La cybersécurité des infrastructures énergétiques

Nicolas Mazzucchi*

@ 79012

Mots-clés : risques, enjeux, géopolitique, règlementation, technologies

La numérisation croissante du secteur de l'énergie, tout au long de la chaîne de valeur, ouvre de nouvelles menaces en termes cyber. La volonté d'un certain nombre d'acteurs malveillants de viser spécifiquement des infrastructures énergétiques induit la nécessité d'appréhender de manière spécifique la cybersécurité du secteur. Entre enjeux technologiques, humains et règlementaires, la cybersécurité du secteur de l'énergie doit être abordée de manière multidimensionnelle, au risque sinon de faire face à des attaques aux effets potentiellement catastrophiques.

La numérisation croissante du secteur de l'énergie, en lien en particulier avec l'électrification mondiale et la transition énergétique, oblige à appréhender certains enjeux sécuritaires de manière différente. Au premier rang de ceux-ci, la cybersécurité apparaît comme une nécessité absolue afin de garantir à la fois la continuité du service, mais aussi d'éviter des effets cascade qui, dans des cas particuliers comme celui des installations classées Seveso, pourraient engendrer des dommages allant bien au-delà du seul domaine numérique. Le risque est ainsi non nul de voir des cyberattaques engendrer des répercussions physiques, rendant la cyberprotection indispensable. Des cas emblématiques comme Stuxnet en 2010 ont démontré que les infrastructures énergétiques pouvaient être vulnérables aux actions cyber. Identiquement, la persistance d'une cybercriminalité toujours plus inventive dans ses méthodes, ainsi qu'un contexte géopolitique en tension rendant sans cesse plus tentante l'action de perturbation sous le seuil du conflit armé, amènent à redoubler de vigilance en ce qui concerne la cybersécurité des installations énergétiques. Toutefois, il importe de considérer que la spécificité de la cybersécurité du secteur énergétique tient surtout aux impacts engendrés puisque, de manière générale, les attaques qui ciblent le secteur ne diffèrent en rien de celles qui cibleraient des entreprises industrielles. La spécificité de l'énergie dans le domaine de la cybersécurité tient ainsi avant tout aux effets transfrontaliers ou de cascade d'interruptions de service provoquées selon l'endroit de la chaîne de valeur qui serait ciblé.

La cybersécurité des infrastructures énergétiques concerne deux éléments distincts qui se recoupent parfois. D'une part, la cybersécurité des systèmes de traitement bureautiques (IT) des entreprises qui opèrent les infrastructures énergétiques et, d'autre part, la cybersécurité des systèmes de contrôle-commande automatisés (OT) de celles-ci. Si dans les deux cas il s'agit bien d'une approche de la sécurité des systèmes d'information (SSI), les enjeux technologiques sont radicalement différents entre IT et OT, pouvant engendrer des risques supplémentaires en cas de mauvaise prise en compte. Il s'agit donc de faire travailler ces deux éléments en bonne intelligence, y compris en considérant que le maillon

* Centre d'études stratégiques de la Marine.

le plus faible de la sécurité de l'IT, comme de celle de l'OT, est toujours le même : l'être humain.

1. Cybersécurité de l'IT et de l'OT

Avant de s'intéresser plus avant aux différents enjeux et politiques liés à la cybersécurité des infrastructures énergétiques, il importe de considérer les grands enjeux portés par la numérisation du secteur, ainsi que la définition précise des concepts considérés. La cybersécurité est avant tout un état recherché. Résultat d'une politique volontariste au sein d'une organisation, la cybersécurité vise avant tout à mettre dans un état de protection et de préparation satisfaisant l'ensemble des systèmes d'information, des plus critiques aux plus secondaires, afin de faire face à des menaces intentionnelles étatiques, activistes ou criminelles. Elle intègre un volet technique, lié à la protection à la fois du *hardware* (éléments physiques) et du *software* (éléments dématérialisés), ainsi qu'un volet humain fondé sur l'organisation interne de la gestion de la cybersécurité et sur la formation des personnels de l'entité considérée aux règles d'hygiène cyber. La cybersécurité est ainsi tout autant technique qu'humaine et la principale vulnérabilité d'un système d'information est bien souvent l'utilisateur non averti ou indolent. Elle doit donc considérer son besoin de protection suivant un modèle d'approche multicouches à trois niveaux dans lequel les menaces peuvent chercher à atteindre aussi bien les éléments physiques, logiques[1] et humains du système d'information [Huyghe, Kempf, Mazzucchi, 2017].

