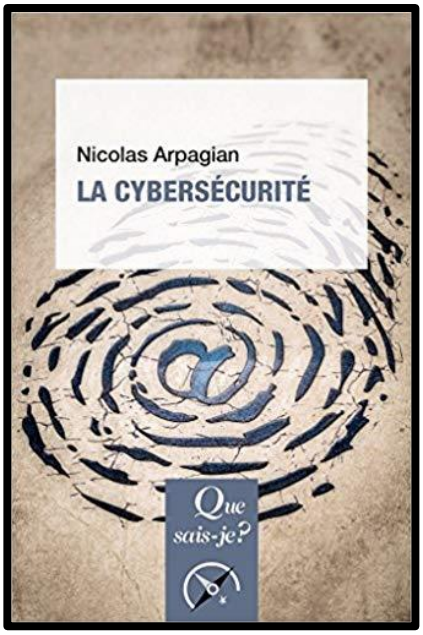
LA CYBERSECURITE

N. Arpagian. Presses universitaires de France, 2018, 128 p.

Cécile Coste, Manon Charrier, Naomie Desfontaines,
Kodjo A. Assigbe, Stéphan Poinsignon



INTERNET, SOURCE DE VULNERABILITE

Les diverses utilisations de l'internet génèrent à chaque instant, volontairement ou non, une quantité importante de données. L'organisation en réseau d'Internet engendre des possibilités infinies de pénétration des systèmes informatiques et transpose ainsi la criminalité vers le web. Le présent ouvrage, écrit par Nicolas Arpagian, vise à susciter une prise de conscience concernant les risques encourus par les usagers d'Internet. *Cybersécurité* expose les différentes formes de criminalités qui envahissent le web et qui se perfectionnent au fur et à mesure de l'évolution technologique. L'auteur distingue différents niveaux de vulnérabilité des systèmes informatiques qui affectent les citoyens, les organisations et les États.

Selon l'auteur, les défaillances de la cybersécurité sont dues à son morcellement. Actuellement, chaque entité (organisation, État, etc.) lutte contre les attaques informatiques à sa manière, compte tenu de ses moyens. Nicolas Arpagian préconise une gestion collective ainsi que des actions concertées afin de prévenir efficacement les risques informatiques. Nous présenterons, dans une première partie, les différentes catégories de cyberattaques dont sont victimes les particuliers et les organisations. Ensuite, nous aborderons les mesures prises par les États en matière de cyber sécurité. Nous évoquerons notamment le cadre législatif européen.

NICOLAS ARPAGIAN – EXPERT EN CYBERSECURITE

Nicolas Arpagian est un expert de l'intelligence économique et de la protection des données. Il travaille aujourd'hui principalement pour Orange Cyberdéfense, en tant que

directeur de l'entité dédiée à la sécurité des entreprises. Il intervient aussi régulièrement auprès des entreprises afin de les sensibiliser aux enjeux de la cybersécurité. Rédacteur en chef de la revue Prospective Stratégique, il enseigne la cybersécurité, la cybercriminalité, le lobbying européen ou encore le management de l'information stratégique dans plusieurs universités de France. Annuellement, il organise le colloque TIC & Géopolitique, dont il est modérateur. Nicolas Arpagian a publié plusieurs ouvrages afin de lever le voile sur les dangers du numérique. *La Cybersécurité* s'inscrit dans cette perspective et confirme la volonté de l'auteur d'informer le grand public sur les enjeux de la sécurité numérique.

PRESENTATION DE L'OUVRAGE

Dans son ouvrage, l'auteur révèle les différents types d'attaques auxquelles nous, usagers de l'internet, sommes exposés. Il explique la manière dont des particuliers se font arnaquer ou rançonner, notamment par des techniques de *phishing* et de *revenge porn*. La cybercriminalité affecte aussi les entreprises et peut s'opérer par la manipulation de leurs informations afin de ternir leur réputation. De même, des informations leur sont dérobées et peuvent être revendues à des entreprises concurrentes. Selon Nicolas Arpagian, les structures étatiques sont également concernées par ces attaques. Les systèmes de gestion de l'information et les installations stratégiques des États sont souvent la cible des hackers et même d'autres d'États. Mais, les États sont aussi confrontés au cyberterrorisme, car l'internet est devenu un moyen de propagande et de recrutement pour ces criminels.

