Observatoire de l'Industrie Electrique
www.observatoire-electricite.fr

Novembre 2017

Note de conjoncture

# LA CYBER RESILIENCE DES SYSTEMES ELECTRIQUES

Depuis plusieurs années, l'actualité nous fournit des exemples de cyberattaques qui touchent les infrastructures énergétiques, souvent dans les zones de conflit (Ukraine), mais pas uniquement (Etats-Unis par exemple). Les systèmes électriques sont de plus en plus les cibles d'actions cybernétiques malveillantes. L'OIE présente les origines de ces attaques, leurs enjeux pour les systèmes électriques, ainsi que les réponses apportées par l'industrie électrique et les pouvoirs publics nationaux et européens.

# Points clés

· Les systèmes énergétiques sont des actifs stratégiques majeurs et font l'objet d'un nombre croissant de cyberattaques : plus de 20 cyberattaques de grande ampleur ont concerné des systèmes énergétiques dans le monde depuis 1982, avec une accélération du rythme depuis 2010.

• Les cyberattaques ont essentiellement des origines externes aux installations (le sabotage interne est rare) et peuvent découler de motivations politiques et géopolitiques, financières ou de notoriété.

• Le développement des applications numériques et des objets connectés génère de nouveaux flux d'informations dans les systèmes électriques. Ces flux de communication représentent des enjeux supplémentaires en termes de résilience des systèmes électriques.

• La cybersécurité des infrastructures énergétiques relève désormais de la compétence militaire dans plusieurs pays. Ainsi, aux Etats-Unis, la cyber résilience de l'industrie électrique relève de la compétence du Secretary of Defense (et non de l'Energie), tandis qu'en France la protection des installations électriques est régie par la Loi de Programmation Militaire de 2013.

• La cybersécurité recouvre des enjeux régaliens et industriels, et nécessite une bonne coopération entre les acteurs. La résilience du système électrique français dépend ainsi à fois des réponses mises en œuvre au niveau national, européen et de l'OTAN.

# LES ORIGINES DE LA CYBERCRIMINALITÉ

Si la première attaque informatique de grande ampleur remonte aux années 1980 avec l'explosion d'un gazoduc en Sibérie, la cybersécurité est un sujet qui n'occupe que depuis peu l'espace public. La dernière cyberattaque de grande ampleur, connue sous *Wannacry*[1], a particulièrement frappé les esprits et révélé à la fois le danger majeur que constitue la cybercriminalité et le degré d'impréparation du système informatique mondial face à cette menace. Ce *ransomware*, en attaquant plus de 200 000 ordinateurs à travers 150 pays, avait pour but d'extorquer une rançon aux utilisateurs. De surcroît, cette attaque a permis d'en masquer une autre, baptisée *Adylkuzz*, qui a concerné des centaines de milliers d'ordinateurs[2].

Avant d'en arriver à un tel stade, le développement de la cybercriminalité s'est réalisé en parallèle à celui d'internet. Il a été reconnu officiellement pour la première fois en 1996 lors d'une réunion du G8 à Lyon, avec la décision de créer un sous-groupe d'experts pour étudier les nouveaux types de criminalité se propageant sur internet.

D'une certaine façon, la méthodologie utilisée par les cybercriminels est issue de l'action de *hackers* qui détectaient les failles de sécurité des systèmes informatiques et les signalaient. Cette activité existe d'ailleurs toujours et elle a été officialisée économiquement sous le terme de « *Bug Bounty* »[3].

Ces compétences ont pour partie progressivement évolué vers une réelle action criminelle présentant plusieurs formes :

- l'escroquerie ou le non-respect du copyright (plateforme de téléchargement illégale),
- le piratage ou l'espionnage de systèmes informatiques,
- Plus récemment, une nouvelle criminalité visant à porter atteinte à l'identité numérique a commencé à émerger.

Comme le fait remarquer Guillaume Poupard, Directeur Général de l'ANSSI[4], « *s'il faut bien distinguer entre la propagande et les attaques informatiques… On ne peut écarter l'hypothèse selon laquelle des gens préparent les conflits du futur, et par moment, procèdent à des tests* ». Le stade auquel nous nous trouvons nécessite plus que jamais des mesures de cybersécurité pour maintenir le haut niveau de résilience des systèmes électriques.

# L'HISTORIQUE DES CYBERATTAQUES SUR LES SYSTEMES ENERGETIQUES

Depuis 1982[5], 20 cyberattaques majeures ont impacté des éléments du système énergétique mondial. Les plus abouties ont frappé spécifiquement les systèmes électriques : il s'agit de Stuxnet[6] en 2010 (dommages majeurs infligés à une usine d'enrichissement d'uranium en Iran) et de Black Energy en 2015 (déconnexion d'une partie du réseau électrique ukrainien suivi d'un fonctionnement en mode dégradé pendant plusieurs semaines).