Outre cette vision de la cybersécurité, commune à l'ensemble des organisations quel que soit leur secteur d'activité, il est nécessaire de considérer, dans le cas d'opérateurs d'infrastructures énergétiques, la différence entre les systèmes d'informatique bureautique (IT) et ceux d'informatique industrielle (OT). En effet, si l'ensemble des entreprises a recours — de manière extensive le plus souvent — à l'informatique bureautique pour le traitement numérisé de ses activités de gestion interne ou de relations avec l'extérieur, seuls les opérateurs d'infrastructures numérisées intègrent de manière importante les enjeux de l'OT, les deux se différenciant de manière très importante dans le contexte de la cybersécurité. Les enjeux d'une compromission d'un système OT, appuyé sur des systèmes de contrôle industriels (ICS) automatisés, incluant capteurs et contrôles-commandes, peuvent se révéler d'une ampleur dramatique, s'agissant par exemple d'équipements sous pression ou de systèmes de transport de matières dangereuses, explosives ou inflammables.

La différenciation entre la cybersécurité de l'IT et celle de l'OT correspond le plus souvent à une question d'appréhension temporelle de la menace et de la protection. Si dans le domaine IT les enjeux de cybersécurité sont bien compris et, le plus souvent, relativement bien pris en compte, la question de ceux-ci pour l'OT est plus floue, d'autant que les systèmes IT et OT sont le plus souvent très différents. En effet, les obligations règlementaires d'une part, mais aussi le retour d'expérience des grandes cyberattaques d'autre part, font qu'aujourd'hui plus aucun acteur d'importance ne néglige les mesures basiques de protection de ses systèmes d'information bureautiques, à commencer par les mises à jour. Fréquentes, relativement simples à exécuter à partir d'une politique de sécurité des systèmes d'information (SSI) au niveau de l'entreprise ou de l'entité considérée, elles sont l'un des deux grands piliers de la sécurité des systèmes d'information, aux côtés de la formation des personnels. Mise à jour des logiciels, des procédures d'hygiène cyber et contrôle de la conformité cyber des partenaires, sont ainsi au cœur de cette cybersécurité de l'IT qui nécessite toutefois une attention constante à la fois à l'évolution des menaces, mais aussi à la gestion du périmètre numérique de l'entreprise, en termes de données et d'infrastructures, pour être performante.

À la fois s'agissant de l'IT et l'OT, l'évolution des usages doit être prise en compte. Le nomadisme des collaborateurs notamment, avec en corollaire la volonté pour certaines entités de disposer de systèmes de pilotage des infrastructures à distance. Ce besoin d'un accès lointain à des données ou à un ICS oblige à penser une cybersécurité plus complexe, faite de dématérialisation de réseaux et de systèmes — avec le

recours au *cloud* notamment — et donc le besoin de sécuriser des accès à partir d'un réseau numérique — internet — qui présente d'importantes failles intrinsèques. Accès nomade et sans fil, avec le recours à des protocoles comme la 5G et le wifi, entraînent forcément des évolutions dans la politique de cybersécurité d'une entité. Ce même nomadisme inclut parfois un brouillage entre privé et professionnel à la fois dans le temps et dans l'espace, avec le télétravail notamment. En termes de cybersécurité, le risque ici est avant tout l'utilisation par les personnels d'appareils non certifiés, dont le degré de protection soit trop faible. Même si certaines entreprises font le choix d'accepter cette politique dite BYOD (*bring your own device*), il s'agit là d'une multiplication dangereuse des risques cyber puisqu'une seule faille bien exploitée peut, suivant les cas, se révéler catastrophique pour l'entreprise.

