeu complexe, puisqu'elle concerne un secteur en développement, qui regroupe une grande diversité d'acteurs et d'échelles territoriales. Le propos de cet article est ainsi d'essayer de comprendre cette complexité, d'abord en s'intéressant au concept même d'infrastructure critique pour le réseau électrique et aux vulnérabilités qui y sont associées. Il s'agira ensuite de s'intéresser au développement de cette gouvernance européenne, pour l'instant sectorielle et qui peine à coordonner les différents acteurs concernés. Enfin, la dernière partie tâchera de donner un aperçu de la spécificité que représente la cybersécurité dans l'UE sur les questions énergétiques et comment celle-ci s'articule avec d'autres acteurs, notamment l'OTAN.

[3] Angélique Palle, « Vulnérabilité et protection des réseaux électriques : approches comparées Union européenne – Etats-Unis », *IRSEM*, note de recherche N°62, 28 septembre 2018

[4] 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 : http://doi.org/10.1080/09662839.2013.856307

Infrastructures critiques européennes : faire face à d'anciennes et de nouvelles vulnérabilités

Qu'est-ce qu'une infrastructure critique et à quels risques est-elle exposée ?

Le réseau électrique européen repose sur un ensemble d'infrastructures nationales et transfrontalières qui permettent la production de l'électricité et sa distribution. Si ces infrastructures sont reconnues comme stratégiques, c'est-à-dire essentielles à l'activité des États, le terme « d'infrastructure critique » fait débat. La notion apparaît dans les textes officiels américains dans les années 1950 et suite aux attentats du 11 septembre 2001, Washington décide de définir une stratégie nationale pour leur protection[5]. En France, le concept apparaît après la Seconde Guerre mondiale dans le Code de la défense de 1958 mais revêt le nom de « secteurs d'activité opérateurs d'importance vitale ». Cette définition inclut toutes les activités « 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 »[6]. À échelle européenne, c'est suite aux attentats de Londres et de Madrid en 2004 et 2005 que le concept se diffuse. À partir de 2006, dans la directive pour l'identification des infrastructures critiques européennes, la Commission adopte le terme « d'infrastructure critique européenne » dont la « destruction ou l'endommagement auraient des impacts significatifs sur au moins deux États-membres »[7].

La protection de ces infrastructures critiques face à différents risques pose la question de la définition de ces derniers. Longtemps circonscrits à une aire géographique et une temporelle spécifiques, par exemple les effets directs d'une inondation, cette méthode d'analyse a représenté un obstacle à leur compréhension et donc leur gestion[8]. À partir des années 2000, dans le sillage de plusieurs crises d'ampleur mondiale (les attentats du 11 septembre 2001, la crise des *supbrimes* de 2008, le tsunami de 2011 au Japon), des chercheurs et géographes

[5] Angélique Palle, « Vulnérabilité et protection des réseaux électriques : approches comparées Union européenne – Etats-Unis », *IRSEM*, note de recherche N°62, 28 septembre 2018

[6] Danile d'Elia, « Opérations et stratégies défensives, les systèmes d'information d'importance vitale », *La Cyberdéfense, politique de l'espace numérique*, chapitre 8, pp. 167 à 175, Armand Collin, 2018

[7] 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 : http://doi.org/10.1080/09662839.2013.856307

[8] Magali Reghezza-Zitt, « Penser la vulnérabilité dans un contexte de globalisation des risques grâces aux échelles spatiales et temporalles », *Espace population société*, 2016/3

analysent ces « nouveaux risques » à l'aune des dommages qu'ils causent, souvent transfrontaliers et durables dans le temps. Cette « globalisation » du risque, étudié selon le prisme de la vulnérabilité des populations, territoires ou infrastructures qui en subissent les effets, permet une analyse plus large qui considère leurs impacts directs et indirects et les différentes échelles spatiales et temporelles qui en subissent les conséquences[9].

Selon cette approche globale, le risque est composé de trois éléments : l'aléa, la vulnérabilité et la résilience. Appliqués aux réseaux électriques, ils représentent le risque que les infrastructures subissent une attaque physique ou cyber (aléa), les potentiels facteurs aggravants de cette attaque, en fonction de leur accessibilité, de leur vétusté, de la redondance des infrastructures (vulnérabilité) et enfin, la capacité du gestionnaire du réseau à intervenir rapidement et répondre en lien avec les acteurs concernés aux problèmes générés par l'attaque (résilience)[10]. En outre, l'analyse des risques et l'identification des infrastructures critiques dépendent de critères politiques qui évoluent en fonction des intérêts nationaux. En effet, les coûts qui seront engagés pour les protéger doivent être proportionnés aux coûts potentiels d'une attaque, de sa probabilité d'occurence et du coût d'un retour à la normale. Cette étude au cas par cas s'accompagne ainsi de la considération de « seuils de vulnérabilité acceptable »[11], changeant selon les moyens économiques et politiques des États-membres.