La découverte de Stuxnet a provoqué un premier choc en révélant à la fois des vulnérabilités inconnues dans l'industrie énergétique mais aussi et surtout la dimension politique et non plus simplement financière des attaques.

Selon Symantec[7], l'ensemble des attaques sur les systèmes énergétiques a augmenté de 380 % entre 2014 et 2015. Ainsi, plus de 80 % des compagnies pétrolières et gazières ont enregistré une hausse du nombre de cyberattaques réussies en 2015, et ces industries pourraient être amenées à dépenser près de 2 Mds$ par an d'ici 2018 pour s'en protéger.
Les attaques peuvent se classer en trois grandes catégories :

- celles qui visent à interrompre la disponibilité d'un service ou d'un système ;
- les attaques de confidentialité qui ont pour but d'exfiltrer des informations ou de surveiller une activité, souvent à des fins lucratives ;
- les attaques sur l'intégrité d'un système, visant à altérer des informations ou des processus.

Sur les 25 dernières années, les principales cyber-attaques concernant le secteur électrique ont été les suivantes :

| Année | Pays | Nom de l'attaque | Objectif | Origine |
|---|---|---|---|---|
| 1992 | Lituanie | - | Sabotage | Interne |
| 2003 | USA | Slammer | Inconnu | Externe |
| 2010 | Iran | Stuxnet | Sabotage | Externe |
| 2011 | Monde | Night Dragon | Espionnage | Externe |
| 2014 | Monde | Energetic Bear | Espionnage | Externe |
| 2014 | Corée du Sud | - | Chantage | Externe |
| 2015 | Ukraine | Black Energy | Sabotage | Externe |
| 2016 | Ukraine | Industroyer | Sabotage | Externe |

Cet inventaire[8] révèle deux éléments d'intérêt. Tout d'abord, la dernière attaque connue d'une installation par voie interne remonte à 1992.
Depuis, toutes les attaques ont été basées sur des virus ou sur des vers électroniques introduits depuis l'extérieur.
Ensuite, l'accélération de la fréquence des attaques de grande ampleur démontre l'enjeu croissant de la cybersécurité.

1. Ce virus qui porte le nom de WanaCryptOr 2.0 s'est attaqué aussi bien aux hôpitaux britanniques, qu'à Renault ou au système bancaire russe. Il a exploité une faille dans les systèmes Windows XP qui a été divulguée à la suite du piratage de documents appartenant à la NSA. Celle-ci se servait elle-même de la faille pour procéder à des opérations de hacking.
2. Adylkuzz était un crypto-mineur qui a réalisé des transferts de monnaie à l'insu des propriétaires des ordinateurs.
3. Un *bug bounty* est une récompense attribuée par un site web ou un développeur de logiciels.
4. Agence Nationale de Sécurité des Systèmes d'Information.
5. Le premier acte majeur d'attaque informatique a été commis en 1982 en Sibérie et il conduit à l'explosion d'un gazoduc.
6. Une variante de Stuxnet, apparue en 2014 sous le nom d'Energetic Bear, a déstabilisé 250 entreprises énergétiques américaines et européennes par contagion successive à partir de l'infestation de 3 sites de contrôle industriel.
7. Symantec, Internet Security Threat Report, 2016.
8. Voir étude IFRI de Gabrielle Desarnaud : Cyberattaques et systèmes énergétiques / Faire face au risque, 2017.

# LES BUTS DE CES CYBERATTAQUES

Les motivations des cyberattaques sont très variées, mais elles peuvent être regroupées en différentes catégories :

• le sabotage militaire ou terroriste sur la base de facteurs politiques et géopolitiques,

• l'espionnage, vol de données, chantage, demande de rançon… pour des motivations financières ou économiques,

• le test de méthodes ou l'action de notoriété

Dans certains cas, comme Wannacry, la motivation a pu sembler floue et ne pas reposer uniquement sur l'extorsion mais aussi sur la recherche de notoriété.

L'année 2017 est en train de marquer un tournant dans la cybercriminalité, le champ des attaques se déplaçant vers le sabotage des systèmes industriels, des systèmes d'importance vitale, des systèmes de transport et des systèmes énergétiques, soit dans le cadre de conflits entre Etats, soit dans le cadre d'actions terroristes. La cyberdéfense et la cyberattaque s'imposent progressivement comme de nouvelles armes stratégiques visant tout particulièrement le fonctionnement des Etats.