2. Les risques cyber pour les infrastructures énergétiques

À un modèle en couches du cyberespace tel que mentionné — physique, logique, sémantique/informationnelle — correspond une typologie des différentes cyberagressions qui peuvent viser les organisations. La première d'entre elles et probablement la plus importante pour les acteurs énergétiques est le sabotage des SI, le but d'une cyberattaque de ce type étant d'empêcher un SI de fonctionner de manière temporaire ou définitive. Il s'agit des cyberattaques à la fois les plus fulgurantes, mais aussi les plus médiatisées. Œuvre d'acteurs étatiques agissant sous faux drapeau ou d'organisations activistes ou terroristes, ces attaques de sabotage sont souvent les plus visibles pour les organisations. Profitant des failles au sein des systèmes de l'organisation mais aussi, de plus en plus, au sein des sous-traitants et partenaires de celle-ci, suivant le modèle des attaques sur les chaînes de valeur, très en vogue depuis quelques années[2].

Le risque mafieux est particulièrement important dans le cadre d'acteurs de petite et moyenne taille, peu sensibilisés à la possibilité d'être frappés par un *ransomware*, voire échappant à certaines règlementations à cause justement de leur petite taille. Des travaux de hackers éthiques ont démontré par exemple la vulnérabilité des parcs éoliens à ce type d'attaque, avec des maliciels développés *ad hoc* pour infecter le contrôle à distance des éoliennes [Mazzucchi, 2019]. L'évolution de la criminalité organisée traditionnelle vers un panachage des activités vers la cybercriminalité alerte ainsi sur le risque de multiplication dans les années à venir de ce type d'action à l'encontre des opérateurs du secteur de l'énergie qui n'auraient pas adopté les bonnes pratiques en termes de sécurité.

Au niveau des menaces étatiques ou paraétatiques, l'abondance des risques cyber induit un panel extrêmement large d'atteintes possibles, directes ou indirectes. La plus dangereuse tient probablement aux attaques dites cyberphysiques qui verraient, au travers de la compromission d'un employé ou de l'infiltration d'un individu malintentionné, l'implantation d'un maliciel au sein d'un système OT par action physique directe, par exemple en utilisant une clé USB infectée pour mettre hors service un SI, ou pire. Cet exemple, qui pourrait sembler maximaliste, retrace l'action combinée américano-israélienne ayant permis en 2009 d'implanter le maliciel Stuxnet au sein du centre d'enrichissement de combustible nucléaire iranien de Natanz. Certes, il s'agit là d'un exemple extrême, toutefois la même mécanique peut être envisagée de manière plus légère pour l'attaque cyberphysique de champs d'éoliennes terrestres ou maritimes. En effet, en regard de la dynamique de transition énergétique qui voit la décentralisation de la production électrique, avec une réticulation plus forte des moyens au plus près des clients finaux, l'enjeu de cybersécurité, pris ici dans une approche cyberphysique, se transforme également.

Les impacts cyber peuvent aussi parfois se révéler les conséquences d'une intégration poussée des systèmes, en regard notamment de la dépendance de plus en plus grande aux technologies spatiales. Ainsi en 2022, au début de l'invasion russe de l'Ukraine, l'attaque cyber sur les stations-sol du système satellitaire KA-SAT géré par l'entreprise Viasat, touche de manière indirecte les fermes éoliennes en bloquant l'accès

aux systèmes satellitaires utilisés pour le pilotage et la surveillance des éoliennes. L'attaque est par la suite formellement attribuée à la Russie par les autorités américaines et européennes [Council of the EU, 2022]. Au total, elle aura paralysé plus de 3000 éoliennes, notamment en Allemagne, pendant plusieurs jours.

