

Espionner, mentir, détruire Comment le cyberspace est devenu un champ de bataille

Martin Untersinger

Editions Grasset, 227 pages, 20,50 €



C'est à une passionnante visite du monde de la cybersécurité et de la cyberguerre que nous invite Martin Untersinger journaliste au Monde et spécialiste de ces questions. C'est un monde plein de tentatives d'espionnage, d'attaques plus ou moins destructrices et de tentatives de manipulation : en connaître les auteurs, les commanditaires et leurs motivations nécessite beaucoup d'efforts et de temps et

échoue souvent faute de preuves formelles les enquêtes n'aboutissant, le plus souvent, qu'à des incriminations plus ou moins probables.

Remarquablement informé, l'auteur évoque de nombreux cas d'attaque contre les systèmes et les réseaux informatiques, depuis la première intrusion à distance de pirates allemands détectée par un informaticien de Berkeley dans le système informatique d'une base militaire américaine en 1987 en passant par l'attaque du système informatique du ministère de l'économie à Bercy, très probablement par des chinois, puis celle du réseau de l'Élysée que les fuites d'Edgar Snowden conduisent à attribuer à des services occidentaux. Il décrit également l'attaque des centrifugeuses iraniennes par le virus Stuxnet et comment le virus Not-Petya s'est répandu via un logiciel de comptabilité ukrainien infectant le système informatique du groupe Saint Gobain.

En France on prendra pleinement conscience de la nécessité de se protéger et de pouvoir riposter à ces attaques avec le livre blanc sur la défense et la sécurité nationale de 2008 qui préconisait la création de l'agence spécialisée l'ANSSI¹ créée en 2009. Dans une première période, les espions ne font guère d'efforts pour éviter d'être identifiés, mais au fil des années, ils agissent via des intermédiaires et il devient de plus en plus difficile de le faire. De plus l'espionnage n'a pas seulement sa source chez de potentiels adversaires mais également chez ses alliés. Tous les pays tentent de se protéger des attaques mais ont des pratiques différentes quant à la publicité donnée aux attaques qu'ils ont su déjouer : vaut-il mieux les rendre publiques au risque de donner à l'adversaire des éléments sur le niveau de sa propre protection ou bien les cacher au risque de voir la population sous-évaluer les risques encourus ? Les moyens de riposter à des cyberattaques imposent aux états d'avoir des moyens humains compétents et de développer eux-mêmes des virus qui, le moment venu, pourront être utilisés. Ils exploitent des vulnérabilités résiduelles dans les systèmes les plus répandus : leur identification est devenue une activité commerciale. Faut-il garder pour soi une vulnérabilité pour l'utiliser pour de futures attaques ou bien la rendre publique pour qu'elle soit corrigée ? L'ouvrage développe de façon très documentée toutes ces questions. Un ouvrage à lire par tous ceux qui s'intéressent au numérique. **PC**

¹ ANSSI : Agence nationale de la sécurité des systèmes d'information

Le mur énergétique français Le rapport accablant sur 30 ans d'erreurs politiques

Antoine Armand

Editions Stock, 336 pages, 24,00 €



Ce livre est issu d'une commission parlementaire qui a pour mission de parler

Armand a

les raisons de la

d'indépendance énergétique.

En effet fin 2022 le gouvernement alertait sur les risques de coupures d'électricité durant l'hiver qui arrivait. Ces alertes intervenaient dans un contexte international particulier marqué par la guerre d'Ukraine

et la crise énergétique qui s'ensuivit ainsi que la faible disponibilité de nos centrales nucléaires. La vulnérabilité de la France et l'atteinte à sa souveraineté éclatait au grand jour et entraînait une prise de conscience chez un certain nombre de députés qui demandèrent la création d'une commission d'enquête pour déterminer comment le pays qui était fier de son système de production d'électricité en était arrivé à rationner l'électricité durant l'hiver.

Le livre est divisé en trois parties, la première reprend le titre et expose de manière claire avec de nombreux tableaux l'évolution de la demande d'énergie et détaille les dépendances toujours importantes vis à vis des énergies fossiles et la fragile production d'énergie verte matérialisée par un chapitre sous-intitulé le mythe de l'indépendance énergétique. Le mur énergétique est défini par le dernier chapitre de cette première partie à partir de l'objectif d'atteindre la neutralité carbone en 2050 ce qui représente une transition industrielle inédite. La deuxième partie intitulée « trente ans de divagation » traite en trois chapitres chronologiques partant de 1990 ce qui a provoqué la situation actuelle. La troisième partie propose des solutions réalistes s'appuyant sur des avancées technologiques pour mener à bien la transition énergétique.

Le livre est ponctué de nombreux encadrés présentant les interventions des industriels, politiques et spécialistes qui répondent aux questions de la commission. Les interventions montrent des politiques soucieux de justifier leurs actions alors qu'il apparaît aujourd'hui qu'elles ont été néfastes. Certaines décisions comme l'abandon de Superphénix et l'arrêt du développement du réacteur de quatrième génération Astrid semblent des décisions guidées uniquement par l'idéologie antinucléaire et apparaissent comme telles dans les réponses des politiques qui les ont actées. Ces derniers points sont particulièrement développés et montre que la versatilité de l'action politique est incompatible avec les grands programmes industriels. La vision des auditions avait été relayée par la presse et les réseaux sociaux et ce livre complète de manière très efficace et pédagogique le travail de la commission dont le rapporteur, auteur du livre, est aujourd'hui ministre de l'économie. C'est donc une lecture très éclairante et documentée sur les trente dernières années de politique énergétique. **ML**