Un secteur spécifique avec d'anciennes et de nouvelles vulnérabilités

L'étude du risque pour le secteur de l'énergie doit prendre en compte le fait que celui-ci possède des spécificités qui représentent des contraintes structurelles à toute volonté de sécurisation. La Commission européenne en identifie trois. D'abord, le besoin en temps réel, soit une réactivité indispensable qui ne permet pas d'appliquer des mesures de sécurité trop lourdes. Ensuite, l'effet de cascade, car les grilles électriques sont interconnectées dans l'UE et au-delà et qu'un effet sur un pays peut avoir des conséquences dans d'autres secteurs et pays. Cela a par exemple été le cas en 2006 lorsqu'un incident en Allemagne a affecté 15 millions de

[9] *Ibid.*
[10] Angélique Palle, « Vulnérabilité et protection des réseaux électriques : approches comparées Union européenne – Etats-Unis », *IRSEM*, note de recherche N°62, 28 septembre 2018
[11] *Ibid.*

consommateurs dans douze pays de l'UE[12]. Enfin, la nécessité de combiner des systèmes anciens, pensés et mis en place au siècle précédent et des nouvelles technologies[13]. En effet, que ce soit dans une logique de transition énergétique en recourant davantage aux énergies renouvelables ou pour approfondir l'intégration du marché commun de l'énergie, le réseau électrique européen a besoin d'être plus flexible et donc digitalisé[14].

Depuis le début des années 2000, on assiste ainsi à une plus grande prise en compte du risque sécuritaire dans le secteur de l'énergie par les États-membres de l'UE. Aujourd'hui, il se décline sous deux formes : la menace physique et la menace cyber. Pour la première, les risques peuvent être à la fois liés à des aléas techniques ou des défaillances de maintenance, mais également à des attaques malveillantes. Ainsi en 2013, aux États-Unis, le poste électrique de *Metcalf* qui alimente la Silicon Valley a subi une attaque à l'AK-47 qui a mis hors service dix-sept transformateurs pendant plus de vingt minutes[15]. Pour la seconde, le développement rapide des nouvelles technologies a engendré l'apparition de nouvelles vulnérabilités, dont l'attaque ukrainienne de 2015 a représenté un exemple marquant. Bien qu'il n'y ait pas eu de conséquences mortelles, le coût des attaques cyber pour les acteurs touchés sont considérables. En outre, le rapport annuel de l'Agence de l'UE pour la cybersécurité (ENISA) de 2020 révèle une complexification des cyberattaques, qui sont devenues plus sophistiquées, massives et difficiles à détecter. Il souligne aussi la diversification des secteurs attaqués, ce qui rend encore plus difficile l'identification de quelques infrastructures plus critiques que d'autres[16].

La difficulté d'identifier les infrastructures considérées comme critiques et de répondre ensuite à ces attaques est ainsi exacerbée par le fait qu'elles touchent une grande diversité de secteurs et nécessitent une capacité de coordination de nombreux acteurs, aussi bien institutionnels que privés. Pour l'UE, elle est amplifiée par l'interdépendance des réseaux électriques et leur caractère transfrontalier, ainsi que la quantité d'acteurs mobilisés sur le sujet,

---

[12] Angélique Palle, « Power networks as targets : hazards, vulnerabilities and protection of electricity networks from the Second World War to 21th Century asymmetric conflicts », *Flux*, 2019/4 n°118, pp. 46-58, Université Gustave Eiffel

[13] Commission européenne, « Critical infrastructure and cybersecurité », 28 avril 2021, consulté le 25 mai 2021 : https://ec.europa.eu/energy/topics/energy-security/critical-infrastructure-and-cybersecurity_en

[14] Commission européenne, « Electricity market design », 20 mai 2021, consulté le 25 mai 2021 : https://ec.europa.eu/energy/topics/markets-and-consumers/market-legislation/electricity-market-design_en

