CHAIRE **RAOUL-DANDURAND**
EN ÉTUDES STRATÉGIQUES ET DIPLOMATIQUES
20 ANS

Le Réseau électrique intelligent :

entre sécurité énergétique et informatique

Nicolas Pellerin-Roy

Le réseau électrique intelligent :
entre sécurité énergétique et informatique

Nicolas Pellerin-Roy

ÉTUDE RAOUL-DANDURAND #31

Chaire Raoul-Dandurand en études stratégiques et diplomatiques
Université du Québec à Montréal
455, boul. René-Lévesque Est, Pavillon Hubert-Aquin
4e étage, bureau A-4410
Montréal (Québec) H2L 4Y2
chaire.strat@uqam.ca | dandurand.uqam.ca

Dépôt légal – Bibliothèque et Archives nationales du Québec
ISBN : 978-2-922844-68-9
Décembre 2015

TABLE DES MATIÈRES

Résumé

De plus en plus de pays adoptent un discours favorisant la production d'énergies renouvelables et la mise en place d'un réseau électrique rendu intelligent par l'incorporation massive des technologies de l'information et de la communication (TIC). Cette étude vise premièrement à comprendre les raisons motivant une telle mise à jour du réseau électrique et deuxièmement à comprendre quels sont les enjeux sécuritaires d'une telle informatisation, à une époque où les cyberattaques et les vols de données informatisées se font de plus en plus nombreux. De cette étude, cinq points attirent notre attention :

1. Puisque la forte demande mondiale en ressources énergétiques est difficile à combler par leur rareté, la complexité de leur production et de possibles troubles géopolitiques, le rôle grandissant des énergies renouvelables comme garantes de la sécurité énergétique de nombreux pays nécessite une mise à jour du réseau électrique en le rendant « intelligent ». Ces améliorations permettent d'optimiser et de mieux contrôler les activités du secteur de l'énergie électrique et de rendre l'approvisionnement plus stable, autant par une résilience accrue que par l'incorporation plus aisée de la production d'énergies renouvelables.
2. Si la croissance rapide de l'« Internet des objets » mise avant tout sur la convivialité et la facilité d'utilisation de ses composantes, elle se fait au détriment de leur sécurité informatique. Nécessaire, elle est néanmoins souvent mise de côté également par souci d'économie. Cela pose problème pour la sécurité informatique du réseau électrique intelligent : les TIC sont désormais reliées à des technologies opérationnelles (TO) visant plutôt à superviser et à optimiser les activités d'un réseau interne, elles n'ont donc pas été pensées afin d'entrer en communication avec le monde extérieur et contiennent très peu, voire pas du tout, de mesures de sécurité informatique.
3. Cette fusion technologique facile les intrusions dans des réseaux sensibles contrôlant des éléments dont le dysfonctionnement pourrait avoir des répercussions graves. Si des évènements tragiques ne sont toujours pas survenus, plusieurs exemples nous démontrent qu'ils demeurent dans l'ordre du possible. Si les infiltrations dans des ordinateurs gouvernementaux et de grandes entreprises, menant au vol d'informations, nous démontrent que cette pratique est simple et répandue, des opérations comme Stuxnet illustrent le fait qu'elles peuvent avoir des impacts physiques importants et dangereux.
4. Les nombreuses contraintes à ce type d'attaques (financières, matérielles, informationnelles, logistiques) limitent les acteurs pouvant les effectuer. Comme dans le cas de Stuxnet, ce sont les États qui sont les mieux outillés pour les mener à bien. Pour le moment, puisque le monde est

interdépendant, une cyberattaque massive sur les infrastructures critiques d'un autre État a peu de chance, pour le moment, de survenir. Cette retenue reste dépendante du contexte international, les armées nationales se préparant de plus en plus à ces éventualités.

5. Si les personnes responsables de la sécurité d'infrastructures critiques comme le réseau électrique intelligent sont de plus en plus conscientisées et ont davantage de moyens pour atteindre leurs objectifs de défense, elles ne peuvent pas en éradiquer la principale vulnérabilité : le facteur humain. Souvent, il suffit qu'un employé télécharge un virus camouflé en pièce jointe d'un courriel ou insère une clé USB infectée pour donner accès et mettre en péril l'entièreté d'un réseau informatique. Si l'aspect informatique de la sécurité du réseau électrique intelligent demeure un paramètre qu'il est possible de contrôler, il est par contre ardu de veiller sur le comportement et les habitudes de l'entièreté des utilisateurs d'un réseau.

AUTEUR

Nicolas Pellerin-Roy, chercheur en résidence à l'Observatoire de géopolitique , Chaire Raoul-Dandurand, et candidat à la maîtrise en science politique, Université du Québec à Montréal (UQAM).

LE RÉSEAU ÉLECTRIQUE INTELLIGENT : ENTRE SÉCURITÉ ÉNERGÉTIQUE ET INFORMATIQUE

Introduction

En 2009, pour répondre à la crise financière qui venait de frapper sévèrement les États-Unis, le président américain Barack Obama annonçait l'*American Recovery and Reinvestment Act*, un grand chantier économique visant à stimuler l'économie américaine et à aider, par des mesures fiscales, une population et un secteur industriel sévèrement touchés. Parmi les éléments clés de cette initiative se trouvait l'implantation progressive d'un *réseau électrique intelligent* à l'échelle nationale[1], appuyée par des mesures encourageant l'électrification des transports[2] et l'exploitation de sources d'énergie considérées *propres*.

Le réseau électrique intelligent (ou *smart grid*) est « un système électrique utilisant les technologies de l'information et de la communication (TIC), d'une façon bidirectionnelle et cybersécurisée, et l'intelligence computationnelle de manière intégrée au fil du parcours électrique : génération, transmission, poste électrique, distribution et consommation. Tout ceci dans le but d'obtenir un système électrique qui est

[1] C. L. Doggett. 2009. *Guide to the American Recovery and Reinvestment Act of 2009*, Congrès des États-Unis, p. 14.
[2] *Ibid.*, p. 13-14.

propre, sûr, sécuritaire, fiable, résilient, efficace et durable[3] ». Bien que l'ajout de composantes informatiques à tous les niveaux amène une efficacité et une hausse de productivité semblables à celles obtenues dans son inclusion dans d'autres secteurs industriels, il existe des spécificités à cette informatisation massive d'une des infrastructures majeures de la société.

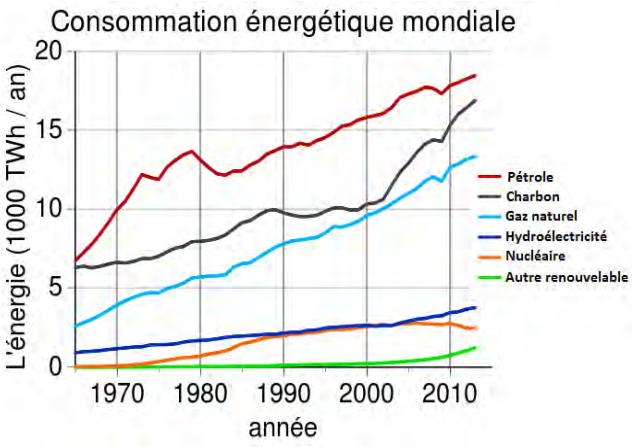
En effet, la mise en place d'un réseau électrique intelligent, visant à répondre aux besoins énergétiques du 21e siècle, a généré un bon nombre de vulnérabilités, pouvant fragiliser autant la sécurité énergétique que la sécurité informatique du réseau électrique. Il s'agit donc tout d'abord de comprendre les raisons de l'avènement, quasi inéluctable, d'un réseau électrique intelligent et informatisé pour assurer la sécurité énergétique d'une société. Ensuite, seront analysés les effets négatifs qu'entraîne cette informatisation massive du réseau électrique, et notamment les vulnérabilités pouvant rendre précaire la sécurité énergétique. Finalement, il s'agira d'évaluer la réalité des risques en remettant en perspective l'impact, les acteurs possibles et le potentiel perturbateur de cyberattaques sur des infrastructures critiques tel que le réseau électrique.

1. Le réseau électrique intelligent : la modernisation nécessaire du réseau actuel

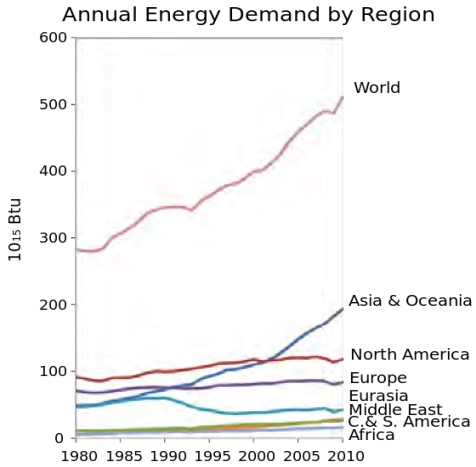
Depuis le début des années 2000, plusieurs États ont dû prendre en compte la précarité de leur *sécurité énergétique*, aspect sécuritaire visant à s'assurer l'accès à des ressources suffisantes pour subvenir aux besoins essentiels et à s'assurer de leur livraison ininterrompue, du lieu de production au consommateur[4]. Toutefois, à l'échelle planétaire, une certaine tendance se fait remarquer; la demande en énergie est en constante progression, notamment en raison de l'émergence de nouvelles puissances économiques telles la Chine et l'Inde, dont la croissance économique est très gourmande en ressources énergétiques de toutes sortes, principalement en hydrocarbures.[5]

Tandis que la demande en énergies fossiles augmente dans certaines régions du monde, l'approvisionnement devient, quant à lui, difficile, et les gisements, ardus à exploiter. Ce déséquilibre énergétique oblige donc une certaine refonte du réseau électrique actuel. De plus en plus sollicité par l'informatisation croissante de la société, il doit être prêt à gérer et à approvisionner cette demande grandissante en électricité.

