Études internationales

Cyberattaque et cyberdéfense, Daniel VENTRE, 2011, Paris, Lavoisier, 312 p.

Laurence Basset

Volume 43, Number 3, September 2012

URI: https://id.erudit.org/iderudit/1012824ar
DOI: https://doi.org/10.7202/1012824ar

See table of contents

Publisher(s)

Institut québécois des hautes études internationales

ISSN

0014-2123 (print)
1703-7891 (digital)

Explore this journal

Cite this review

Basset, L. (2012). Review of [*Cyberattaque et cyberdéfense*, Daniel VENTRE, 2011, Paris, Lavoisier, 312 p.] *Études internationales*, *43*(3), 476–478. https://doi.org/10.7202/1012824ar

À cela s'ajoute une partie sur le désarmement. En ce qui concerne la partie « développement », elle est conjuguée dans le champ économique et dans l'espace social. Matières très larges – entre service postal international et désertification, entre sécurité nucléaire et personnes handicapées, entre propriété intellectuelle et réchauffement de la planète –, mais aussi matières souvent peu connues dans leur association avec l'ONU. Bien entendu, les droits de l'homme sont mis également en avant, tout comme les services de protection internationale et d'assistance fournis aux réfugiés.

Certes, l'ouvrage peut être lu de différentes manières. On peut le voir comme un livre de référence officiel à forte composante documentaire. On peut aussi le lire comme un texte promotionnel très lisse, sans autocritique. En ce qui concerne par exemple le Conseil de sécurité, on ne fait pas expressément mention des difficultés susceptibles de surgir lors d'atteintes graves aux droits de l'homme dès lors qu'un ou plusieurs États imposent leur veto. Maints exemples concrets illustrent cet état de fait, mais ne sont pas repris dans le présent *ABC*. De même, autour de la responsabilité de protéger, l'encadré ne décrit pas les arguments sur tel ou tel positionnement des États à ce sujet lorsqu'ils refusent d'intervenir. *A contrario*, lorsqu'il s'agit de présenter les zones d'intervention de l'ONU dans le monde avec la description des missions, les analyses sont plus précises, les difficultés rencontrées plus évidentes et les bilans plus critiques. En vérité, il faudrait entamer une étude pointue pour déterminer les champs de visibilité, la diplomatie publique onusienne et les informations « dissimulées » afin d'avoir une vision précise de la pertinence politologique du document, qui, néanmoins, reste une référence officielle et, en cela, a sa place dans chaque bibliothèque.

Bien évidemment, l'*ABC des Nations Unies* se situe en partie, selon les thématiques abordées, dans un cadre temporel précis. Ce genre d'ouvrage doit assez régulièrement être actualisé. C'est ce qui a été fait avec la présente édition, qui en verra d'autres lui succéder. Ce qui ne peut qu'améliorer la connaissance de cette grande organisation mondiale, à la condition évidemment que les chercheurs et les lecteurs approfondissent avec d'autres sources les thématiques ici abordées.

André DUMOULIN
Université de Liège

ÉTUDES STRATÉGIQUES ET SÉCURITÉ

Cyberattaque et cyberdéfense

Daniel VENTRE, 2011, Paris, Lavoisier, 312 p.

La guerre de l'information, qu'elle soit militaire ou économique, comme la cyberdélinquance, ainsi que les stratégies de dominance informationnelle ou le cyberterrorisme occupent de plus en plus régulièrement le premier plan de l'actualité et posent – entre autres – des questions de libertés publiques. La défense de la Nation contre tous les types d'attaques cybernétiques, quel que soit d'ailleurs le vocabulaire employé (il s'agit bien de tout ce qui touche au cyberespace, au non-visible), la défense de la Nation, donc, est devenue un élément essentiel de la politique nationale et internationale des États. Il semble qu'il ne soit plus l'heure de se demander si une attaque informationnelle est probable

ou non, ni même de savoir si cela constituerait un instrument stratégique efficace. Il est acquis que cette menace est réelle et que les pays doivent adapter leurs stratégies de défense aux armes nouvellement créées et de plus en plus diffusées dans le monde.

D'ici à 2020, le cyberespace devrait générer – notamment par le commerce électronique – entre trois et quatre trillions de dollars. Devant cette croissance effrénée, le cyberespace se positionne progressivement au centre des activités créatrices de richesse dans le monde et il n'est désormais plus possible d'ignorer le formidable facteur de vulnérabilité que les nouvelles technologies de l'information induisent pour les États et leur population. L'augmentation de l'utilisation de ces nouvelles technologies accroît la quantité de failles « mises au service » d'ennemis potentiels, de même que leur vulnérabilité.

L'ouvrage de D. Ventre définit très bien les différentes conceptions que l'on peut trouver des acceptions « cyberespace », « cybernétique », « cyberdéfense », « cyberguerre »... En y consacrant plusieurs chapitres, l'auteur s'assure que tous les aspects sont abordés.