[15] Angélique Palle, « Vulnérabilité et protection des réseaux électriques : approches comparées Union européenne – Etats-Unis », *IRSEM*, note de recherche N°62, 28 septembre 2018

[16] Commission européenne, « rapport sur l'inventaire des cybermenaces dans l'UE : les attaques deviennent de plus en plus sophistiquées, ciblées et massives », 20 octobre 2020, consulté le 6 juillet 2021 : https://ec.europa.eu/france/news/20201020/rapport_cybermenaces_enisa_fr

puisque qu'on compte aujourd'hui quarante-deux gestionnaires de réseaux au niveau européen qui représentent trente-cinq pays[17]. La sécurité de ces infrastructures représente ainsi un vrai défi de gouvernance à l'échelle européenne.

[17] ENTSO-E, « Mission statement », consulté le 7 juillet 2021 : https://www.entsoe.eu/about/inside-entsoe/objectives/

Un enjeu de gouvernance transfrontalier et multi-sectoriel

Les initiatives institutionnelles européennes

La première tentative d'élaboration d'une gouvernance européenne sur le sujet date de 2005, quand la Commission européenne publie un livre vert dans le but de lancer, en lien avec le Conseil de l'UE, un programme de protection des infrastructures critiques après les attentats de 2004 à Madrid[18]. Dès lors, les divergences de points de vue des États quant à la définition de ce qui constitue ou non une infrastructure critique apparaissent. Si le livre vert comprenait initialement onze secteurs économiques et sociétaux composés d'infrastructures critiques, ils sont réduits à ceux de l'énergie et des transports dans la directive de 2008 qui en est issue, dans laquelle seulement treize infrastructures sont considérées comme critiques au sein de l'UE. Parmi celles-ci, les réseaux de transport de gaz et d'électricité n'en font pas partie[19]. C'est dans cette directive de 2008 qu'apparaît la définition « d'infrastructures critiques européennes » dans le cadre du programme européen pour la protection de ces infrastructures (EPCIP), qui introduit le caractère transfrontalier du risque. En 2013, la Commission européenne identifie les limites de la directive de 2008 et envisage d'étendre cette protection à d'autres secteurs économiques. Elle insiste par ailleurs sur sa volonté de protéger quatre infrastructures européennes qui, jusqu'alors, étaient à la charge des États-membres qui les accueillent : le système de contrôle de l'aviation européenne (Eurocontrol), le système de navigation satellitaire GALILEO et les réseaux de transmission énergétiques et gaziers transfrontaliers[20].

La sécurité de ces infrastructures électriques est cependant intégrée dans une approche plus vaste, qui est celle de la sécurité de l'approvisionnement. Elle dépend de la capacité du réseau à maintenir un flux ininterrompu d'électricité malgré un plus grand recours aux énergies renouvelables, dont l'irrégularité le met sous tension[21]. Cet impératif politique, ajouté à celui

[18] Angélique Palle, « Power networks as targets : hazards, vulnerabilities and protection of electricity networks from the Second World War to 21th Century asymmetric conflicts », *Flux*, 2019/4 n°118, pp. 46-58, Université Gustave Eiffel

[19] *Ibid.*

[20] 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 : http://doi.org/10.1080/09662839.2013.856307.

[21] Commission européenne, « à la une : sécurité de l'approvisionnement énergétique de l'UE », 27 avril 2020, consulté le 25 mai 2021 : https://ec.europa.eu/info/news/focus-energy-security-eu-2020-avr-27_fr

d'une plus grande intégration économique du marché de l'énergie, sont prioritaires par rapport à une approche strictement sécuritaire de défense des infrastructures énergétiques. La protection du réseau électrique est ainsi traitée dans le cadre du règlement sur la préparation aux risques dans le secteur de l'électricité, intégré au paquet « une énergie propre pour tous les Européens » de 2019. Ce règlement exige des États-membres qu'ils utilisent des méthodes communes, identifient tout le spectre de crises potentielles liées à l'électricité, recensées sous forme de scénarios et se préparent en fonction de ceux-ci. Il fait suite à un rapport indépendant de mai 2015 qui soulignait que les réponses des États-membres à des crises potentielles dans le secteur de l'énergie tendaient à être strictement nationales[22]. Pour inciter au partage d'expérience et d'expertise, la Commission met également en place un groupe de coordination de l'électricité qui l'assiste sur ses réflexions et productions écrites sur la sécurité de l'approvisionnement énergétique, composé de représentants des gouvernements nationaux, des agences de régulation des énergies nationales, de l'association du réseau des gestionnaires de l'électricité (ENTSO-E) et de l'Agence de coopération pour les gestionnaires de l'énergie (ACER)[23]. Le rôle de cette dernière est redéfini dans le paquet de 2019 et, en plus de ses missions de soutien à l'intégration énergétique des États et au respect des règles du marché intérieur européen pour l'énergie et le gaz naturel, elle devient le coordinateur des gestionnaires de l'énergie nationaux et des centres de coordination régionaux et intervient dans les dossiers où les divergences entre les États-membres sont particulièrement saillantes[24].