[3] Hamid Gharavi et Reza Ghafurian. 2011. « Smart Grid: The Electric Energy System of the Future », *Proceedings of the IEEE*, vol. 99, no 6, p. 917.
[4] Michael T. Klare. 2012. « Energy Security », dans Paul D. Williams (éd.), *Security Studies: An Introduction*, 2e édition. Londres, New York : Routledge, p. 536-537.
[5] Daniel Yergin. 2006. « Ensuring Energy Security », *Foreign Affairs*, vol. 85, no 2, p. 71.



Source : British Petroleum. 2014. BP Statistical Review of World Energy 2014. En ligne, <https://upload.wikimedia.org/wikipedia/commons/thumb/1/13/World_energy_consumption_fr.svg/660px-World_energy_consumption_fr.svg.png>.



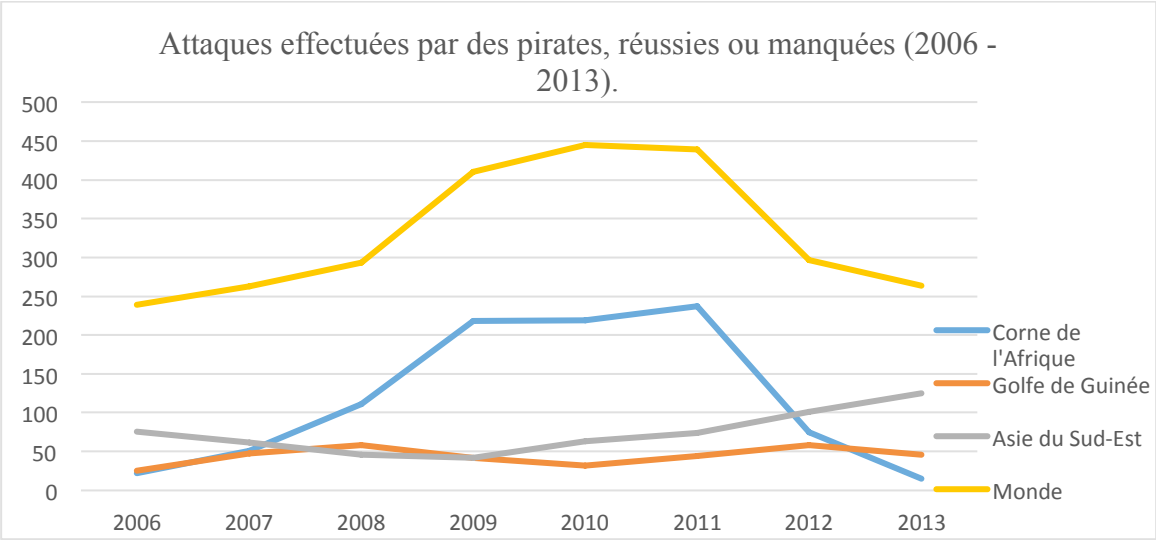
Source : Martin Kraus. 2013. Primary Energy Consumption in Quadrillion Btu from 1980 to 2010 by Region, données de la U.S. Energy Information Administration. En ligne, <https://en.wiki2.org/wiki/File:World_primary_energy_consumption_in_quadrillion_Btu_by_region_svg>

1.1 La demande énergétique en progression constante

Tandis que la demande en énergie est en progression constante, l'offre, de son côté, devient de plus en plus instable, soumise aux aléas de la nature et à des situations géopolitiques parfois difficiles[6]. Ainsi, en 2005, les ouragans *Katrina* et *Rita* ont frappé de plein fouet le sud des États-Unis et ont créé d'importantes perturbations dans la région, touchant notamment les compagnies pétrolières, cœur de la production nationale d'énergies fossiles, qui ont vu la productivité de leurs raffineries chuter, handicapant ainsi les États-Unis de 23 % de leur capacité de raffinage de pétrole[7]. La question de la sécurité des importations est tout aussi problématique, comme en témoigne le phénomène résurgent de la piraterie maritime dans d'importantes zones de transit de pétrole tels le golfe d'Aden, l'océan Indien, le détroit de Malacca ou le golfe de Guinée.

[6] *Ibid.*, p. 70.

[7] « Rita and Katrina Have Shut 23 Percent of U.S. Oil Refining Capacity ». 2005. *Reuters*, 22 septembre. En ligne, http://www.nytimes.com/2005/09/22/business/RITAFACTBOX.html.



D'après : Bruce A. Forster. 2014. « Modern Maritime Piracy: An Overview of Somali Piracy, Gulf of Guinea Piracy and South East Asian Piracy ». British Journal of Economics, Management & Trade, vol. 4, no 8, p. 1258.

Ainsi, les attaques à l'encontre de pétroliers augmentent d'année en année[8] et entraînent des hausses importantes du coût de transport dans ces zones désormais considérées comme à haut risque, en raison de l'augmentation des primes d'assurances, de l'embauche de firmes de sécurité privées et des rançons payées en cas d'attaques réussies[9].

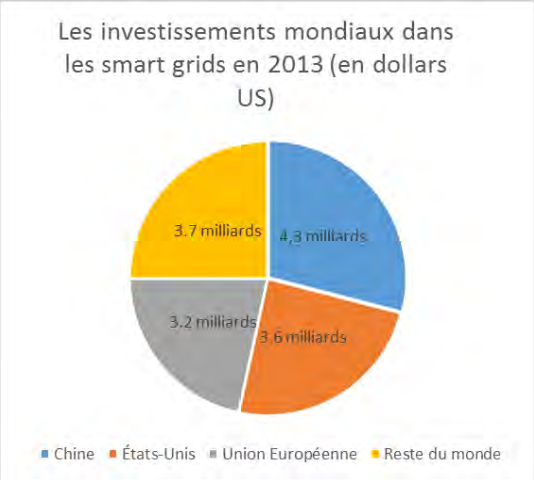
À ces problématiques s'ajoute également la difficulté croissante de développer de nouveaux gisements et de nouvelles sources d'approvisionnement. En effet, ceux-ci se situent souvent dans des endroits difficiles à atteindre et présentant de plus grands risques logistiques et environnementaux. L'exemple de Deepwater Horizon, plateforme pétrolière de forage en mer opérée par British Petroleum dans le golfe du Mexique, est probant. Elle possédait un puits mesurant plus de 10 kilomètres situé sous plus d'un kilomètre d'eau[10]. Ces conditions particulières ont joué un rôle clé lors de son explosion en 2010 : le puits s'est mis à fuir, créant une marée noire, mais il était trop profond pour que le colmatage de la suite possible. Par la suite, l'exploitation de nouveaux gisements de pétrole provenant du forage en mer a été suspendue dans le golfe du Mexique par l'administration Obama, dernier a par le fait entrepris d'intensifier

[8] United Nations Conference on Trade and Development. 2014. *Maritime Piracy – Part I: An Overview of Trends, Costs and Trade-related Implications*. Genève et New York : Nations Unies. En ligne, http://www.nytimes.com/2005/09/22/business/RITAFACTBOX.html, p. 7.

[9] J.W. Reuchlin. 2012. *Dalhousie Marine Piracy Project: The Economic Impacts of Piracy on the Commercial Shipping Industry – A Regional Perspective*. Halifax : Dalhousie University. En ligne, http://dmpp.management.dal.ca/wp-content/uploads/DMPP_Economic.pdf, pp.1-6. Par exemple, des pirates somaliens ont réussi à capturer le *Sirius Star*, en 2008, et le *Maran Centaurus*, en 2009, navires dont les libérations ont exigé une rançon de respectivement 3 millions et entre 5,5 millions et 7 millions. « Somali pirates fight over huge tanker ransom ». 2010. *BBC News*, 18 janvier. En ligne, <news.bbc.co.uk/1/hi/world/Africa/8464737.stm>; Sam Jones. 2009. « Somali pirates hijack oil tanker ». *The Guardian*, 30 novembre. En ligne, www.the guardian.com/world/2009/nov/30/pirates-seize-supertanker-somalia.

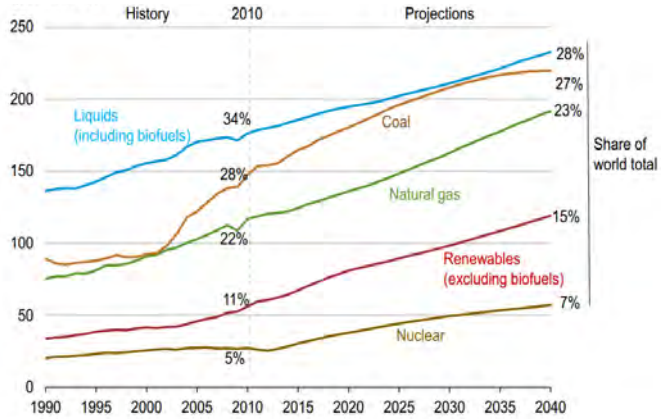
[10] " Transocean Says Well at BP Discovery Deepest Ever". 2009. Reuters, 2 septembre. En ligne, http://www.reuters.com/article/2009/09/02/bp-transocean-idUSN02119720090902.

l'effort américain pour se tourner vers d'autres sources d'énergie afin, en plus de rapprocher les États-Unis de ses objectifs environnementaux[11], de garder un approvisionnement énergétique constant à des prix plus abordables et stables. Si ce virage implique notamment la croissance de la production de ressources pétrolifères en sol américain, il fait aussi place à une présence importante des énergies *renouvelables*, que ce soit l'énergie solaire, éolienne, géothermique ou hydroélectrique.



Source : Louise Downing. 2014. « China Beats U.S. on Smart-Grid Spending for First Time », Bloomberg New Energy Finance, 19 février. En ligne, <www.bloomberg.com/news/articles/2014-02-18/china-spends-more-on-energy-efficiency-than-u-s-for-first-time>

Consommation mondiale par type de carburant (en quadrillion de BTU)



Source : Adam Sieminski, 2013. International Energy Outlook 2013, Center for Strategic and International Studies Washington, DC, <www.eia.gov/pressroom/presentations/sieminski_07252013.pdf.>

Alors que la diversification des sources d'énergie disponibles a toujours été un des aspects cruciaux de la sécurité énergétique[12], plusieurs États ont amorcé un virage semblable à celui des États-Unis, notamment ceux de l'Union européenne de même que la Chine, en proie à de graves problèmes de pollution atmosphérique. Pour y arriver ont été mis en place des programmes encourageant principalement la production d'énergies propres et l'achat de voitures électriques, dont le nombre est appelé à croître au cours des prochaines années. Par contre, afin de rendre efficace cette multiplication des points de production et cet effort de diminution de la dépendance envers les producteurs étrangers, et toutes les incertitudes y étant reliées, la mise en place d'un *smart grid*, ou *réseau électrique intelligent*, est devenu nécessaire.