# DES SYSTEMES ELECTRIQUES DE PLUS EN PLUS VISES

Selon le World Energy Council, les infrastructures énergétiques sont particulièrement à risque en raison de leur rôle central dans le fonctionnement de l'économie et de la possibilité pour les cybersaboteurs d'y causer des dommages physiques.

Ainsi, en 2014, les USA ont recensé 245 attaques de sites industriels dont une grande majorité dans le secteur énergétique. Une bonne moitié d'entre elles peuvent être considérées comme des menaces persistantes avancées (*Advanced Persistant Threat*). Celles-ci ne sont découvertes en moyenne que plus de 200 jours après l'infiltration[9].

Concernant les systèmes électriques, leur âge peut être un facteur de vulnérabilité. D'une durée de vie très longue (certains actifs ont des durées de vie supérieures à 50 ans), leur technologie est décalée par rapport aux applications numériques. D'autre part, les systèmes électriques utilisent souvent des systèmes d'exploitation clés en main, disponibles sur le marché, et donc bien connus des attaquants potentiels. De plus, comme dans d'autres domaines, l'origine de failles résulte souvent de l'erreur humaine (manque de formation aux risques de l'usage des objets connectés, non renouvellement des mots de passe, manque de systèmes performants d'identification à distance…).

Pour répondre à ce type de menace, l'industrie électrique applique à ses actifs les principes de la sureté nucléaire, à savoir la défense en profondeur et la diversification. Dans les centrales, les différents réseaux informatiques sont séparés les uns des autres et les systèmes de contrôle commande des réacteurs ne sont pas accessibles par internet.

S'agissant des réseaux électriques, les systèmes de contrôle et de commande régionaux ou nationaux peuvent être spécifiquement visés. Le Department of Energy, dans un récent rapport[10], a précisé que, « *dans l'environnement actuel, les réseaux américains risquaient d'être confrontés de façon imminente à des cyberattaques* ». Ainsi, en 2016, des pirates russes sont parvenus à infester un équipement de Burlington Electric (Vermont). Utilisant Grizzly Steppe[11], l'attaque a été sans conséquence mais son objectif était probablement de servir de test de vulnérabilité pour une opération ultérieure.

Le développement des bâtiments et des objets connectés constitue également une source croissante de vulnérabilité, le principal danger à ce niveau étant l'invalidation des sources, qui rend les objets connectés inopérants ou qui coupe les accès du gestionnaire au pilotage des systèmes.

Les risques d'attaques sont devenus tellement importants que la stratégie de protection relève maintenant aux USA du *Secretary of Defense* et non plus de l'énergie. En France, les Systèmes d'Information d'Importance Vitale (SIIV) des réseaux électriques ou des centrales font l'objet de mesures de protection imposées par la LPM (Loi de Programmation Militaire, 2013). Ces dispositions révèlent que la qualification générique de la cyberattaque relève de la « guerre » et non d'actes de droit commun.

# UNE MENACE QUI EVOLUE

Malgré toutes les mesures de protection envisagées, la sécurisation totale des installations électriques est impossible, tout comme la prévention d'actes de sabotage physiques par des personnes très motivées et compétentes, pendant que le développement permanent de nouvelles fonctionnalités par les TIC est porteur en parallèle de l'apparition de nouvelles failles potentielles.

Par exemple, il s'avère que le logiciel utilisé dans l'attaque de décembre 2016 contre l'Ukraine[12] a été spécialement conçu pour s'attaquer aux réseaux électriques. Appelée « Industroyer » ou « Crashoverride » par les experts, cette menace[13] a pour cible principale les disjoncteurs. La logique d'attaque sur

9. Mandiant, M-Trends 2015 : A view from the front lines, 2015.
10. Department of Energy, Quadrennial Energy Review (QER) 2017, 2017.
11. Virus utilisé pour infiltrer les opérations électorales américaines de 2016.
12. Cette attaque, qui a privé Kiev d'électricité pendant une heure, aurait utilisé une partie d'Industroyer, et pourrait avoir un lien avec le russe Sandworm utilisé en 2015 également contre l'Ukraine. Washington Post, Russia has developed a cyberweapon that can disrupt power grids, according to new research, 2017.
13. Le terme menace correspond à un processus d'attaque beaucoup plus sophistiqué qu'un simple virus dont la propagation est assez restrictive. Ce malware a été conçu pour cartographier le réseau informatique interne d'une station électrique et le rendre inopérant sans intervention humaine. En ce sens, il est assez proche de Stuxnet.

les SCADA[14] repose sur le fait qu'ils n'ont pas été conçus pour être connectés entre eux. Très évoluée dans ses capacités à s'introduire dans les systèmes, à y rester et à y agir, cette menace pourrait aboutir à des coupures de réseau de plusieurs heures, voire de plusieurs jours en cas d'attaque multisites. Elle est également susceptible de détériorer physiquement une centrale[15]. Si son utilisation en 2016 doit être considérée plutôt comme un simple test, la conception de cette menace a clairement nécessité une expertise et une connaissance très fines du fonctionnement des systèmes électriques.