Ainsi pour l'UE, la sécurité de son réseau électrique reste subordonnée à la question du marché intérieur de l'énergie et de la transition énergétique. Si des initiatives ont vu le jour, elles incitent surtout les États-membres à prendre en compte la menace sécuritaire et à coopérer, sans pour autant être contraignantes ni centralisées autour d'une agence supranationale de coordination des politiques sur les infrastructures critiques[25]. Les institutions européennes se heurtent ainsi aux réticences des États-membres à se coordonner sur des sujets stratégiques sensibles, à la difficulté de gérer de façon multi-sectorielle des politiques qui sont par ailleurs régulées par secteurs et enfin, d'impliquer des acteurs institutionnels, industriels ou

[22] Commission européenne, « Electricity market design », 20 mai 2021, consulté le 25 mai 2021 : https://ec.europa.eu/energy/topics/markets-and-consumers/market-legislation/electricity-market-design_en
[23] Commission européenne, « Security of electricity supply », 16 juin 2020, consulté le 25 mai 2021 : https://ec.europa.eu/energy/topics/energy-security/security-electricity-supply_en?redir=1
[24] Commission européenne, « Electricity market design », 20 mai 2021, consulté le 25 mai 2021 : https://ec.europa.eu/energy/topics/markets-and-consumers/market-legislation/electricity-market-design_en
[25] 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 : http://doi.org/10.1080/09662839.2013.856307

scientifiques. Ces derniers défendent alors leur propre approche de la protection des réseaux électriques, à la fois révélatrice de manquements institutionnels et moteur pour développer la coopération sur le sujet dans l'UE.

Des acteurs privés dynamiques

En 2008, les quarante-deux gestionnaires réseaux nationaux qui constituent le réseau européen de distribution électrique, fondent l'association ENTSO-E. Elle définit son objectif principal comme la facilitation de « la coordination régionale entre les gestionnaires » et souhaite « assurer un accès efficace et transparent aux systèmes de transmission, tout en fournissant une planification coordonnée et prospective »[26]. Ce sont en effet les gestionnaires réseaux qui sont responsables à la fois de la sécurité d'approvisionnement dans leur territoire national en temps réel et d'une projection à long terme sur les évolutions des grilles électriques (décentralisation, recours aux énergies renouvelables, stockage, etc.), qu'ils planifient sur dix ans aux niveaux national et européen. Pour harmoniser la gestion à échelle européenne, ils se reposent sur des coordinateurs de sécurité régionaux, qui apparaissent officiellement en 2015 dans le cadre d'un accord multilatéral signé entre tous les gestionnaires au sein de l'ENTSO-E, suivi en 2016 de la publication d'un guide de bonnes pratiques[27]. Chaque gestionnaire possède ainsi un coordinateur régional de référence pour assurer une stratégie concertée. Ces derniers fournissent des modèles de grilles communs, issus de la centralisation des données nationales des gestionnaires, ainsi que des analyses sécuritaires régionales. L'ENTSO-E met également à disposition une base de données et une plateforme d'échanges pour favoriser le partage d'outils.