[11] The White House. 2010. *Remarks by the President to the Nation on the BP Oil Spill.*15 juin. En ligne, www.whitehouse.gov/the-press-office/remarks-president-nation-bp-oil-spill.
[12] Yergin, *op. cit.*, p.70.

1.2 La nécessaire adaptation des fournisseurs en électricité

En août 2003, une panne électrique majeure frappait de plein fouet le nord-est des États-Unis et une bonne partie de l'Ontario, faisant sombrer de grandes villes comme New York ou Toronto dans le noir. Au total, près de 50 millions de personnes ont été touchées et des estimations font état de pertes financières se situant entre 4 et 10 milliards de dollars, aux États-Unis seulement[13]. C'est finalement le simple contact d'une ligne à haute tension surchargée avec un arbre qui aurait causé un court-circuit menant à un gigantesque effet domino. Dans la foulée, les lignes électriques encore fonctionnelles ont alors été sur sollicitées et ont également fini par être mises hors service : le surplus d'électricité à transporter, la demande d'énergie constamment élevée et la chaleur importante sont des facteurs qui ont mené au ramollissement des fils, qui sont à leur tour entrés en contact avec de la végétation[14].

Cette gigantesque interruption de service illustre bien la vulnérabilité d'un réseau électrique traditionnel et séculaire : « Il a répondu à nos besoins dans le passé; malgré tout, alors que notre société progresse technologiquement, nos attentes envers le système de livraison d'énergie électrique aussi. Le *smart grid* est un mouvement visant à actualiser le réseau électrique actuel pour le rendre conforme aux exigences actuelles et futures des consommateurs[15] ». Une société devenant progressivement numérisée, et aux exigences énergétiques croissantes[16], s'est mise en place pour englober et interconnecter tous les pans de la société, où la présence d'ordinateurs, de composantes électroniques et de communications sans fil rend possible la mise en place de processus automatisés. De plus, avec la mise en marché de plus en plus fréquente de moyens de transport hybrides ou entièrement électriques, il est attendu que cette demande en électricité soit en pleine hausse[17]. Ces innovations technologiques, intégrées dans des secteurs fortement interdépendants, ont également rendu indispensable l'idée d'un approvisionnement électrique stable[18]. La congestion du réseau et la variation du flux ne font qu'augmenter, situation menant souvent à des interruptions de services qui engendrent, aux États-Unis seulement, des pertes de 49 milliards de dollars par année. Or ces pertes financières pourraient être réduites de moitié en augmentant l'efficacité du réseau[19].

---

[13] U.S.-Canada Power System Outage Task Force. 2004. *Final Report on the August 14, 2003 Blackout in United States and Canada: Causes and Recommendations*. En ligne, <energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinal-Web.pdf>, p. 1.

[14] JR. Minkel. 2008. « The 2003 Northeast Blackout–Five Years Later », *Scientic American*, 13 août. En ligne, www.scientificamerican.com/article/2003-blackout-five-years-laters/.

[15] Todd Baumeister. 2010. *Literature Review on Smart Grid Cyber Security*. Honolulu : Université d'Hawaii. En ligne, https://csdl-techreports.googlecode.com/svn/trunk/techreports/2010/10-11/10-11.pdf. p.6.

[16] Massoud Amin et Anthony M. Giacomoni. 2012. « Smart Grid – Safe, Secure, Self-Healing : Challenges and Opportunities in Power System Security, Resiliency, and Privacy », *IEEE Power & Energy Magazine*, janvier/février 2012, p. 35.

[17] Antonio Collela, Anielle Castiglione et Clara Maria Colombini. 2014. « Industrial Control System Cyber Threats Indicators in Smart Grid Technology », *2014 International Conference on Network-Based Information Systems*, Salerne (Italie), 10-12 septembre, p. 153.

[18] Amin et Giacomoni, *op. cit.*, p. 34.

[19] *Ibid.*, p. 38.

Dès lors, en plus de permettre un approvisionnement stable et optimal, cette informatisation du réseau électrique actuel vise, par l'intégration massive des technologies de l'information et de la communication (TIC), à le rendre plus efficace par la rationalisation et la décentralisation de la production, du transport et de la consommation d'électricité, rendant ces opérations plus fluides par la multiplication des points intermédiaires entre le producteur et le consommateur.

Parallèlement, se développent des capacités de stockage de l'énergie pour une utilisation ultérieure, ce qui a longtemps été impossible avec le réseau actuel. Cela permet désormais de s'adapter à la production instable de sources d'énergie électrique, telles que l'éolien ou le solaire, et de maximiser leur apport[20]. Cela permet également d'établir une structure décentralisée qui permet au consommateur d'éventuellement produire sa propre électricité et de la vendre par l'entremise du réseau électrique, qui passe ainsi d'une interaction unidirectionnelle, du producteur au consommateur, à bidirectionnelle[21]. De plus, le développement et l'intégration croissante de sources d'énergie dites *vertes* dans des réseaux plus vastes permettront, à terme, d'augmenter le bassin d'électricité en circulation et de multiplier les points de production. Ainsi, un centre de distribution local pourra avoir accès à une panoplie de sources d'énergie éloignées pouvant compenser rapidement les manques de sa propre production, notamment en déterminant le moyen le plus rapide de transporter de l'électricité d'un point à un autre. La création d'une telle *autoroute* de l'électricité permet alors de réduire les effets de la distance géographique sur le transport de l'électricité et de développer un marché économique plus grand, plus fluide et plus compétitif[22].

Finalement, cette recherche d'efficacité vise également à minimiser les pertes et à éviter les surcharges pouvant mener à des pannes importantes. Au niveau du consommateur, celui-ci peut, par l'entremise d'un compteur intelligent, prendre connaissance de sa consommation électrique quotidienne et l'ajuster s'il cherche à réaliser des économies[23]. Pour les producteurs, cet effort de régulation de la consommation peut s'effectuer en aval par la présence de plus en plus nombreuse d'objets domestiques dits *intelligents*, communiquant avec le réseau électrique via les réseaux sans fil et recevant des informations leur indiquant les périodes de fonctionnement où il y a une moins grande demande[24]. De cette façon, en prenant en compte divers paramètres (température, niveau de la production, prix, etc.) et en contrôlant les

[20] Kallisthenis I. Sgouras, Athina D. Birda et Dimitris P. Labridis. 2014. « Cyber Attack Impact on Critical Smart Grid Infrastructures », *Innovative Smart Grid Technologies Conference* (ISGT), Washington D.C. (États-Unis), 19 au 22 février, p. 1.
[21] Baumeister, *op. cit.*, p. 2.
[22] Carlos Barreto et collab. . 2014. « Control Systems for the Power Grid and Their Resiliency to Attacks », *Security & Privacy, IEEE*, vol. 12, no 6. p. 18.
[23] Collela, Castiglione et Colombini, *op. cit.*, p. 375.
[24] U.S. Department of Energy. s.d. « The Smart Home », *What is the Smart Grid?*. En ligne, <www.smartgrid.gov/the_smart_grid/smart_home>.

modalités d'usage de certains objets, le réseau intelligent parvient à répartir plus équitablement la demande en électricité. Par cette recherche constante d'efficacité et d'optimisation, le réseau électrique gagne également en fiabilité : puisqu'il est composé d'un très grand nombre de centrales-relais réparties sur l'ensemble du territoire, une interruption de service sera presque immédiatement localisée grâce aux compteurs intelligents et corrigée rapidement en déroutant le flux électrique afin qu'il transite par d'autres points pour réalimenter le secteur touché[25].

Ainsi, cette recherche de rationalisation du réseau électrique se fait avec l'introduction à tous les niveaux de composantes informatiques servant à obtenir des informations en temps réel et à réagir de manière optimale. Pour autant, cet accroissement subséquent de la sécurité de l'approvisionnement énergétique va de pair avec des questionnements accrus sur la sécurité cybernétique[26] d'un réseau plus informatisé et automatisé.

2. Le réseau électrique intelligent : une sécurité informatique fragile

Compte tenu du fait que le réseau électrique d'un pays fait partie de ses *infrastructures critiques* nationales, son « dysfonctionnement pourrait mener à une crise socio-économique d'envergure pouvant potentiellement miner la stabilité d'une société et par le fait même, avoir des impacts politiques, stratégiques et sécuritaires[27] ». Ainsi, des pans entiers de la société, comme la santé, l'économie, le transport et le secteur industriel, sont tout à la fois cruciaux et terriblement dépendants du secteur de l'énergie. Car de la fiabilité de ce dernier dépend le fonctionnement normal des autres[28]. Si les avancées technologiques dans le domaine des TIC permettent d'optimiser les activités du secteur de l'énergie électrique, elles ouvrent également la porte à l'exploitation possible des éléments informatiques par des pirates. Ces éléments (périphériques, systèmes, réseaux) d'un réseau intelligent fortement décentralisé, notamment au niveau de sa sécurité, seront d'ailleurs de plus en plus nombreux, proportionnellement à l'expansion du réseau. Ainsi, seul un utilisateur autorisé doit pouvoir avoir accès aux données transmises via un réseau sans fil et avoir la capacité de modifier ces données, tout en étant en mesure d'y accéder au moment opportun[29].

[25] Baumeister, *op. cit.*, p. 1.
[26] La cybersécurité est « la protection requise pour s'assurer de la confidentialité, de l'intégrité et de la disponibilité d'un système électronique de communication d'informations. » Gopalakrishnan Iyer et Prathima Agrawal. 2010. « Smart Power Grids ». *2010 42nd Southeastern Symposium on System Theory*, Tyler (Texas, États-Unis), 7 au 9 mars, p. 152.
[27] Lior Tabansky. 2011. « Critical Infrastructure Protection against Cyber Threats », *Military and Strategic Affairs*, vol. 3, no 2, p. 62.
[28] U.S. Department of Homeland Security. 2013. « Energy Sector », *Critical Infrastructure Sectors*. En ligne, <www.dhs.gov/energy-sector>.
[29] Collela, Castiglione et Colombini, *op. cit.*, p. 376.