On a coutume de considérer que, depuis le 11 septembre 2001, tout a changé dès lors qu'il est question de concept militaire. Combien d'ouvrages ont été consacrés aux évolutions forcées ou supposées des aspects de défense nationale après les attaques sur le sol américain ? Parmi tous les concepts qu'il a fallu revoir, celui du cyberespace est progressivement apparu comme un des aspects importants de cette évolution théorique. En effet, la notion de cyberespace se confond largement avec Internet : il représente donc tout à la fois la masse, toujours en croissance, des connaissances humaines, mais aussi une structure particulière où tout est directement ou indirectement relié à tout, puisque les informations se renvoient les unes aux autres.

La première partie est un peu longue mais très bien documentée. Elle construit par exemple une étude sur la représentation qu'ont les internautes des notions étudiées dans le livre, sur la base des résultats de recherche dans Google, en français et en anglais. Les deux parties suivantes sont essentielles pour recadrer les différentes notions. Elles s'attaquent tour à tour aux notions de cyberattaque et de cyberdéfense. L'étude est poussée, enrichissante.

Les deux derniers chapitres de l'ouvrage sont sans aucun doute les plus intéressants pour qui connaît déjà les différents concepts dont il est question ici. En effet, l'auteur aborde les notions de cyberattaque et de cyberdéfense d'un point de vue stratégique : la comparaison entre le cyberespace et l'espace sous-marin est novatrice. Les analogies entre ces deux domaines sont riches de sens et l'identification de points communs permet de mettre en perspective la notion de cyberespace. Le débat traditionnel autour de ce sujet est de savoir si l'on peut parler de cyberguerre, qui viendrait remplacer la guerre traditionnelle en se portant sur un autre terrain, ou si le cyberespace deviendrait un autre moyen de se battre, d'autres armes au service d'une même cause, avec une stratégie militaire propre, induites par les caractéristiques mêmes de l'arme (on n'emploierait pas un char à la place d'un avion : à chaque objectif sa capacité). Il semble

plus mesuré de penser que le terrain du cyberespace deviendrait un nouvel espace de combat, comme le fond des mers l'est devenu avec la construction des premiers sous-marins.

Tout comme les populations situées dans les zones de guerre se sont habituées, à partir des années 1920, à voir apparaître des avions – nouvelles capacités d'atteindre l'ennemi en profondeur et accessoirement d'étendre le champ de bataille au-delà des limites historiques et ainsi d'augmenter les risques d'erreur de frappes, créant des dommages collatéraux parmi les populations des alentours –, les habitants des espaces reliés entre eux par des réseaux informatiques et reposant sur le même protocole de communication s'habitueront, dans les moments de conflits, à voir leurs habitudes changer.

Les attaques peuvent prendre des formes diverses : attaques de masse, piratage informatique de données de haute sécurité, intrusion dans des centrales nucléaires… Les exemples foisonnent dans le monde depuis quelques années. Cependant, même si les avis d'experts varient quant à ce que l'on peut ou non considérer comme un cas de cyberattaque, tous ces évènements mettent en perspective un point essentiel : le manque de prévisibilité de ces actions. Désormais en effet, n'importe quel pays est susceptible de faire l'objet d'une série d'attaques cybernétiques mettant en péril sa stabilité intérieure et donc la sécurité de son territoire et de sa population.

La qualité de l'ouvrage n'est pas à remettre en cause : l'auteur étaye généralement ses propos de nombreux exemples, de sources variées (on y trouve même des références à Wikipédia...) et les nombreuses représentations graphiques illustrent bien sa pensée. Cela facilite l'intégration dans notre quotidien de ce nouveau mode de guerre qui – à n'en pas douter – s'étendra à toute notre modernité.

Laurence BASSET
Mariusa Consulting

MONDIALISATION

Immigrant Politics. Race and Representation in Western Europe

Terri E. GIVENS et Rahsaan MAXWELL (dir.), 2012, Boulder/Londres, Lynne Rienner Publishers, 179 p.

Mettant à contribution de nombreux universitaires européens et états-uniens issus de la science politique et des sciences sociales, cet ouvrage collectif se penche sur la question de l'intégration politique des immigrants en Europe de l'Ouest en se focalisant sur la représentation politique des minorités issues de l'immigration en Grande-Bretagne, en France, en Allemagne et aux Pays-Bas. Le livre situe cette question dans le contexte d'une conception de plus en plus négative de l'immigration dans le discours politique. Plusieurs questions traversent l'ensemble des chapitres, conférant à ce livre une cohérence interne remarquable pour un ouvrage collectif : Pourquoi la représentation politique des minorités connaît-elle depuis peu une croissance ? Quels rôles y jouent les facteurs conjoncturels et la mobilisation de base ? Pourquoi les partis politiques majeurs souhaitent-ils se diversifier et quel est le rôle politique des représentants des minorités ? En plus des analyses empiriques nationales, l'intérêt de l'ouvrage réside dans sa contribution sur le plan théorique,