Outre les cyberattaques de sabotage, il faut mentionner les cyberattaques d'espionnage, dont le but est ici de s'introduire dans un SI — bureautique la plupart du temps — afin de dérober des données. Les entreprises les plus sensibles à ce type d'attaque sont les développeurs de solutions technologiques et notamment industrielles, en particulier dans le nucléaire civil pour le secteur de l'énergie. En 2011, Areva avait ainsi été la cible d'une telle attaque, dont le but était probablement de s'emparer de données liées à la R&D de l'entreprise, la compétition dans les technologies stratégiques les plus avancées pouvant parfois aiguiser les appétits de compétiteurs étrangers.

Enfin, les cyberattaques de subversion tendent à toucher de manière forte les entreprises de l'énergie, en particulier de l'*Oil & Gas*, en regard de la manipulation qui peut être faite d'un certain nombre de données, dans le contexte des enjeux liés à la lutte contre le changement climatique. Le vol de données via une attaque d'espionnage, suivi d'une diffusion de certaines de ces données «sélectionnées» et orientées de manière idoine sur les réseaux sociaux, peut ainsi nuire de manière extrêmement forte à une entreprise, en décrédibilisant sa stratégie ou ses dirigeants, ainsi qu'en semant dans l'opinion publique le soupçon d'un comportement non vertueux vis-à-vis de l'environnement ou des populations locales des pays dans lesquels elle opère. De nombreuses entreprises françaises ont depuis plus d'une décennie été victimes de ce type de guerre de l'information qui trouve une efficacité renforcée à l'heure du web 2.0 et de l'abolition de la barrière entre producteurs et consommateurs d'informations. Le *name and shame* en ligne risquant d'induire de fortes pertes économiques pour les acteurs de l'énergie, il importe de considérer ces potentielles atteintes à l'image en ligne comme faisant partiellement partie du périmètre de leur cybersécurité, étant donné que les stratégies mises en œuvre par des acteurs malintentionnés utilisent le plus souvent le canal numérique à cette fin.

Toutefois, face à la multiplication des menaces, les règlementations nationales et supranationales évoluent de manière relativement réactive, induisant des obligations toujours plus importantes pour les acteurs jugés comme critiques pour les États et leurs économies. L'Union européenne, notamment, a été pionnière dans ce domaine, en se fondant sur l'exemple français.

3. L'évolution de la règlementation européenne sur les infrastructures critiques

L'enjeu de la règlementation, prise dans le sens d'une imposition des règles de sécurité par la puissance publique, est au cœur de la cybersécurité, car celle-ci tend à être considérée avant tout comme une structure de coût par les acteurs économiques. À cet égard, il importe de considérer l'importance des travaux conduits en Europe, aussi bien par les États membres qu'à l'échelon communautaire. L'Union européenne a ainsi été la première grande entité supranationale à mettre en œuvre une règlementation contraignante de haut niveau, visant en particulier les opérateurs jugés comme vitaux. Ce corpus règlementaire tend ainsi à évoluer de manière assez constante, avec des avancées nettes. Deux étapes majeures peuvent être soulignées, avec la définition puis l'entrée en vigueur, d'une part, de la directive NIS (*Network and Information Security*) en 2018 puis, d'autre part, des directives NIS 2 et CER (*Critical Entities Resilience*) en 2022. Ces grands textes ne sont bien entendu pas les seuls éléments de règlementation s'intéressant aux questions de cybersécurité des infrastructures énergétiques, mais ce sont eux qui dessinent les grandes orientations ainsi que les principales obligations auxquelles sont astreints les opérateurs énergétiques.