Désormais, par la mise en place des *smart grids,* la sécurité énergétique d'un pays est intrinsèquement liée à sa sécurité informatique. Tout comme pour les autres systèmes s'y apparentant, les craintes concernant la cybersécurité émanent d'une part des vulnérabilités et faiblesses que l'on trouve dans l'architecture ou dans la conception même de ces systèmes, mais aussi, d'autre part, d'incidents qui ont rendu tangible l'exploitation de ces vulnérabilités; et qui donnent un aperçu de ce qui pourrait être fait à l'encontre du réseau électrique intelligent.

2.1 De nombreuses vulnérabilités déjà identifiées

Rendu possible par l'explosion des possibilités offertes par une industrie des TIC qui réussit à constamment réduire la taille et le prix des matériaux, le *réseau électrique intelligent* émerge parallèlement à l'apparition et à l'expansion de l'*Internet des objets*, où, à travers le cyberespace, des milliards d'appareils de diverses natures sont reliés[30] : des objets domestiques considérés comme étant *intelligents*, mais aussi des éléments faisant partie de processus industriels, utilisant le cyberespace pour communiquer, s'échanger des données, être en constante interaction et même influer l'un sur l'autre par le biais du sans fil. L'élargissement constant de cet *Internet des objets*, qui pourrait en inclure plus de 50 milliards en 2020[31], permet également de multiplier les points d'entrées accessibles à ceux désirant les exploiter, par la présence fréquente de graves lacunes au niveau de la sécurité informatique[32]. Cette présence de failles est symptomatique d'une complexification de la technologie, mais également d'une industrie où la sécurité est souvent reléguée au second plan, supplantée par l'objectif de rendre un produit convivial, facile d'utilisation et financièrement profitable (la batterie de tests visant la sécurisation pouvant s'avérer longue et onéreuse[33]). Si la prise de contrôle à distance d'un réfrigérateur par une tierce personne pour envoyer des pourriels[34] peut sembler bénigne bien que préoccupante, il n'en est pas de même pour les appareils reliés de près ou de loin au *smart grid* et dont l'accès ou le dérèglement par une personne non autorisée pourrait avoir des conséquences considérables.

Si les objets intelligents reliés au réseau domestique, incluant les compteurs intelligents, peuvent ouvrir la porte à des fraudes potentielles et à des problèmes de confidentialité des informations des

[30] « The Internet of Things ». s.d. *Cisco Visualisation.* En ligne, <share.cisco.com/internet-of-things.html>.
[31] *Id.*
[32] Ijeoma Onyeji, Morgan Bazilian et Chris Bronk. 2014. « Cyber Security and Critical Energy Infrastructure ». *The Electricity Journal*, vol. 27, no 2, p. 56.
[33] Collela, Castiglione et Colombini, *op.cit.*, p. 375.
[34] Hu, Elise. 2014. « What Do You Do If Your Refrigerator Begins Sending Malicious Emails? », *National Public Radio*, 16 janvier. En ligne, <www.npr.org/blogs/alltechconsidered/2014/01/16/263111193/refrigerator-hacked-reveals-internet-of-things-security-gaps>.

consommateurs[35], la plus grande faiblesse du réseau tient plutôt au croisement des TIC et des technologies opérationnelles (TO), « le matériel et le logiciel qui détecte et amène des changements par la supervision directe et/ou le contrôle de dispositifs physiques, de processus ou d'évènements dans l'entreprise[36] ». L'intelligence du réseau électrique réside justement dans le processus où de multiples capteurs acheminent des informations précises et en temps réel sur l'état du réseau à un système de type SCADA[37], qui captera, analysera et réagira rapidement en conséquence[38]. Le problème est qu'en terme de sécurité informatique, ceux-ci sont très loin d'avoir été conçus en prévision de l'intégration des TIC dans leur fonctionnement : ce qui fut originalement prévu pour superviser un réseau interne, formé de composantes de surveillance et de contrôle ne nécessitant pas a priori de sécurité informatique et qui était isolé du monde extérieur, doit désormais cohabiter avec la multiplication des accès, des outils, des périphériques et des acteurs liés au cyberespace. Certains systèmes SCADA ont été mis en place il y a des dizaines d'années et sont désormais impossibles à mettre à jour. Ils doivent alors absolument être remplacés par du matériel plus récent, plus sécuritaire, mais cela est synonyme d'investissements majeurs donc souvent reportés. Le « nombre de brèches de sécurité découvertes lors de la dernière décennie illustre que [la] conception originale et évolution subséquente [de ces systèmes] a échoué à considérer adéquatement les risques d'une attaque délibérée[39] ».

Une des sources de vulnérabilité résultant de l'intégration des TIC aux TO repose sur le fait que tous les appareils font transiter leurs données via le réseau public qu'est Internet en utilisant l'*Internet Protocol* (IP)[40]. Or, ce moyen, commode et commun, a des faiblesses connues qui peuvent faciliter les risques d'intrusions ou d'interceptions de données. Si ce protocole grand public est utilisé, c'est en raison de la perception de rentabilité qu'inspire la gestion à distance d'énormes et complexes systèmes avec l'aide de programmes, de protocoles et de produits communs, fabriqués en série, déjà fonctionnels, simples et peu coûteux à utiliser. Ils présentent cependant de graves lacunes au niveau de la sécurité[41]. Un cryptage renforcé des informations transitant via l'IP assurerait une bonne sécurité tout en préservant la convivialité de ce système. Par contre, deux obstacles ralentissent la mise en place de cette solution : les coûts

[35] Amin et Giacomoni, *op. cit.*, p. 38.
[36] Gartner. s.d. « Operational Technology », *IT Glossary*. En ligne, <www.gartner.com/it-glossary/operational-technology-ot>. Consulté le 1er décembre 2014.
[37] Acronyme de *Supervisory Control and Data Acquisition*, des « systèmes fortement distribués servant à contrôler des actifs géographiquement dispersés, souvent disséminés sur des milliers de kilomètres carrés, où l'acquisition et le contrôle centralisé des données sont essentiels au fonctionnement du système. » Keith Stouffer, Joe Falco et Karen Ken. 2006. *Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control System Security*. Gaithersburg, Maryland : National Institute of Standards and Technology (NIST), p. 2-1.
[38] Iyer et Agrawal, *op. cit.*, p. 152.
[39] A. Nicholson et collab. 2012. « SCADA Security in the Light of Cyber-Warfare », *Computers & Security*, vol. 31, no 4, p. 1.
[40] Protocole permettant d'attribuer aux objets composant un réseau, privé ou public, une adresse unique permettant de l'identifier et d'y accéder.
[41] Kenneth Geers. 2009. « The Cyber Threat to National Critical Infrastructures: Beyond Theory », *Information Security Journal: A Global Perspective*, vol. 18, no 1, p. 3; Nicholson et collab., *op. cit.*, p. 11.

accompagnant la recherche, le développement et la mise en place d'un processus de cryptage, et le fait que les appareils ne soient pas assez performants pour mener à bien cette fonction[42]. De ce fait, les incidents qui font la démonstration de la vulnérabilité du réseau soulèvent de manière récurrente la question de la sécurité des approvisionnements énergétiques.

2.2 Des questionnements récurrents

Les questionnements à propos de la cybersécurité du réseau électrique intelligent ne proviennent pas seulement des vulnérabilités potentiellement exploitables reposant sur la fusion entre les TIC et les systèmes industriels, ainsi que sur les très nombreux objets intelligents vendus sur le marché. En effet, si ces lacunes montrent les conséquences potentielles des failles observées et découvertes, de nombreux *cyberincidents* ont également eu lieu au cours des dernières années et ont permis l'observation réelle des modalités et impacts d'une cyberattaque sur des infrastructures dites critiques s'apparentant au *smart grid*.

2.2.1 Un accès illicite grandement facilité

La délocalisation de certains processus, confiés souvent à de plus en plus nombreux sous-traitants à des fins de productivité et d'économies, est en réalité un problème de taille pour la sécurité d'un système : tout lien de télécommunication se trouvant en dehors du contrôle direct d'une organisation est potentiellement une porte ouverte sur les opérations et le réseau électrique[43]. Alors que la sécurité des SCADA repose habituellement sur des pare-feu dont le mandat est d'en permettre l'accès aux utilisateurs autorisés seulement, il est impossible pour eux d'assurer cette protection si la cyberintrusion se déguise sous une identité autorisée pour se faire passer comme étant légitime[44].

Par exemple, pour un pirate cherchant à accéder aux serveurs d'une grande entreprise, la priorité pourra alors être d'obtenir un accès au réseau d'un de ses sous-traitants qui possèdent les autorisations nécessaires pour accéder à la cible principale. La technique la plus simple et la plus efficace est celle de l'hameçonnage, technique d'ingénierie sociale souvent utilisée et qui consiste à convaincre un employé d'ouvrir un fichier, qui est en fait un virus, donnant accès à l'ordinateur de cette personne, mais également à

[42] Collela, Castiglione et Colombini, *op. cit.*, p. 377.
[43] Amin et Giacomoni, *op. cit*., p.37.
[44] Alexandru Stefanov et Chen-Ching Liu. 2012. « Cyber-Power System Security in a Smart Grid Environment », *2012 IEEE PES Innovative Smart Grid Technologies*, Washington D.C. (États-Unis), 16 au 20 janvier 2012, p. 1.

son réseau en entier[45]. Ce faisant, le pirate informatique peut librement franchir un pare-feu en se faisant passer pour le sous-traitant et accéder aux systèmes de contrôle industriel et ses multiples composantes. Il aura alors la possibilité de compromettre « les opérations des capteurs, des communications et des systèmes de contrôles en imitant, en créant de l'interférence ou en envoyant de fausses commandes pouvant perturber le système, causer des pannes et dans certains cas, provoquer des dommages physiques sur des éléments clés du système[46] », évènement pouvant provoquer un important effet domino sur les autres infrastructures reliées.