Ainsi, afin d'assurer la sécurité du territoire et des citoyens, les agences gouvernementales surveillent les réseaux informatiques et n'hésitent pas à utiliser les technologies dites du *big data*. Les faiblesses de la législation en matière de cybersécurité sont peu à peu comblées. De nombreuses organisations internationales et non gouvernementales s'y investissent et des agences de coopération internationale contre la cybercriminalité sont créés, en particulier, dans le contexte européen. Toutefois, elles sont souvent confrontées aux problèmes de territorialité et aux longues procédures diplomatiques et judiciaires.

INTERNET, LES CITOYENS ET SES DANGERS

Actuellement, l'utilisation d'Internet est permanente. Que ce soit par le biais de nos téléphones portables, ordinateurs, tablettes, GPS et même les objets connectés à l'intérieur de la maison. L'ensemble des outils nous entourant sont reliés entre eux et connectés à Internet, pouvant alors générer des problèmes divers. Dans son ouvrage, l'auteur nous livre de nombreux exemples poignants de cyberattaques subies par des particuliers.

L'ACTUALITE DRAMATIQUE SOURCE DE FRAUDE

Lors du tsunami survenu en Asie en décembre 2004, du tremblement de terre en Haïti en janvier 2010, ou encore lors des attaques terroristes pendant le marathon de Boston en avril 2013, de fausses collectes d'argents et de données personnelles ont été organisées. À la suite de ces événements tragiques, de nombreux citoyens ont renseigné des informations personnelles sur des formulaires en ligne et offert d'importantes sommes d'argent en croyant bien faire. Les escrocs ont joué et jouent encore sur ce que l'auteur appelle la "compassion générale". Ce type d'escroquerie est basé sur l'envoi massif de mails, faisant appel à la générosité des internautes sous couvert du titre fictif d'une institution officielle qui crédibilise le message.

L'ATTAQUE A LA NIGERIANE

« L'attaque dite 'à la nigériane' reste un grand classique. Une jeune Africaine - veuve ou orpheline - vous adresse un message de détresse. Elle vous a opportunément choisi pour l'aider à la faire sortir du pays - en échange d'un pourcentage - les millions de dollars de son héritage familial. [...] » Nul besoin de finir cette citation pour comprendre que ce fameux héritage n'existe pas et que les individus crédules ne reverront jamais l'argent avancé. Tous les jours, de nombreux mails frauduleux de ce genre sont envoyés massivement dans l'espoir que quelqu'un « morde à l'hameçon ».

LES ENTREPRISES ET LES ATTAQUES INFORMATIONNELLES

Les entreprises sont confrontées à un certain nombre de risques informatiques qui peuvent porter préjudice à leur réputation. C'est le cas pour Google, Intel, Coca-Cola, Disney ou encore Louis Vuitton. Toute atteinte à la réputation de ces marques peut mettre en péril leur valeur financière comme symbolique. Elles s'avèrent particulièrement vulnérables aux campagnes de dénigrement. À titre d'illustration, en 2009, des vidéos montrant des salariés de la chaîne Domino's Pizza en train de dégrader des plats à livrer avaient été largement relayées sur les réseaux sociaux.

D'autre part, certaines entreprises commettent des actes illégaux afin de faire de l'ombre à leurs rivaux. Pour exemple, le groupe Samsung Electronics avait financé des internautes afin qu'ils publient, de manière anonyme, des commentaires négatifs à l'encontre de son concurrent, la société de fabrication HTC. En octobre 2013, l'autorité de la concurrence de Taïwan (Taiwan's Fair Trade Commission) avait alors condamné le groupe Samsung pour avoir conduit cette campagne de dénigrement sur le net.