La directive NIS a été, lors de son entrée en vigueur en 2018, le premier grand texte de cybersécurité des infrastructures critiques à portée transnationale disposant d'un volet de contrainte règlementaire. En érigeant les opérateurs d'un

certain nombre de secteurs considérés comme indispensables au fonctionnement des sociétés comme «opérateurs d'importance vitale» (OIV), NIS offrait la possibilité aux régulateurs dans le domaine de la cybersécurité — l'Agence nationale de la sécurité des systèmes d'information (ANSSI) en France par exemple — d'imposer aux opérateurs désignés comme OIV un certain nombre de règles liées à la sécurité des systèmes d'information, aussi bien sur le volet technique que sur le domaine de l'organisation et de la formation. Cet enjeu des OIV qui, en France, préexiste à la directive NIS, ne concerne bien entendu pas que les risques cyber. D'ailleurs, NIS 2 — fonctionnant avec son pendant CER pour la résilience en dehors des atteintes cyber — a permis d'approfondir cette approche, en élargissant d'une part le nombre d'acteurs concernés par les obligations, mais aussi d'autre part en créant une nouvelle catégorie pour les acteurs considérés comme critiques au niveau transnational. NIS 2 permet donc de mieux aborder la question des infrastructures transfrontalières, pipelines et lignes électriques en particulier.

Ces règlementations, qui pourraient sembler très contraignantes pour les opérateurs, en les positionnant sous la supervision d'un régulateur supplémentaire, sont en réalité essentielles pour éviter les interruptions dans le service, lesquelles peuvent avoir des conséquences extrêmement importantes. Ainsi, au contraire de l'Union européenne, les États-Unis ont fait le choix d'un modèle de cybersécurité très libéralisé, dans lequel l'État fédéral — au travers du Department of Homeland Security — ne dispose que d'un poids mineur dans sa capacité de régulation. Au titre des règlementations fédérales liées aux opérateurs, ce sont les États fédérés qui font le choix de durcir les normes fédérales ainsi que les entreprises qui sont libres d'appliquer des politiques SSI plus fortes que ne leur prescrit la loi. Le résultat — étant donné que la cybersécurité est souvent vue comme un facteur de coût négatif pour la compétitivité — est un niveau tendanciellement bien plus faible de cybersécurité aux États-Unis qu'il ne l'est en Europe. L'exemple le plus criant des risques induits par cette approche exclusivement libérale est l'attaque sur l'entreprise Colonial Pipeline en 2021 qui a conduit à une quasi-paralysie du secteur du transport aérien sur la côte Est des États-Unis pendant plusieurs jours. En effet, en s'attaquant à l'IT d'une infrastructure aussi critique que ce réseau d'oléoducs, il a été possible aux pirates de paralyser la distribution, en bloquant notamment l'accès aux fichiers de gestion des livraisons et de la facturation. L'analyse *a posteriori* de l'attaque révèle, comme souvent, une disproportion entre le niveau de sophistication technique de l'agression et les effets observés, signe d'une mauvaise appréhension du risque cyber. Même si le Department of Homeland Security alertait depuis plusieurs années sur ces enjeux, la question éminemment politique sous-jacente de la «liberté des États» a eu tendance à ralentir le processus de prise en compte, celui-ci n'étant à l'heure actuelle toujours principalement traité que par les entreprises et non par l'administration.

Conclusion

L'exposition des entreprises du secteur de l'énergie aux cybermenaces n'a jamais été aussi grande. Certes, la prise en compte progressive de la part des grands et des moyens acteurs du domaine en particulier, de la criticité de leur périmètre numérique, a permis de réduire cette vulnérabilité par la mise en place de politiques SSI efficaces. Identiquement, les règlementations nationales et supranationales — au plan européen en tout cas — ont permis là aussi de renforcer les interactions entre les entreprises et les administrations afin d'offrir le meilleur niveau de cybersécurité possible. La tendance semble donc positive de prime abord.