Avoir accès à des éléments sensibles d'un système peut s'avérer parfois beaucoup plus simple. En effet, en 2013, des utilisateurs d'un forum de discussion découvraient un moteur de recherche nommé Shodan, répertoriant les adresses IP d'une très grande quantité d'objets de différents types reliés au cyberespace et situés aux quatre coins du monde. Parmi ceux-ci se trouvaient une multitude de périphériques dénués de protection et auxquels il était possible d'accéder à distance. Ses appareils étaient autant des objets intelligents domestiques que des éléments industriels, l'accès à chacun d'eux pouvant avoir des répercussions importantes sur le réseau électrique 2.0. Par exemple, John Matherly (le créateur de Shodan, ce moteur de recherche qui recense tous les objets reliés à l'internet) a affirmé avoir réussi à accéder au système de contrôle d'un crematorium, à celui d'un barrage situé en territoire français et à celui d'une usine de traitement des eaux[47]. Si ces résultats sont également utilisés par les experts en sécurité informatique pour apporter des correctifs aux accès de certains systèmes, Shodan a permis de découvrir comment l'informatisation croissante amène aussi le risque que de nouveaux éléments d'une grande valeur soient facilement accessibles, laissés à eux-mêmes et exploités par qui le veut bien avant même que quelqu'un en constate le risque et la possibilité.

2.2.2 Des vulnérabilités potentiellement coûteuses

Dès 2003, la sécurité informatique apparaît comme une nouvelle vulnérabilité menaçant la sécurité énergétique : bien que la panne majeure ayant touché le nord-est de l'Amérique du Nord ait été provoquée par un bris physique, c'est originalement une défaillance dans le système informatique de la compagnie FirstEnergy qui est le premier maillon de cette catastrophe en chaîne. En effet, les capteurs installés sur le

[45] Hannes Holm, Waldo Rocha Flores et Göran Ericsson. 2013. « Cyber Security for a Smart Grid – What About Phishing? », *2013 4th IEEE PES Innovative Smart Grid Technologies Europe (ISGT Europe)*, Copenhague (Danemark), 6 au 9 octobre, p. 1; John Hastings, David M. Laverty et D. John Morrow. 2014. « Securing the Smart Grid ». In *Power Engineering Conference (UPEC), 2014 49th International Universities*, 2 au 5 septembre, p. 3.

[46] Amin et Giacomoni, *op. cit.*, p. 5.

[47] Sam Clements. 2013. « Is Shodan Really the World's Most Dangerous Search Engine? », *Vice*, 26 avril. En ligne, http://www.vice.com/en_uk/read/shodan-exposes-the-dark-side-of-the-net.

réseau et le système qui aurait dû normalement alerter la compagnie d'une situation problématique n'ont tout simplement pas fonctionné[48], empêchant ainsi FirstEnergy d'avoir une compréhension optimale de son réseau et des évènements s'y déroulant, élément crucial permettant de prévenir et de contenir rapidement une panne comme celle de 2003. En un sens, peu importe que certains membres d'agences de renseignements américaines soupçonnent l'armée chinoise d'avoir pénétré le réseau électrique américain pour provoquer cette situation[49], puisque cet évènement illustre au final les répercussions que peut provoquer un système industriel informatisé qui flanche.

En 2006, le U.S. Department of Homeland Security a lancé le Projet Aurora, dans lequel le piratage d'une réplique d'un système de contrôle d'une centrale électrique a mené à l'autodestruction d'une génératrice. Cette expérience, bien que limitée en ampleur, démontrait plus concrètement la vulnérabilité du réseau électrique aux cyberattaques[50]. Bien qu'un seul bris d'équipement ne permet pas d'interrompre le fonctionnement de l'entièreté d'un réseau électrique, la Federal Energy Regulatory Commission des États-Unis a récemment conclu qu'il suffisait, dans leur cas, de mettre hors service neuf postes électriques, chargés de redistribuer régionalement l'électricité reçue du réseau, pour stopper le fonctionnement de la totalité du réseau électrique américain pendant dix-huit mois, sinon plus[51]. Récemment, le Projet Aurora est revenu dans l'actualité lorsque le Department of Homeland Security en a publié accidentellement le rapport, qui contenait des informations sur les composantes à risque et sur la manière de les détruire. Pour certains experts, « cette diffusion ne va certainement pas aider à rendre nos infrastructures critiques plus sécuritaires et, pour certains types d'attaquants, ces informations vont leur permettre de sauver beaucoup de temps pour la préparation d'éventuelles cyberattaques[52] ».

Malgré les conclusions médiatisées du Projet Aurora, Stuxnet est probablement l'incident le plus connu des évènements liés à la sécurité des systèmes de contrôle industriels. Stuxnet est un virus qui détenait une architecture très complexe et une cible précise : la machinerie industrielle de la multinationale allemande Siemens utilisée pour contrôler des centrifugeuses nucléaires[53]. Son objectif était de prendre le contrôle du système SCADA relié à ses équipements et de le reprogrammer afin de rendre dysfonctionnelles et inutilisables les centrifugeuses nucléaires qui y étaient rattachées. C'est ce qui arrivera à la centrale

[48] Minkel, *loc. cit*.
[49] Shane Harris. 2008. « China's Cyber Militia », *National Journal*, 31 mai. En ligne, <www.nationaljournal.com/magazine/china-s-cyber-militia-20080531>.
[50] Stefanov et Liu, *op. cit.*, p. 1; Onyeji, Bazilian et Bronk, *op. cit.*, p. 54.
[51] Rebecca Smith. 2014. « U.S. Risks National Blackout From Small-Scale Attack », *The Wall Street Journal*, 12 mars. En ligne, <online.wsj.com/news/articles/SB10001420527023040201045794336702840612 20>.
[52] Jeffrey Carr, cité dans Patrice Tucker. 2014. « Forget the Sony Hack, This Could Be the Biggest Cyber Attack of 2015 », *Defense One*, 19 décembre. En ligne, <http://www.defenseone.com/technology/2014/12/forget-sony-hack-could-be-hebiggest-cyber-attack-2015/101727/>.
[53] James P. Farwell et Rafal Rohozinski. 2011. « Stuxnet and the Future of Cyberwar », *Survival*, vol. 53, no 1, p. 24.

nucléaire iranienne de Natanz, un site présumé d'enrichissement d'uranium à des fins militaires. Bien qu'elle ne soit parvenue à son objectif (mettre un terme au programme nucléaire iranien), cette opération a réussi à repousser les limites de ce qui avait été jusqu'à maintenant largement qualifié de « cyberattaque ». Avec Stuxnet, l'opérationnalisation d'un nouveau champ de bataille a atteint un nouveau palier, puisqu'une capacité destructrice potentielle et inédite à l'encontre d'une infrastructure critique avait été atteinte par une arme cybernétique. Fort probablement introduit par une clé USB infectée[54], le virus utilisait plus de quatre vulnérabilités alors inconnues, mais présentes dans le système d'opération Windows[55]. Pendant des semaines, « le virus enregistrait les signaux électriques indiquant que les centrifugeuses fonctionnaient normalement. Ensuite, il repassait ses informations pendant qu'il prenait le contrôle et ainsi faire tourner les centrifugeuses à vive allure ou les freiner brusquement[56] » pour finalement les briser. La découverte de Stuxnet est fortuite : après que quelqu'un ait infecté son ordinateur portable en le connectant au réseau de la centrale, puis sur Internet par la suite, le virus s'est alors répandu très rapidement aux quatre coins du monde, faisant en sorte que s'il avait trouvé par accident une centrale nucléaire à la configuration identique à celle de Nantanz, Stuxnet se serait alors mis en marche et aurait affecté une autre cible que celle prévue initialement.

Cette opération, menée conjointement par les services secrets américains et israéliens, a créé des remous dans l'administration américaine et a alerté plusieurs décideurs des impacts éventuels qu'une telle manœuvre furtive, que l'on sait désormais possible et dont on connaît également le processus, pourrait avoir sur leur propre territoire et au niveau de leurs propres infrastructures dites critiques. En 2010, un haut gradé du Département de l'Énergie américain, Bill Hunteman, affirmait que Stuxnet ne s'avérait qu'être le commencement d'une future vague de cyberattaques qui allait reproduire la voie prise par le virus, la plus grosse partie du travail ayant été fait, selon lui[57]. De son côté, Richard Clarke, qui fut le conseiller spécial en cybersécurité du président W. Bush, a affirmé que malgré leur grande capacité de cyberoffensive, les États-Unis restaient extrêmement vulnérables aux capacités que Stuxnet venait de démontrer[58]. Pour autant, appliqué au réseau électrique, la sécurité s'évalue plus en termes de risques que de menaces.

[54] *Ibid.*, p. 24.
[55] Ronald J. Deibert. 2013. *Black Code: Inside the Battle for Cyberspace*. Toronto : McClelland & Stewart, p. 177.
[56] David E. Sanger. 2012. *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*. New York : Broadway Paperbacks, p. 199.
[57] Alexis C. Madrigal, « Stuxnet? Bah, That's Just the Beginning », *The Atlantic*, 16 décembre 2010. En ligne, www.atlanctic.com/technology/archive/2010/12/stuxnet-bah-thatsjust-the beginning/68154/.
[58] Richard A. Clarke et Robert Knake. 2010. *Cyber War: The Next Threat to National Security and What to Do about It*. New York : Harpercollins, p.145.

3. Les risques relatifs du réseau électrique intelligent

Si la sécurité informatique des composantes vitales du *smart grid* a longtemps été négligée, Stuxnet a eu l'effet d'un électrochoc : « pour plusieurs, c'était un signal d'alarme qui augmentait la sensibilisation sur la sécurité de ces systèmes, encore vu comme une addition facultative et non pas comme un processus continu devant être intégré dans tous les aspects opérationnels[59] ».