La capacité de coordination régionale mise en place par l'ENTSO-E a incité la Commission européenne à la mandater pour rédiger des codes de réseau communs à l'UE[28], en lien avec l'ACER. Ces codes sont un ensemble de règles communes qui définissent, chacun dans leur champ d'application, des « exigences techniques ou opérationnelles applicables aux différentes catégories d'acteurs » [29]. Ils prennent la forme législative de règlements européens et sont donc

[26] Rapport de ENTSO-E, « managing critical grid situations – success and challenges », mai 2017, consulté le 08 juin 2021 : https://www.entsoe.eu/publications/system-operations-reports/#managing-critical-grid-situations---success-and-challenges

[27] *Ibid.*

[28] Angélique Palle, « Power networks as targets: hazards, vulnerabilities and protection of electricity networks from the Second World War to 21th Century asymmetric conflicts », *Flux*, 2019/4 n°118, pp. 46-58, Université Gustave Eiffel

[29] Commission de régulation de l'énergie (CRE), « Codes des réseaux européens », 13 janvier 2020, consulté le 5 juillet 2021 : https://www.cre.fr/Electricite/Reseaux-d-electricite/codes-de-reseau-europeens

mis en œuvre à échelle nationale, les gestionnaires réseaux proposant certains paramètres spécifiques qui doivent être approuvés par les autorités nationales compétentes. Ces codes sont également accompagnés de lignes directrices qui définissent les grands principes de gestion des systèmes électriques entre les États-membres sur les plans technique et de marché intérieur.

Le fait qu'il soit plus facile de passer par des acteurs sectoriels pour une coordination européenne de la sécurité des infrastructures électriques est également visible au niveau de la coopération scientifique. En 2011, le centre de recherche conjointe (JRC), dans le cadre du programme européen pour la protection des infrastructures critiques, lance le projet de réseau européen de référence sur la protection des infrastructures critiques (ERNCIP). Il a vocation à faire le lien entre les laboratoires et les infrastructures expérimentales qui travaillent sur les vulnérabilités des infrastructures critiques à travers des travaux de recherche par groupes thématiques. En 2020 par exemple, des rapports ont été publiés sur le contrôle industriel automatique des « grilles intelligentes », l'usage de la vidéosurveillance ou encore les risques nucléaires, biologiques et chimiques pour ces infrastructures[30]. Cette coopération de la recherche scientifique permet ainsi la production d'études comparatives et a pour but de stimuler une harmonisation des standards de sécurité. Le réseau permet en outre de dynamiser les rencontres entre les acteurs dont les discussions se tiennent également au sein de la Direction générale énergie de la Commission européenne.

L'UE utilise par ailleurs le financement de projets de recherche pour stimuler la coopération européenne sur le sujet. Dans le cadre de son septième programme de recherche et de développement technologique, la Commission a par exemple co-financé le projet SESAME[31], coordonné par l'institut *Politecnico di Torino* et un consortium de recherche qui regroupait des industriels italiens, autrichiens, espagnols, néerlandais, roumains et britanniques. Le programme, clôturé en 2014, insistait notamment sur les nouvelles menaces qui pesaient sur l'approvisionnement en énergie, aussi bien physiques que cyber. Le nouveau programme d'appel à projets, Horizon 2020, a poursuivi cette démarche en insistant davantage sur le lien opérationnel entre la production scientifique et les industriels du secteur.

[30] Joint Research Center, « The European Reference Network for Critical Infrastructure Protection (ERNCIP) Project Platform », last update 24 avril 2021, consulté le 6 juillet 2021 : https://erncip-project.jrc.ec.europa.eu

[31] « Sécuriser le système électrique européen contre les menaces accidentelles et malveillantes », voir notamment les divers travaux d'Angélique Palle sur celui-ci.

L'absence de la France dans le programme SESAME alors que son réseau électrique est l'un des plus performants de l'UE et son gestionnaire réseau, RTE, un acteur européen central[32], illustre cependant les difficultés de coordination entre les États-membres. L'architecture institutionnelle européenne de réponse à la menace sécuritaire des réseaux électriques est ainsi davantage à l'initiative des gestionnaires réseaux ou des scientifiques, dont les propositions sont soutenues de près ou de loin par la Commission européenne, que des États-membres. Cette gestion sectorielle est par ailleurs renforcée par le fait que l'UE dissocie la gestion des risques physiques et des risques cyber[33]. Avec cette approche, elle se démarque d'une vision plus intégrée de la protection des infrastructures critiques, ce qui représente un enjeu de coopération supplémentaire avec d'autres organisations sécuritaires régionales, comme l'OTAN.