# LE PROBLEME DE LA TRANSMISSION DES DONNEES

L'industrie énergétique, et en particulier le secteur électrique, met en œuvre un changement profond de ses modes de fonctionnement, que ce soit au niveau de l'ensemble des infrastructures technologiques ou de la relation entre les entreprises et leurs clients.

Ce changement repose sur la digitalisation de l'ensemble des processus et sur le traitement de flux de données de plus en plus massifs, qualifiés encore de data management. La réversibilité des flux (l'aval compteur pouvant maintenant émettre vers l'amont par le biais des compteurs communicants) et leur universalité (le déploiement de la norme IPv6 devant permettre dans les années à venir de connecter des milliards d'objets aux réseaux de communication), ouvrent l'ère de l'internet des objets.

Ces évolutions posent la question des modalités de transmission des données. En effet, le développement de l'internet des objets, inséparable de celui des technologies de transmission de données à très bas débit[16], permettra une connexion économiquement acceptable de plusieurs milliards d'objets aux réseaux, mais pourrait accroître la vulnérabilité des systèmes électriques.

Ces technologies sont essentielles dans la transmission des données de comptage, et elles sont portées en France par deux pépites, à savoir Sigfox (soutenue par Total, Intel et Salesforce) et la LoRaAlliance portée en particulier par Orange. Du côté allemand, une alliance Vodafone Deutschland et Deutsche Telecom s'est constituée.

La structuration de l'activité économique liée à la donnée présente un enjeu majeur pour l'activité des objets connectés. Dans ce contexte, l'ENISA[18] a publié une position commune avec l'industrie des semi-conducteurs (Infineon, NXP, SMT Microelectronics…) pour préparer une certification de l'internet des objets destinée à assurer la sécurité des objets connectés. Il y a en effet urgence sur ce sujet, considérant que le nombre d'objets connectés[19] en Europe devrait atteindre 6 milliards d'ici 2020, et que ceux-ci pourraient constituer des chevaux de Troie idéaux pour les hackers de toute nature.

S'il est encore difficile d'évaluer le niveau d'accroissement, à la fois en étendue et en impact, des risques sous-jacents à ces évolutions, nous sommes certainement entrés dans une période de grande vigilance quant à la résilience des systèmes électriques face aux différents actes de cyber malveillance envisageables.

# LES STRUCTURES DE REPONSE

La croissance des risques n'a pas laissé les responsables nationaux et supranationaux sans réaction.

Au niveau français, l'ANSSI pilote la politique française de cybersécurité.

La France a en effet adopté, à partir de la LPM (Loi de programmation militaire) de 2013, une approche réglementaire qui vise à définir les obligations qui pèsent sur les « *Opérateurs d'Importance Vitale* » (OIV) pour l'économie nationale. Dans ce groupe d'opérateurs figurent en bonne place ceux du secteur énergétique. L'approche allemande, assez similaire sur le plan des principes, se distingue par une liste d'OIV plus importante mais également par l'absence de mesures spécifiques imposées à celles-ci.

En 2016, face à l'évolution des menaces, la France a lancé une révision de sa doctrine militaire en s'appuyant sur le centre de maîtrise de l'information de la Direction Générale de l'Armement, qui dispose de moyens importants. En particulier, l'armée française disposera au total de 2 600 combattants « numériques » en 2019, regroupés dans le COMCYBER.

Au niveau de l'Union Européenne, l'ENISA exerce un rôle d'expertise sur ce sujet et un rôle de coordination en cas de crise. Par contre, elle ne possède ni la capacité de mettre en œuvre une procédure de réaction graduelle, de la détection à la réaction, ni un pouvoir d'initiative.