3.1 Une sécurisation graduelle

Si Stuxnet constitue une avancée, il apparaît que la centrale de Natanz, bien qu'elle n'ait pas été directement connectée à Internet à des fins de protection, ne possédait aucune cyberdéfense digne de ce nom ; malgré l'exploit technique qu'il représente, Stuxnet n'a pas eu à franchir beaucoup d'obstacles pour se déployer. Si le gouvernement iranien avait le moindrement équipé sa centrale de défenses informatiques et s'était penché sur la sécurité de ses équipements[60], tout le déroulement de l'opération aurait pu être contrarié. C'est justement sur la mise en valeur de la cyberdéfense des infrastructures critiques que portent de nombreux efforts des praticiens en sécurité informatique[61].

En ce qui a trait aux réseaux électriques nord-américains, des tentatives d'intrusions sont quotidiennement répertoriées. Néanmoins, les entreprises dans le milieu de l'énergie électrique sont assujetties aux normes américaines, instituées par l'agence gouvernementale qu'est la National Institute of Standards and Technology (NIST). Ces normes ont spécifiquement été mises en place pour les réseaux électriques intelligents et dictent les standards pour l'interopérabilité, la cybersécurité du réseau, pour la production et le transport d'énergie ; le respect des critères est un prérequis à l'obtention des subventions et nombreux contrats publics. En effet, la question de la sécurité informatique est importante dans leur attribution, puisque 20 % de la note, pour déterminer le candidat récoltant une subvention ou un contrat, est attribué à ce seul point lors de l'évaluation des candidatures, obligeant les postulants à fournir un effort de sécurité supplémentaire. Par contre, les contrats publics ou de sous-traitance sont habituellement octroyés au soumissionnaire conforme présentant le plus bas prix, un avantage pécuniaire que certains obtiennent en

[59] Stamatis Karnouskos. 2011. « Stuxnet Worm Impact on Industrial Cyber-Physical System Security ». *IECON 2011 - 37th Annual Conference of the IEEE Industrial Electronics Society*, Novembre 2011, pp.4490

[60] *Ibid.*, p. 4491.

[61] Entrevue menée avec M. Jean LeDuc, responsable de la sécurité informatique chez Hydro-Québec, le 24 novembre 2014. Cette entrevue nous a permis de constater les mesures prises par les organisations concernant la sécurité informatique de leurs installations.

sabrant dans la sécurité de leurs logiciels et de leurs périphériques, et dans la formation des employés concernant « les erreurs ou transgressions pouvant mener à une cyberintrusion[62] ».

Hydro-Québec, société d'État québécoise, oblige contractuellement ses fournisseurs à mener une batterie de tests visant à s'assurer de leur propre sécurité informatique, les simples normes et standards de sécurité communes à l'industrie ne suffisant pas toujours[63] selon eux. Ainsi, des entreprises de pirates informatiques sont engagées spécialement pour faire des tests d'intrusion : attaquer un périphérique, un service offert ou le réseau pour en découvrir les vulnérabilités avant qu'un inconnu ne le fasse. Il est alors possible d'apporter les correctifs nécessaires pour une sécurité de pointe[64]. Les tierces parties ne sont pas naturellement portées à s'attarder à la question de la sécurité informatique de ce qu'elles offrent, les coûts pouvant être exorbitants et l'apport potentiel, abstrait[65].

Si plusieurs croient que dans le cyberespace, l'offensive a toujours l'avantage sur la défensive, cette dernière peut néanmoins se renforcer, corriger rapidement ses vulnérabilités et ainsi rendre désuètes les « cyberarmes » qui les exploitaient et dont l'efficacité dépendait. La sensibilisation auprès des gens, souvent la porte d'entrée d'attaques potentielles, l'amélioration constante des équipements, et la prise de conscience collective des enjeux cruciaux reliés à la sécurité informatique des infrastructures critiques, dont font partie les réseaux électriques intelligents, peuvent permettre de limiter le spectre des cyberattaques possibles.

Malgré cette conscientisation concernant la sécurité informatique d'un réseau, celle-ci repose en dernier ressort sur les personnes y ayant accès. Le facteur humain reste le maillon faible du réseau. En effet, il suffit qu'une seule personne ouvre une pièce jointe porteuse d'un virus ou insère une clé USB infectée dans un ordinateur relié au réseau ciblé pour compromettre entièrement la sécurité informatique du système. La curiosité, la naïveté ou une simple méconnaissance de l'informatique d'une personne peuvent ainsi avoir des conséquences considérables[66]. Ainsi, lorsque de très grandes organisations sont ciblées, les probabilités qu'une tentative d'hameçonnage fonctionne augmentent en raison du nombre important d'employés, et de la difficulté pour la personne responsable des TIC de défendre un si grand front. Heureusement, l'accomplissement d'un acte dommageable de grande ampleur dans le domaine cybernétique demeure encore hors de portée du plus grand nombre, tant sa réalisation est complexe.

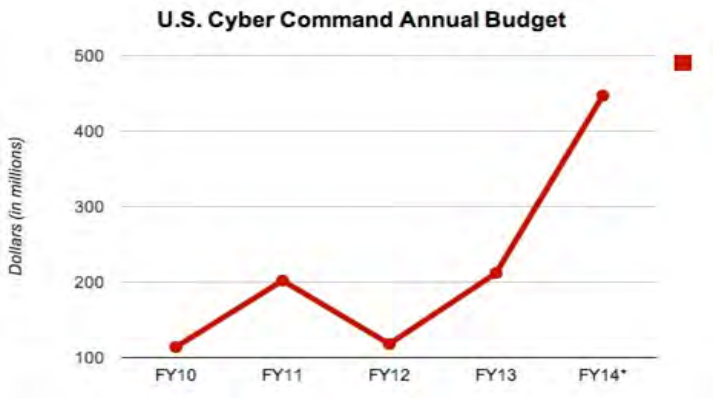
[62] James P. Farwell et Rafal Rohozinski. 2012. « The New Reality of Cyber War », *Survival*, vol. 54, no 4, p. 109.
[63] Jean LeDuc, *op. cit.*
[64] Hastings, Laverty et Morrow, *op. cit.*, p. 1.
[65] Jean LeDuc, *op. cit.*
[66] Holm, Flores et Ericsson, *op. cit.*, p. 4.

3.2 Des attaques complexes

Ultimement, le dernier élément rendant relatif des cyberattaques de grandes envergures sur le réseau électrique intelligent est la question des acteurs pouvant potentiellement les mener. La création et la mise en place de ces cyberattaques contre des infrastructures critiques et le *smart grid* sont des processus de longue haleine, gourmands en ressources. Après les évènements du 11 septembre 2001, la question du cyberterrorisme avait été mise à l'agenda. Cependant, cette voie a été démontrée comme étant trop dispendieuse et présentant des retombées trop incertaines pour être pleinement efficace[67]. Pour un groupe terroriste aux moyens modestes, le coût opérationnel pour entreprendre ce type d'attaques explose par la simple nécessité d'engager des spécialistes informatiques, déjà recrutés à grands frais dans le secteur privé[68]. Le général Keith B. Alexander, ancien chef de la National Security Agency et du U.S. Cyber Command, a même proclamé en 2013 que « capacité [des groupes terroristes] à mener une telle action ne correspond pas à leurs intentions[69] ». Il préférait concentrer ses efforts sur le rôle des États et de leurs agences de renseignements, acteurs possédant un avantage stratégique certain par leur capacité supérieure de coordination des ressources[70]. Le regard se tourne vers eux, car des cyberattaques nécessitent un travail de longue haleine pour demeurer furtives et efficaces : après un effort de reconnaissance nécessaire du réseau à attaquer, des composantes informatiques y étant reliées et des vulnérabilités qu'elles contiennent, il est alors nécessaire de fabriquer un virus sur mesure, comme le fut Stuxnet[71]. Le *modus operandi* de ce dernier était d'envergure : changer le comportement physique d'un élément, camoufler les effets du virus sur la cible et en empêcher la rémission et l'arrêt de l'opération[72]. L'atteinte de ces buts a nécessité une collaboration d'experts dispendieux et de divers milieux concernés par l'attaque : programmeurs informatiques, experts en systèmes de contrôle industriels, etc. L'équipe derrière Stuxnet avait un budget de 300 millions de dollars pour le seul développement du virus[73].

---

[67] Giampiero Giacomello. 2004. « Bangs for the Buck: A Cost-Benefit Analysis of Cyberterrorism », *Studies in Conflict and Terrorism*, vol. 27, no 5, p. 388.
[68] *Ibid.*, p. 396.
[69] États-Unis, Department of Defense. 2013. *Statement of General Keith B. Alexander, Commander of United States Cyber Command Before the House Committee on Armed Services, Intelligence, Emerging Threats and Capabilities Subcommittee – 13 March 2013*. Washington D.C. : The White House, p.4.
[70] Douglas Warfield. 2012. « Critical Infrastructures : IT Security and Threats from Private Sector Ownership ». *Information Security Journal : A Global Perspective*, vol.21, no.3, p.129
[71] Hastings, Laverty et Morrow, op.cit., p.3
[72] Byungho Min et Vijay Varadharajan. 2014. « Design and Analysis of Security Attacks against Critical Smart Grid Infrastructures ». *2014 19th International Conference on Engineering of Complex Computer Systems*, Tianjin (Chine), 4 – 7 août 2014, p.61
[73] Jon R. Lindsay. 2013. « Stuxnet and the Limits of Cyber Warfare », *Security Studies*, vol.22, no.3, p.38



Source: Brian Fung. 2014. "Cyber Command's exploding budget, in 1 chart", The Washington Post, 15 janvier. En ligne, <https://www.washingtonpost.com/news/the-switch/wp/2014/01/15/cyber-commands-exploding-budget-in-1-chart/>.