Les entreprises peuvent également être victimes d'usurpation d'identité sur les réseaux sociaux. Entre la publication de faux communiqués de presse et d'articles mensongers sur leur site web, les entreprises ne sont plus à l'abris des attaques rendues possibles par l'internet. Si les entreprises doivent veiller à la préservation de leur réputation, elles

doivent également garantir la protection de leurs données. Confier la gestion de leurs serveurs et de leurs bases de données à des sous-traitants ne constitue pas le moyen le plus fiable pour se protéger des attaques.

CYBERGUERRE ETATIQUE

Le cyberespace constitue aujourd'hui un terrain d'affrontement entre États au même titre que la terre ou l'air. Pour ces acteurs, la cybersécurité représente un enjeu nécessaire au maintien de leur souveraineté. À travers de nombreux exemples, Nicolas Arpagian détaille les cyber menaces auxquelles les États sont confrontés.

ATTAQUES NUMERIQUES ET OPINION PUBLIQUE

À l'échelle d'un pays les assauts numériques peuvent avoir des conséquences désastreuses pour l'opinion publique et l'organisation d'une société. Ici, l'auteur met en garde contre les possibilités d'utiliser les attaques numériques comme complément d'attentats réels.

Les Systèmes de Contrôle et d'Acquisition de Données (SCADA) permettent notamment de piloter les équipements techniques des transports d'une ville. Selon Nicolas Arpagian, un attentat dans le métro du centre-ville pourrait s'accompagner d'attaques numériques, via le piratage des SCADA. Les pirates pourraient être en mesure de contrôler à distance, grâce aux SCADA, les feux de signalisation et ainsi provoquer la panique sur les axes routiers. Les conséquences s'enchaîneraient alors, l'intervention des secours serait plus difficile et le bilan des victimes de l'attentat s'alourdirait. Des images chocs seraient alors relayées par les médias et les réseaux sociaux… L'opinion publique prendrait alors conscience de l'incapacité des autorités à assurer la sécurité et à protéger la collectivité contre ce type d'attaque. Dans la cyberguerre, la prise de contrôle de ces systèmes devient stratégique. En effet un dérèglement peut entraîner des pertes à la fois humaines, économiques, environnementales mais aussi susciter des émotions fortes et façonner le débat public.

LA TECHNOLOGIE COMME SOUTIEN POLITIQUE

L'auteur évoque les cyberattaques qui ont frappé l'Estonie et de la Géorgie. Dans ces cas précis, les attaques ont été mises au profit d'un jeu diplomatique et géopolitique.

En 2007, l'Estonie s'est trouvée au centre de la première génération de cyberguerre de grande ampleur. Suite à d'importants conflits au sein de la population et d'émeutes, une série d'opérations de déni de services a été orchestrée dans le but d'amplifier les protestations. Les sites institutionnels ont été détournés et certaines pages d'accueil des sites ministériels estoniens étaient occupées par des portraits d'Hitler. L'Estonie, qui a

très vite pris le tournant du tout-numérique et a privilégié l'Internet pour son développement économique et administratif, fut totalement paralysée.

Un an plus tard, les sites Internet de la présidence de la République de Géorgie et les sites des principaux médias ont été attaqués par des « ordinateurs zombies ». Cette attaque avait pour but de montrer combien il était facile de pirater et contrôler des systèmes informatiques gouvernementaux. Dans les cyberguerres étatiques, les responsables sont difficilement identifiables, pourtant ici la Russie était toute désignée. En effet, ce pays semble responsable de beaucoup d'attaques informationnelles ou d'espionnage. L'auteur fait d'ailleurs référence au rapport annuel de l'Agence de janvier 2018 désignant la Chine et la Russie comme étant à l'origine des principales cyber menaces étatiques.

LA LEGISLATION D'INTERNET

Du fait de la dimension internationale du réseau internet, son encadrement judiciaire est très compliqué. Selon Nicolas Arpagian, les États auraient un rôle majeur dans la régulation et la prévention des risques numériques.

UNE LEGISLATION PRINCIPALEMENT EUROPEENNE

D'après l'auteur, l'Europe serait leader en termes de législation internationale du numérique. En effet, le Conseil de l'Europe considère que « la cybercriminalité constitue une menace pour la démocratie et l'État de droit ». Un des principaux textes fut la convention de Budapest du 23 novembre 2001 sur la cybercriminalité. Ce texte a été signé par les 45 États membres et seuls la Suède et l'Irlande ne l'ont pas ratifié. En revanche, les États-Unis l'ont signé également mais pas la Russie qui ne juge pas utile de le signer.