L'attaque Wannacry a néanmoins modifié les vues de la Commission Européenne sur le sujet. Celle-ci va tenter de renforcer la coopération entre Etats-membres via le mécanisme d'échange pour la coopération opérationnelle (Computer Security Incident Response Team Network) mis en place dans le cadre de la directive Network and Information System. Ceci implique une coopération accrue avec les autorités policières et le secteur privé[20]. Parallèlement, la DG Energie de la Commission Européenne a demandé à l'EECSP[21] de produire un rapport analysant les enjeux de cyber sécurité et les domaines stratégiques du secteur de l'énergie[22]. Enfin, le Commissaire en charge du domaine,

14. Supervisory Control and Data Acquisition, système qui contrôle de façon centralisée les équipements d'un industriel sur différents sites.
15. En empêchant les disjoncteurs de fonctionner, l'attaque pourrait générer une surchauffe destructrice des systèmes.
16. Narrow Band IoT.
17. LoRaWAN : Long Range Wide Area Networks for IoT.
18. European Network and Information Security Agency.
19. Outils personnels, équipement des foyers, smart homes, moyens de déplacement…
20. Note to the Council of the EU : Telecom 138/Cyber 86/Enfopol 280.
21. Energy Expert Cyber Security Platform.

Andrus Ansip, a déclaré avoir hâte de relancer la coordination dans ce domaine car selon lui « *aucun Etat-membre ne peut traiter ces problèmes seul* ».

Du côté des industriels, Eurelectric, dans un nouveau rapport[23] a mis en avant le besoin d'« *améliorer la cybersécurité en Europe* ». Ceci passe par la nécessité pour les opérateurs de réseaux de mettre en place une stratégie de cybersécurité bien structurée et de développer les compétences nécessaires pour éviter les pertes de données, les ruptures d'alimentation et les incursions dans la vie privée des consommateurs.

Au niveau de l'OTAN la préoccupation est également très grande. Le Supreme Allied Commander for Transformation (SAC-T) a déclaré : « *Notre contexte sécuritaire est caractérisé par sa volatilité, son imprévisibilité et surtout par sa complexité. La première question n'est donc pas de quoi avons-nous besoin, mais que voulons-nous faire ?* ». Ceci a abouti à engager une large réflexion sur la protection des infrastructures vitales pour l'Europe à la suite du sommet de Varsovie en 2016. Parmi les sept exigences retenues en matière de résilience nationale et gouvernementale figure en bonne place celle de la sécurité d'approvisionnement en énergie. Dans ce cadre, Eurelectric a été appelée par l'OTAN à apporter sa contribution à la préparation du NATO Defense Planning Process 2017.

Enfin, le G7 a mandaté son groupe de cyber-experts pour présenter à compter d'octobre 2017 « *des éléments de haut niveau et non contraignants* » permettant d'évaluer l'état de la cybersécurité[24]. Côté américain, suite à l'attaque d'hackers russes sur le Vermont, le Departement de l'Energie a mis l'accent dans son Quadrennial Energy Review sur la protection des réseaux aussi bien électriques que gaziers. Ceci devrait entraîner une réforme du Federal Power Act pour acter son importance en termes de sécurité nationale. Dans ce cadre, le Président Trump a signé le 11 mai dernier un Executive order dont le but était d'améliorer la protection des infrastructures vitales contre les cyberattaques.

# CONCLUSION

Comme l'explique le World Energy Council[25] « *les entreprises du secteur de l'énergie doivent intégrer le fait que les cyberattaques constituent aujourd'hui des menaces majeures pour les grandes infrastructures au même titre qu'une inondation, un incendie ou un cyclone* ».

Ces cyberattaques peuvent avoir des motivations différentes (financières, géopolitiques ou de réputation), ce qui démultiplie leurs origines et la complexité de la cyberdéfense. Cette hybridation des cyberattaques est à mettre au regard du développement croissant des applications numériques dans les systèmes électrique (postes intelligents, objets connectés, comptage).

De fait, la nature stratégique des systèmes électriques en font l'objet d'un nombre croissant de cyberattaques : plus de 20 cyberattaques de grande ampleur ont concerné des systèmes électriques ces dernières années.

Les industriels ont pris la mesure de la menace en investissant de plus en plus dans leurs systèmes de protection pour atteindre l'objectif de cyber résilience. La réaction industrielle à des enjeux stratégiques nationaux et internationaux doit néanmoins être accompagnée de réponses des autorités nationales et supranationales, qui doivent pouvoir évoluer au moins aussi rapidement que les menaces.

22. EECSP, Cyber Security in the Energy Sector, 20170.
23. Eurelectric, Smart Grid Cyber Security, 2017. Eurelectric est l'union professionnelle de l'industrie électrique européenne.
24. G7 Finance Ministers Meeting: Bari May 12/13 2017. Point n°14 of the final communiqué.
25. WEC, New cyber resilience report : energy sector prime target for cyber-attacks, 2016.