Cependant, un acteur étatique, se trouvant dans une situation d'interdépendance économique, a peu de chance de vouloir se lancer dans des cyberopérations militaires pour à « infliger à distance des dommages douloureux et asymétrique à un adversaire[74] » en attaquant ses infrastructures importantes pour saper sa volonté combattante. Le risque de représailles et de retombées négatives de telles actions pouvant sembler trop important, un État pourra vraisemblablement plutôt choisir une forme de dissuasion auprès de ses « adversaires » par le doute qu'il sème chez ses derniers. En effet, pour Martin Libicki, chercheur à la RAND Corporation, un *think tank* américain œuvrant dans le milieu de la défense, « la cible d'une attaque n'est pas un système informatique, mais la *confiance* en celui-ci ou dans tous les autres systèmes informatiques[75]». Puisqu'il est impossible d'assurer qu'une cyberattaque initiale puisse empêcher des représailles sévères ou des contrecoups inattendus, ce doute pousse tout le monde à la retenue, limitant fortement le risque qu'une attaque vienne perturber de manière importante le cours normal de la société. Toutefois, on peut opposer à l'application du concept de dissuasion à l'espace cybernétique celui de « dilemme de sécurité » : l'État, toujours incertain de ce qui se trame dans un espace qu'il ne contrôle pas vraiment, ne cesse de renforcer ses capacités défensives et offensives, pendant que ces « opposants » finissent par faire autant.

Ainsi, l'émergence de tensions internationales pourrait rapidement changer l'état de dissuasion ayant cours présentement, dans la mesure où les acteurs ne sont pas uniquement étatiques – et donc moins prévisibles. Par exemple, un groupe armé tel que l'État islamique, possédant à la fois des ambitions politiques et territoriales et des ressources humaines et monétaires considérables, pourrait mener une cyberattaque, lui qui, jusqu'à maintenant, semble prêt à agir de manière non conventionnelle pour arriver à ses fins. Alors que de plus en plus d'Occidentaux scolarisés rejoignent les rangs de l'EI, l'accès facilité à des

[74] Geers, *op. cit.*, p. 3.
[75] Martin C. Libicki. 2011. « Cyberwar as a Confidence Game », *Strategic Studies Quarterly*, vol. 5, no 1, p. 140.

programmeurs informatiques talentueux, à des ingénieurs spécialisés, ou encore à d'anciens employés d'entreprises fabriquant des composantes informatiques sensibles destinées à des infrastructures critiques situées dans des pays ciblés par le groupe, peut représenter une force de taille. Il est alors tout à fait possible d'imaginer, à l'instar des scénarios élaborés par les gouvernements à l'issue du 11 Septembre, que les infrastructures représentent alors le talon d'Achille[76] de ces derniers.

À ce titre, la Chine représente par exemple une source constante d'inquiétudes chez les responsables de la sécurité nationale américaine : en plus d'être soupçonnée d'avoir pénétré de très nombreux ordinateurs gouvernementaux, militaires et commerciaux à travers le monde[77], un livre de deux généraux chinois, *La guerre sans limites*, décrit ce que plusieurs interprètent comme étant une esquisse de la stratégie chinoise pour un futur conflit, stratégie atypique où tous les moyens seraient bons pour obtenir la victoire, notamment en s'attaquant au réseau électrique adverse par le moyen de virus informatiques :

« [...] après avoir provoqué une crise financière, il opérera une attaque de ses réseaux grâce à des virus implantés à l'avance dans les systèmes informatiques de l'adversaire et à l'intervention d'équipes de pirates informatiques. Il provoquera l'effondrement total du réseau électrique civil, du réseau de régulation des transports, du réseau de transactions boursières, des réseaux de télécommunications et des réseaux médiatiques, déclenchant une panique sociale, des troubles civils et une crise gouvernementale[78]. »

De fait, les armées établissent déjà de nombreux scénarios de conflits qui incluent une dimension cybernétique croissante. Ainsi, le livre blanc du ministère français de la Défense établit clairement les termes des nouvelles tensions, puisqu'il énonce en 2013 la dimension « majeure » de la menace d'une cyberattaque[79]. Dans les conflits à venir, l'effacement de la notion de *distance* dans le cyberespace fait des infrastructures critiques, tel que le réseau électrique intelligent, des cibles de choix, relativement simple à attaquer.

Conclusion

Au final, les grands risques apparents que l'informatisation et la connexion du réseau électrique intelligent au cyberespace semblent amener au niveau de la sécurité énergétique d'un État semblent inévitables : l'accès apparaît simplifié et l'omniprésence des systèmes de contrôle industriels dans la société

[76] Voir Charles-Philippe David et collab. 2006. *Le 11 septembre 2001, 5 ans plus tard*. Québec : Septentrion, p. 120.
[77] Deibert, *op. cit.*, p. 21-28
[78] Qiao Liang et Wang Xiangsui. 1999. *La Guerre hors limites*. Paris : Payot et Rivages, p. 205-206.
[79] Défense et sécurité nationale. 2013. *Livre blanc*. Paris : DILA. En ligne, <http://www.livreblancdefenseetsecurite.gouv.fr/pdf/le_livre_blanc_de_la_defense_2013.pdf>. Consulté le 2 mars 2015

rend celle-ci fragile par la multiplication des points d'entrées potentiels. Malgré tout, l'éventualité qu'une cyberattaque majeure puisse paralyser un État durablement apparaît (pour le moment) mince. D'entrée de jeu, les différents acteurs responsables de la sécurité informatique du réseau électrique semblent avoir intégré, après Stuxnet, la nécessité d'évaluer et d'accroître la sécurité du *smart grid*. Ultimement, la difficulté réelle de mener une cyberattaque restreint considérablement le nombre d'acteurs en mesure d'en concevoir.

Malgré tout, il demeure impossible de rendre étanche une cyberdéfense. Même si des mesures de sécurité matérielles sont prises, telles que des mises à jour fréquentes ou le cryptage des informations, la sécurité informatique comporte encore une dimension humaine et éminemment faillible, que la robotisation ne pourra jamais totalement réduire. La recherche active et la prise de conscience des vulnérabilités informatiques afin de les corriger sont des étapes nécessaires, mais malheureusement, non suffisantes.

Bibliographie

« The Internet of Things ». s.d. Cisco Visualisation. En ligne, <share.cisco.com/internet-of-things.html>. Consulté le 24 novembre 2014.

« Rita and Katrina Have Shut 23 Percent of U.S. Oil Refining Capacity ». 2005. *Reuters*, 22 septembre. En ligne, <http://www.nytimes.com/2005/09/22/business/RITA-FACTBOX.html>. Consulté le 2 novembre 2014.

« Somali pirates fight over huge tanker ransom ». 2010. *BBC News*, 18 janvier. En ligne, <news.bbc.co.uk/1/hi/world/africa/8464737.stm>. Consulté le 3 novembre 2014.

Amin, Massoud et Anthony M. Giacomoni. 2012. « Smart Grid – Safe, Secure, Self-Healing: Challenges and Opportunities in Power System Security, Resiliency, and Privacy », *IEEE Power & Energy Magazine*, janvier/février, p.33-40.

Barreto, Carlos et collab. 2014. « Control Systems for the Power Grid and Their Resiliency to Attacks », In *Security & Privacy, IEEE*, vol. 12, no 6, p. 15-23.

Baumeister, Todd. 2010. *Literature Review on Smart Grid Cyber Security*. Honolulu : Université d'Hawai, 30 p. En ligne, < https://csdl-techreports.googlecode.com/svn/ trunk/techreports/2010/ 10-11/10-11.pdf>. Consulté le 15 février 2015.

British Petroleum. 2014. *BP Statistical Review of World Energy 2014*. En ligne, <https://upload.wikimedia.org/wikipedia/commons/thumb/1/13/World_energy_consumption_fr.svg/660px-World_energy_consumption_fr.svg.png>. Consulté le 25 février 2015.

Clarke, Richard A. et Robert Knake. 2010. *Cyber War: The Next Threat to National Security and What to Do about It*. New York : Harpercollins, 290 p.

Clements, Sam. 2013. « Is Shodan Really the World's Most Dangerous Search Engine? », *Vice*, 26 avril. En ligne, <http://www.vice.com/en_uk/read/shodan-exposes-the-dark-side-of-the-net>. Consulté le 18 novembre 2014.

Collela, Antonio, Anielle Castiglione et Clara Maria Colombini. 2014. « Industrial Control System Cyber Threats Indicators in Smart Grid Technology », *2014 International Conference on Network-Based Information Systems*, Salerne (Italie), 10-12 septembre, p.374-380.

David, Charles-Philippe, et collab. 2006. Le 11 septembre 2001, 5 ans plus tard. Québec : Septentrion, 120 p.

Deibert, Ronald J. 2013. *Black Code: Inside the Battle for Cyberspace*. Toronto : McClelland & Stewart, 312 p.

Défense et sécurité nationale. 2013. Livre blanc. Paris : DILA. En ligne, <http:// www.livreblancdefenseetsecurite.gouv.fr/pdf/le_livre_blanc_de_la_defense_2013.pdf>. Consulté le 2 mars 2015.

Doggett, C. L. 2009. *Guide to the American Recovery and Reinvestment Act of 2009* . Congrès des États-Unis, 35 p. En ligne, <http://dcsintranet.com/ testId/images/stories/RecoveryGuidebookDoggett.pdf>.

Downing, Louise. 2014. « China Beats U.S. on Smart-Grid Spending for First Time », *Bloomberg New Energy Finance*, 19 février. En ligne, <http://www.bloomberg.com/news/articles/2014-02-18/china-spends-more-on-energy-efficiency-than-u-s-for-first-time>. Consulté le 18 novembre 2015.

Entrevue menée avec M. Jean LeDuc, responsable de la sécurité informatique chez Hydro-Québec, le 24 novembre 2014.

Ericsson, Göran N. 2010. « Cyber Security and Power System Communication – Essential Parts of Smart Grid Infrastructure », *IEEE Transactions on Power Delivery*, vol. 25, no 3, p.1501-1507.

Farwell, James P. et Rafal Rohozinski. 2012. « The New Reality of Cyber War », *Survival*, vol. 54, no 4, p. 107-120.

Farwell, James P.; Rafal Rohozinski. 2011. « Stuxnet and the Future of Cyberwar », *Survival*, vol. 53, no 1, p. 23-40.

Forster, Bruce A. 2014. « Modern Maritime Piracy: An Overview of Somali Piracy, Gulf of Guinea Piracy and South East Asian Piracy ». *British Journal of Economics, Management & Trade*, vol. 4, no 8, p. 1251-1272.