Toutefois, cette prise de conscience et ces avancées en termes de SSI ne doivent pas cacher plusieurs phénomènes inquiétants pour les entreprises de taille locale et nationale aussi bien que pour les grandes transnationales. D'une part, l'écart tend à se creuser entre les règlementations des pays ou des régions du monde qui ont décidé de considérer le problème de manière volontariste et les autres. Alors que la numérisation ne cesse de progresser et que l'interconnexion entre les SI des entreprises — à la fois les différentes filiales

des transnationales au plan horizontal, mais aussi entre les entreprises et leurs sous-traitants au plan vertical — se développe identiquement, la surface d'exposition connaît elle aussi un développement exponentiel. Avec une différenciation des règles de SSI au plan national et la facilité d'attaquer un SI depuis n'importe où sur la planète, il devient aisé de choisir le point le plus faible. D'autre part, les règles liées à la cybersécurité — y compris au plan européen — tendent à «oublier» certains acteurs, dont la taille est considérée comme trop petite pour justifier une inclusion sur la liste des OIV. Or, à l'heure de la transition énergétique et prenant en compte la décentralisation des moyens de production et de transmission électrique, même des acteurs de petite taille deviennent stratégiques en termes d'équilibrage de l'ensemble du système et une atteinte à une poignée d'entre eux peut potentiellement entraîner des effets de cascade, en provoquant un blackout sur tout ou partie d'un réseau par exemple.

De fait, de nombreux chantiers demeurent ouverts, à une époque où l'exposition au risque numérique — surtout de manière indirecte comme l'a démontré l'attaque sur Viasat — n'a jamais été aussi forte. La maîtrise du risque cyber, en regard de ses impacts potentiels, doit ainsi tendre vers la valorisation de la SSI comme une compétence-clé de l'entreprise, alors qu'elle est surtout perçue aujourd'hui comme un centre de coût. Le risque réputationnel cyber, en regard notamment des attaques de subversion, pourrait bien entraîner à l'avenir une nouvelle forme de classification-valorisation des entreprises, à l'image de ce qui s'est passé dans les années 2010 avec les critères ESG ; malheur dans ce cas à ceux qui n'auraient pas anticipé ce tournant.

Notes

1. La couche logique comprend les logiciels (permettant d'établir une discussion homme-machine) et les protocoles (discussion machine-machine).

2. L'exemple type est l'attaque d'un sous-traitant permettant de s'infiltrer dans le SI de l'entreprise visée, par exemple en utilisant des failles dans la sécurité des clés-token de connexion à distance.

Références

Council of the EU, 2022. Russian cyber operations against Ukraine: Declaration by the High Representative on behalf of the European Union, Press release, https://www.consilium.europa.eu/en/press/press-releases/2022/05/10/russian-cyber-operations-against-ukraine-declaration-by-the-high-representative-on-behalf-of-the-european-union/.

Huyghe F.-B., Kempf O., Mazzucchi N., 2017. *Gagner les cyberconflits*, Paris, Economica.

Mazzucchi N., 2019. "Renewable Energy Infrastructure: Physical and Cyber Vulnerabilities Assessment", *Energy Security: Operational Highlights*, n° 12, Vilnius, ENSEC COE, pp. 32-40.

Biographie

Nicolas Mazzucchi est directeur de recherche au Centre d'études stratégiques de la Marine. Docteur en géographie économique, il est spécialiste des questions énergétiques, de matières premières, de cyber et de stratégie navale. Il est l'auteur de plusieurs ouvrages dont *Gagner les cyberconflits* (avec F.-B. Huyghe et O. Kempf), notamment sur le croisement énergie-numérique.

À lire également dans *La Revue de l'Énergie*

- Actes du 9e Forum Européen de l'Énergie – La sécurité énergétique : un enjeu d'une étonnante modernité *(n° 664, septembre-octobre 2022)*
- Les dimensions géopolitiques de la relance de l'énergie nucléaire, *Teva Meyer (n° 668, septembre-octobre 2023)*

À retrouver sur **www.larevuedelenergie.com**.