[32] Angélique Palle, « Vulnérabilité et protection des réseaux électriques : approches comparées Union européenne – Etats-Unis », *IRSEM*, note de recherche N°62, 28 septembre 2018
[33] *Ibid.*

La cybersécurité européenne : enjeu de sécurité et de coopération à part entière

La cybermenace dans le secteur énergétique : un élément à part entière

Avec près de 500 millions de citoyens à approvisionner en énergie[34], l'UE cherche à renforcer la capacité de son réseau électrique à maintenir un flux ininterrompu tout en recourant davantage aux énergies renouvelables, censées fournir 32% de son énergie d'ici 2030[35]. Or, que ce soit pour stocker l'énergie, compenser les mises sous tension ou favoriser l'efficacité de la production, la digitalisation représente de plus en plus un outil ambivalent, rendant les grilles électriques vulnérables face à de nouveaux risques, dont les cyberattaques.

Dans la première directive européenne de 2008 sur la protection des infrastructures critiques, l'UE développe un agenda indépendant sur la cybersécurité, focalisée sur le développement des nouvelles technologies et la compétitivité économique, séparée des risques physiques[36]. En effet, l'UE n'aborde pas la question de la cybersécurité, prérogative des États, avant 2013 avec la « stratégie de cybersécurité de l'UE : un cyberespace ouvert, sûr et sécurisé ». Publiée conjointement par la Commission européenne et la haute représentante pour les affaires étrangères et la politique de sécurité, elle soutient une approche de consolidation des systèmes informatiques et de renforcement de leur capacité de résilience, plutôt qu'une suppression de la menace cyber[37]. La stratégie est complétée en 2016 par la directive *Network and Information System Security* qui détermine des normes auxquelles les entreprises doivent se soumettre pour renforcer la cybersécurité civile et exige la notification des incidents pour les entreprises qualifiées « d'opérateurs de services essentiels ». En 2017, avec le « paquet cybersécurité », la Commission reconnaît que chaque secteur est confronté à ses propres enjeux

[34] Commission européenne, « à la une : sécurité de l'approvisionnement énergétique de l'UE », 27 avril 2020, consulté le 25 mai 2021 : https://ec.europa.eu/info/news/focus-energy-security-eu-2020-avr-27_fr

[35] Conseil de l'Union européenne, *Efficacité énergétique, énergies renouvelables, gouvernance de l'union de l'énergie : le Conseil approuve 3 grands dossiers en matière d'énergie propre*, communiqué de presse, 4 décembre 2018, consulté le 7 juillet 2021 : https://www.consilium.europa.eu/fr/press/press-releases/2018/12/04/energy-efficiency-renewables-governance-of-the-energy-union-council-signs-off-on-3-major-clean-energy-files/

[36] 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 : http://doi.org/10.1080/09662839.2013.856307

[37] Morgan Jouy, « Une cyberdéfense collective en Europe ? L'articulation entre cyberdéfense européenne et transatlantique », *IRSEM*, note de recherche n°83, 23 octobre 2019

cyber et soutient une approche sectorielle, y compris dans le secteur de l'énergie[38]. Dès lors, la Commission souhaite favoriser le partage d'information et d'expérience via l'organisation de forums et tables rondes, comme à Bruxelles en 2018 avec la conférence de haut niveau sur la cybersécurité dans le domaine de l'énergie. En 2019, elle publie au journal officiel de l'UE un rapport avec des recommandations sur la cybersécurité dans le secteur de l'énergie[39]. Celui-ci insiste sur les défis sécuritaires spécifiques du secteur énergétique et si les recommandations sont détaillées en fonction de ceux-ci, elles ont pour point commun de défendre une articulation multi-sectorielle et multi-scalaire. Elles énoncent ainsi la nécessité de prendre en compte à la fois les normes internationales en matière de cybersécurité et celles techniques spécifiques au secteur et incitent les États-membres à identifier et évaluer lors de leur application l'intensité de leurs interdépendances. Dans chaque cas, le rapport insiste sur la bonne communication qui doit exister entre les États-membres par le biais de la Commission européenne.

Néanmoins, la menace cyber dans le secteur de l'énergie, au même titre que la protection générale du réseau, est subordonnée à échelle européenne aux priorités que sont le marché commun de l'énergie et la transition énergétique. En ce sens, l'UE se repose sur un ensemble d'institutions, de centres de formation et de publication qui soutiennent une approche doctrinale et prospective de la cybersécurité, plus préventive qu'opérationnelle[40]. C'est par exemple le rôle de l'ENISA ou encore de l'Institut européen pour les études de sécurité, qui vont mettre à disposition une veille stratégique et des analyses, à destination de la Commission et des États-membres, dans le but de soutenir leurs initiatives nationales.