En 2013, au sein d'Europol, le Centre européen de lutte contre la cybercriminalité (EC3) a été créé. Ainsi, les policiers de chaque États membres évitent de passer par les voies diplomatiques ou judiciaires et saisissent directement L'EC3, afin de rendre les enquêtes et actions contre les cybercriminels plus rapides et plus efficaces.

L'Union européenne dispose, depuis 2004, de l'ENISA (European Network and Information Security Agency) qui a pour objectif de sécuriser le réseau et les informations. En réalité, cette agence ne dispose que de 10 millions d'euros de budget annuel, ce que l'auteur juge dérisoire compte tenu de la tâche qui incombe à cette institution. Récemment, l'Union Européenne a établi le Règlement Général sur la Protection des Données (RGPD) qui renforce la cybersécurité au sein de l'Union Européenne.

À travers l'exemple de l'Estonie, on s'aperçoit que les cyberattaques peuvent ne pas être prises au sérieux par les gouvernements. Suite à l'attaque, le pays a invoqué l'article 5 du traité de l'OTAN qui prévoit une intervention militaire des pays européens si un des états membres est attaqué. Aucun allié ne lui est venu en aide car, à cette époque, les

cyberattaques n'étaient pas considérées comme de potentielles menaces de guerre. Depuis cet incident, l'OTAN a réagi et a mis à jour sa politique sur les cyberguerres.

DES TEXTES LEGISLATIFS MAIS PEU D'ACTES

En dehors du cadre européen, la coopération internationale reste très lente et s'avère souvent inefficace. En effet, les procédures judiciaires et diplomatiques se révèlent complexes et laborieuses, comparées à la rapidité des actes illégaux commis par les cyber criminels. Ces derniers ont largement le temps d'opérer puis de disparaitre avant que les relations internationales n'aboutissent.

En 2010, le secrétaire général de l'Union Internationale des Télécommunications (UIT), Hamadou Traoré a proposé un traité international sur la cybersécurité. En 2017, le G7 a entamé des négociations sur une éventuelle responsabilité internationale contre les cyberattaques, mais les mots sont restés sur le papier. Dans les actes, aucune réelle mesure n'a été mise en place car, selon l'auteur, les États craindraient de perdre leur liberté d'agir sur internet. En effet, comme le livre le montre, les États utilisent Internet dans leur propre intérêt et certains usent de cette arme pour porter directement atteinte à leurs adversaires.

Cependant, il faut souligner que quelques actions internationales ont été menées. L'UIT, dans le cadre d'un sommet de l'ONU, a lancé le programme IMPACT (International Multilateral Partnership Against Cyber-Terrorism) qui, comme son nom l'indique, est un programme international contre le cyber terrorisme. L'UIT a aussi développé un programme de protection de l'enfance en ligne : COP (Children Online Protection). Le G8 participe aussi à la lutte contre la cybercriminalité, même si les mesures ne sont pas à la hauteur des crimes commis sur la toile. Dès 1997, un réseau de communication opérationnel 24h sur 24 et 7 jours sur 7 a été mis en place par le sommet afin que les États membres puissent réagir immédiatement en cas de cyberattaque.

CONCLUSION

L'ouvrage de Nicolas Arpagian appelle à une prise de conscience collective face à l'augmentation du nombre de personnes touchées par les attaques. Les professionnels et les particuliers étant largement amenés à utiliser les outils numériques, il leur incombe d'être vigilants et de mettre en place des mesures préventives. Les organisations devraient ainsi jouer un rôle essentiel en invitant toutes leurs parties prenantes (fournisseurs, clients, partenaires) à surveiller davantage leurs systèmes d'informations. Il en va de même pour les États.

Cet ouvrage fut très intéressant à lire. Les explications fournies par l'auteur et enrichies par des exemples marquants permettent de sensibiliser le grand public aux différents dangers du numérique.