Fung, Brian. 2014. "Cyber Command's exploding budget, in 1 chart", The Washington Post, 15 janvier. En ligne, <https://www.washingtonpost.com/news/the-switch/wp/2014/01/15/cyber-commands-exploding-budget-in-1-chart/>. Consulté le 15 janvier 2015.

Gartner. s.d. « Operational Technology », IT Glossary. En ligne, <www.gartner.com/it-glossary/operationaltechnology-ot>. Consulté le 1er décembre 2014.

Geers, Kenneth. 2009. « The Cyber Threat to National Critical Infrastructures : Beyond Theory », *Information Security Journal: A Global Perspective*, vol. 18, no 1, p. 1-7.

Giacomello, Giampiero. 2004. « Bangs for the Buck: A Cost-Benefit Analysis of Cyberterrorism », *Studies in Conflict and Terrorism*, vol. 27, no 5, p.387-408.

Gharavi, Hamid; Reza Ghafurian. 2011. « Smart Grid : The Electric Energy System of the Future », *Proceedings of the IEEE*, vol. 99, no 6, p. 917-921.

Harris, Shane. 2008. « China's Cyber Militia », *National Journal*, 31 mai. En ligne, <www.nationaljournal.com/magazine/china-s-cyber-militia-20080531>. Consulté le 25 février 2015.

Hastings, John, David M. Laverty et D. John Morrow. 2014. « Securing the Smart Grid ». In *Power Engineering Conference (UPEC), 2014 49th International Universities*, 2 au 5 septembre, 6 p.

Holm, Hannes, Waldo Rocha Flores et Göran Ericsson. 2013. « Cyber Security for a Smart Grid – What About Phishing? », *2013 4th IEEE PES Innovative Smart Grid Technologies Europe (ISGT Europe*), Copenhague (Danemark), 6 au 9 octobre, 3 p.

Hu, Elise. 2014. « What Do You Do If Your Refrigerator Begins Sending Malicious Emails? », National Public Radio, 16 janvier. En ligne, <www.npr.org/blogs/alltechconsidered/2014/01/16/263111193/refrigerator-hackedreveals-internet-of-things-security-gaps>. Consulté le 15 novembre 2015.

Iyer, Gopalakrishnan et Prathima Agrawal. 2010. « Smart Power Grids », *2010 42nd Southeastern Symposium on System Theory*, Tyler (Texas, États-Unis), 7 au 9 mars, p. 152 – 155.

Jones, Sam. 2009. « Somali Pirates Hijack Oil Tanker », *The Guardian*, 30 novembre. En ligne, <www.theguardian.com/world/2009/nov/30/pirates-seize-supertanker-somalia>. Consulté le 3 novembre 2014.

Karnouskos, Stamatis. 2011. « Stuxnet Worm Impact on Industrial Cyber-Physical System Security », *IECON 2011 – 37th Annual Conference of the IEEE Industrial Electronics Society*, novembre, p. 4490-4494.

Klare, Michael T. 2012. « Energy Security », dans Paul D. Williams (éd.), *Security Studies: An Introduction*, 2e édition. Londres, New York : Routledge, p. 535-551.

Kraus, Martin. 5 juin 2013. Primary Energy Consumption in Quadrillion Btu from 1980 to 2010 by Region, données de la U.S. Energy Information Administration. En ligne, <https://en.wiki2.org/wiki/File:World_primary_energy_consumption_in_quadrillion_Btu_by_region_svg >. Consulté le 2 mars 2015.

Liang, Qiao et Wang Xiangsui. 1999. *La Guerre hors limites*. Paris : Payot et Rivages, 310 p.

Libicki, Martin C. 2011. « Cyberwar as a Confidence Game », *Strategic Studies Quarterly*, vol.5, no 1, p.132-146.

Lindsay, Jon R. 2013. « Stuxnet and the Limits of Cyber Warfare », *Security Studies*, vol. 22, no 3, juillet 2013, p. 365-404.

Madrigal, Alexis C. 2010. « Stuxnet? Bah, That's Just the Beginning », *The Atlantic*, 16 décembre. En ligne, <www.theatlantic.com/technology/archive/2010/12/stuxnet-bah-thats-just-the-beginning/68154/>. Consulté le 12 décembre 2013.

Min, Byungho et Vijay Varadharajan. 2014. « Design and Analysis of Security Attacks against Critical Smart Grid Infrastructures », *2014 19th International Conference on Engineering of Complex Computer Systems*, Tianjin (Chine), 4 au 7 août, p. 60-68.

Minkel, JR. 2008. « The 2003 Northeast Blackout–Five Years Later », *Scientic American*, 13 août. En ligne, <www.scientificamerican.com/article/2003-blackout-five-years-later/>. Consulté le 2 novembre 2014.

Nicholson, A. et collab. 2012. « SCADA Security in the Light of Cyber-Warfare ». In *Computers & Security*, vol. 31, no4, p. 418-436.

Onyeji, Ijeoma, Morgan Bazilian et Chris Bronk. 2014. « Cyber Security and Critical Energy Infrastructure ». In *The Electricity Journal*, vol. 27, no 2, p. 52-60.

Reuchlin, J.W. 2012. *Dalhousie Marine Piracy Project: The Economic Impacts of Piracy on the Commercial Shipping Industry – A Regional Perspective*. Halifax : Dalhousie University, 65 p. En ligne. <http://dmpp.management.dal.ca/wp-content/uploads/DMPP_Economic.pdf>. Consulté le 22 février 2015.

Reuters, 2 septembre. En ligne, <http//www.reuters.com/article/2009/09/02/bp-transocean-idUSN02119720090902>. Consulté le 4 novembre 2014.

Rosato, Sebastian. 2015. « The Inscrutable Intentions of Great Powers ». *International Security*, vol. 39, no 3, p. 48-88.

Sanger, David E. 2012. *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*. New York : Broadway Paperbacks, 485 p.

Sgouras, Kallisthenis I., Athina D. Birda et Dimitris P. Labridis. 2014. « Cyber Attack Impact on Critical Smart Grid Infrastructures », *Innovative Smart Grid Technologies Conference* (ISGT), Washington D.C. (États-Unis), 19 au 22 février 2014, p. 1-5.

Sieminski, Adam. 2013. International Energy Outlook 2013. Washington D.C. : Center for Strategic and International Studies. En ligne, <http://www.eia.gov/pressroom/ presentations/sieminski_07252013.pdf>. Consulté le 30 mars 2015.

Smith, Rebecca. 2014. « U.S. Risks National Blackout From Small-Scale Attack », *The Wall Street Journal*, 12 mars. En ligne, <online.wsj.com/news/articles/ SB10001424052702304020104579433670284061220>. Consulté le 20 novembre 2014.

Stefanov, Alexandru et Chen-Ching Liu. 2011. « Cyber-Power System Security in a Smart Grid Environment », *2012 IEEE PES Innovative Smart Grid Technologies*, Washington D.C. (États-Unis), 16 au 20 janvier 2012, 3 p.

Stouffer, Keith, Joe Falco et Karen Ken. 2006. *Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control System Security*. Gaithersburg, Maryland : National Institute of Standards and Technology (NIST), 164 p.

Tabansky, Lior. 2011. « Critical Infrastructure Protection against Cyber Threats », *Military and Strategic Affairs*, vol. 3, no 2, p.61-78.

The White House. 2010. *Remarks by the President to the Nation on the BP Oil Spill*, 15 juin. En ligne, <www.whitehouse.gov/the-press-office/remarks-president-nation-bp-oil-spill>. Consulté le 9 décembre 2014.

Tucker, Patrice. 2014. « Forget the Sony Hack, This Could Be the Biggest Cyber Attack of 2015 ». *Defense One*, 19 décembre. En ligne, <http://www.defenseone.com/technology/ 2014/12/forget-sony-hack-could-be-he-biggest-cyber-attack-2015/101727/>. Consulté le 26 février 2015.

U.S.-Canada Power System Outage Task Force. 2004. *Final Report on the August 14, 2003 Blackout in United States and Canada: Causes and Recommendations*, 228 p. En ligne, <energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinal-Web.pdf>. Consulté le 2 novembre 2014.

U.S. Department of Defense. 2013. *Statement of General Keith B. Alexander, Commander of United States Cyber Command Before the House Committee on Armed Services, Intelligence, Emerging Threats and Capabilities Subcommittee – 13 March 2013*. Washington D.C. : The White House, 10 p.

U.S. Department of Energy. s.d. « The Smart Home », What is the Smart Grid? En ligne, <www.smartgrid.gov/the_smart_grid/smart_home>. Consulté le 4 novembre 2014.

U.S. Department of Homeland Security. 2013. « Energy Sector », Critical Infrastructure Sectors. En ligne, <www.dhs.gov/energy-sector>. Consulté le 19 novembre 2014.

United Nations Conference on Trade and Development. 2014. *Maritime Piracy – Part I : An Overview of Trends, Costs and Trade-related Implications*. Genève et New York : Nations Unies, 39 p. En ligne, <http://eprints.soton.ac.uk/ 368254/1/dtltlb2013d1_en.pdf>. Consulté le 23 février 2015.

Warfield, Douglas. 2012. « Critical Infrastructures: IT Security and Threats from Private Sector Ownership », *Information Security Journal: A Global Perspective*, vol. 21, no 3, p.127-136

Yergin, Daniel. 2006. « Ensuring Energy Security », *Foreign Affairs*, vol. 85, no 2, p. 69-82.

La Chaire Raoul-Dandurand est une structure de développement, de formation et de diffusion de la recherche. Elle constitue une interface entre le monde scientifique et le grand public dans le domaine des études stratégiques et diplomatiques.

Les Études de la Chaire Raoul-Dandurand sont évaluées par un comité de lecture.
Les opinions exprimées dans ces Études n'engagent que la responsabilité de leurs auteurs.

Édition : Élisabeth Vallet
Révision : Céline Comtois
Conception graphique et mise en page : Isabelle Mégré

Dépôt légal – Bibliothèque et Archives nationales du Québec
ISBN : 978-2-922844-68-9
Décembre 2015