Cette séparation structurelle entre la gestion de la menace physique et de la menace cyber pour les infrastructures critiques est un des éléments caractéristiques de l'architecture institutionnelle européenne de protection des réseaux énergétiques[41]. En ce sens, elle s'oppose à l'approche nord-américaine qui cherche d'abord à protéger le réseau avant d'identifier la nature de l'attaque. Cette dernière intègre les différents acteurs et favorise leur communication au niveau fédéral et national avec des exercices de simulation, les *GridEx*, qui combinent des attaques cyber et physiques[42]. En outre, à l'intérieur de cette distinction, la menace cyber pour

[38] Journal officiel de l'Union européenne, « Recommandation (UE) 2019/553 de la Commission du 3 avril 2019 relative à la cybersécurité dans le secteur de l'énergie », *Commission européenne,* consulté le 25 mai 2021
[39] *Ibid.*
[40] Morgan Jouy, « Une cyberdéfense collective en Europe ? L'articulation entre cyberdéfense européenne et transatlantique », *IRSEM*, note de recherche n°83, 23 octobre 2019
[41] Angélique Palle, « Vulnérabilité et protection des réseaux électriques : approches comparées Union européenne – Etats-Unis », *IRSEM*, note de recherche N°62, 28 septembre 2018
[42] *Ibid.*

le secteur énergétique est diluée dans une approche plus globale d'analyse de la cybersécurité, ce qui limite les initiatives sectorielles pour y répondre.

Cybersécurité européenne : une approche globale et un enjeu de coopération

Ces différences expliquent en partie les difficultés mais aussi l'intérêt d'une coopération soutenue entre l'UE et l'OTAN sur la question de la cybersécurité et de la cyberdéfense. En effet, l'OTAN, organisation de sécurité et de défense collective, intègre l'enjeu cyber dans une logique de défense des intérêts régionaux de ses États-membres. En 2008, après l'attaque cyber subie par l'Estonie en 2007, l'OTAN publie sa première *Cyber Defense Policy* et au sommet de Varsovie en 2016, elle reconnaît le cyberespace comme un domaine d'opération dans lequel l'organisation doit savoir se défendre. Elle confirme ainsi que son article 5 sur la défense collective peut être invoqué dans le cadre d'une attaque cyber[43]. La cyberdéfense est ainsi considérée comme un défi de sécurité émergent, au même titre que le terrorisme ou l'insécurité énergétique. L'OTAN possède également un centre d'excellence pour la cyberdéfense à Tallin qui, contrairement aux formats européens, forme spécifiquement les personnels sur la cyberdéfense et elle cherche en outre à développer une approche opérationnelle de la gestion du risque en créant en 2018 le centre opérationnel cyber. Intégré comme structure de son commandement renforcé, il a pour but de centraliser les capacités mises à disposition par les États-membres pour répondre conjointement à un incident cyber et devrait être pleinement opérationnel en 2023. Enfin, l'OTAN met également en place un exercice cyber grandeur nature, le *Cyber Coalition*, au sein de son cyberpolygone à Tartu[44].

Bien que leurs approches et leurs moyens soient différents, la menace cyber constitue l'un des sept domaines de coopération renforcée entre l'UE et l'OTAN depuis 2016. Cette coopération soutient l'échange d'informations, de bonnes pratiques, de formations et d'exercices conjoints dans un objectif d'interopérabilité des forces des États-membres. Dans cette répartition, chacun est fidèle à son identité. L'UE possède des atouts dans l'élaboration de normes communes, d'éléments doctrinaux et d'analyses prospectives sur la cybersécurité tandis que l'OTAN défend une approche plus opérationnelle liée à la cyberdéfense. Malgré des

[43] Morgan Jouy, « Une cyberdéfense collective en Europe ? L'articulation entre cyberdéfense européenne et transatlantique », *IRSEM*, note de recherche n°83, 23 octobre 2019
[44] *Ibid.*

redondances et parfois des difficultés de communication, exacerbées dans les deux instances par les intérêts nationaux des États-membres qui les composent, cette coopération favorise un traitement dynamique des enjeux cyber, par exemple en stimulant les interactions avec le secteur privé[45]. Cette coopération est nécessaire pour l'UE, puisque l'OTAN possède des moyens plus importants et qu'elle l'incite à produire des standards sur les enjeux cyber en coopération avec des États qui sont hors de ses frontières. Cette dimension est particulièrement importante, puisque le réseau électrique européen est interdépendant avec des États qui se trouvent hors UE, par exemple la Suisse, la Norvège, la Serbie, la Bosnie-Herzégovine, le Kosovo, le Monténégro ou encore la Macédoine[46].

[45] *Ibid.*

[46] Angélique Palle, « Power networks as targets : hazards, vulnerabilities and protection of electricity networks from the Second World War to 21th Century asymmetric conflicts », *Flux*, 2019/4 n°118, pp. 46-58, Université Gustave Eiffel

CONCLUSION

Le réseau énergétique européen entre dans la définition d'infrastructure critique européenne, puisque son endommagement aurait des conséquences économiques, politiques et sociétales sur plusieurs États-membres et à diverses échelles. Historiquement considérées comme des cibles stratégiques, la digitalisation croissante de la gestion des infrastructures électriques, au service d'une plus grande efficacité économique et énergétique, les rend aujourd'hui plus vulnérables aux nouvelles menaces cyber. Ainsi, si depuis 2015 aucune attaque d'ampleur sur le réseau européen n'a été à déplorer, la force du black-out vénézuélien de 2019 rappelle la vulnérabilité des sociétés face à une panne généralisée du réseau électrique.

À échelle européenne, la prise de conscience de l'interdépendance et donc de la vulnérabilité des États-membres liée à la production et la distribution d'électricité est allée croissante depuis les années 2000, marquées par la panne de 2006 en Allemagne et l'attaque cyber de 2015 en Ukraine. Initialement à charge des États-membres, qui eux-même se reposent sur leurs gestionnaires réseaux nationaux, la sécurité des infrastructures énergétiques apparaît de plus en plus comme un élément à prendre en compte par l'UE, qui la considère cependant plutôt comme une composante de son programme de sécurité de l'approvisionnement que comme un élément spécifique.

Cette approche semble expliquer en partie pourquoi la protection des infrastructures critiques européennes demeure un élément avant tout sectoriel, pris en charge par les gestionnaires réseaux nationaux, coordonnés à échelle européenne ou par le prisme de la recherche scientifique. Elle semble également justifier la séparation européenne de la gestion de la menace physique et de la menace cyber. Cette dernière est de surcroît diluée dans la large définition de l'UE de la cybersécurité, qui se positionne avant tout d'un point de vue doctrinal plutôt qu'opérationnel sur le sujet. En ce sens, sa coopération avec des organisations ayant un point de vue davantage lié à la défense des intérêts régionaux et plus de ressources humaines, financières et opérationnelles, comme l'OTAN, peut être un élément moteur pour forcer une coopération entre différents acteurs et secteurs sur la cyberdéfense. Néanmoins, elle illustre aussi une des caractéristiques du paysage institutionnel européen, qu'est la multiplication

d'initiatives à différentes échelles sans la mise en place d'une vision intégrée du problème[47] et au-delà, sa dépendance aux États-Unis lorsqu'il s'agit de sécurité et de défense régionales.

Néanmoins, si le soutien au marché de l'énergie et à la transition énergétique est un objectif qui consolide ces interdépendances entre les États du réseau et ouvre le champ des vulnérabilités en recourant davantage aux nouvelles technologies, il représente également des atouts. Une vision plus intégrée du sujet permettrait à l'UE de se reposer sur le dynamisme de ses acteurs industriels et scientifiques pour inciter les États-membres à mieux se coordonner et répondre à ses objectifs écologiques et économiques sans délaisser les impératifs sécuritaires. En ce sens, l'UE semblerait gagner à concentrer ses efforts de coordination au sein d'une agence qui aurait une vision multi-sectorielle et transfrontalière du sujet. De même, aussi bien au niveau européen qu'au sein de ses États-membres, la question d'une meilleure articulation entre les acteurs privés et publics pour créer des synergies au service du développement du secteur est également un élément clé. Cette intégration nécessiterait enfin la prise en compte globale des risques, qu'ils soient physiques, cyber ou des aléas naturels. Elle pourrait également reposer sur des exercices conjoints de mise en situation pour favoriser l'interopérabilité et la communication entre les différents acteurs, selon une approche inspirée de celle des États-Unis, qui devrait toutefois être adaptée à la spécificité et la complexité de l'architecture européenne.

[47] Angélique Palle, « Power networks as targets: hazards, vulnerabilities and protection of electricity networks from the Second World War to 21th Century asymmetric conflicts », *Flux*, 2019/4 n°118, pp. 46-58, Université Gustave Eiffel