Études internationales

Michael P. Gallaher, Albert N. Link et Brent R. Rowe, *Cyber Security Economic Strategies and Public Policy Alternatives*, 2008, Cheltenham, Edward Elgar, 266 p.

Hugo Loiseau

Volume 40, Number 1, mars 2009

Carl Schmitt et les relations internationales

URI: https://id.erudit.org/iderudit/037585ar
DOI: https://doi.org/10.7202/037585ar

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

Loiseau, H. (2009). Review of [Michael P. Gallaher, Albert N. Link et Brent R. Rowe, *Cyber Security Economic Strategies and Public Policy Alternatives*, 2008, Cheltenham, Edward Elgar, 266 p.] *Études internationales*, *40*(1), 145–147. https://doi.org/10.7202/037585ar

moment. Et de montrer au passage à la Maison Banche que Moscou ne craignait plus les rapports de force avec les États-Unis et ses alliés européens.

Quant à la poudrière du Moyen-Orient, les auteurs décrivent une situation en trompe-l'œil. Malgré les apparences, l'année 2008 recèle bien des dangers pour l'avenir. Il serait naïf, expliquent-ils, de croire que la situation est calme. Le désintérêt de la communauté internationale qu'il déplore pourrait déboucher sur un chaos incontrôlable. Car les guerres de factions menacent plus que jamais. Moins visibles, moins spectaculaires, mais tout aussi dangereuses pour la stabilité de la région : l'Irak bien sûr où les forces d'Al-Qaïda faiblissent face au « réveil » de la communauté sunnite ; le Liban qui n'a pas su consolider sa cohésion nationale ; le conflit israélo-arabe qui n'en finit pas de pourrir ; les Palestiniens qui se déchirent entre partisans du Hamas et fidèles du Fatah, sans parler de la Turquie dont la démocratie tangue dans le débat sur la laïcité… autant de petites bombes à retardement, préviennent les auteurs, que les grandes puissances doivent prendre en compte.

Au final, cet ouvrage affiche un objectif ambitieux difficilement atteint du fait même de l'objet de l'étude, extrêmement mouvant. Le livre, essentiellement découpé par aire géographique (la Russie et les Balkans, la sécurité européenne, l'instabilité asiatique, le Moyen-Orient, l'Afrique subsaharienne, le narcoterrorisme en Amériques…), parvient tout de même à résumer les principales causes des conflits ainsi qu'à décrire la position des acteurs engagés. Il fournit un éclairage général sur chacun d'eux qui satisfera le lecteur averti, mais frustrera sans doute le spécialiste. Il est difficile en moins de 260 pages d'entrer dans les détails de tous ces conflits. D'où l'impression parfois de lire un excellent compte rendu journalistique plus qu'une étude approfondie. Pour les prochaines éditions, les responsables seraient inspirés de fournir au lecteur des cartes qui permettent de se repérer parmi les différentes revendications territoriales des acteurs.

Ali LAÏDI

Institut de relations internationales et stratégiques (IRIS) et France 24

Cyber Security Economic Strategies and Public Policy Alternatives

Michael P. GALLAHER, Albert N. LINK et Brent R. ROWE, 2008, Cheltenham, Edward Elgar, 266 p.

Le programme de recherche sur la cybersécurité est en pleine émergence actuellement. Bien que profondément multidisciplinaire, ce programme de recherche touche directement les études internationales et l'analyse des politiques publiques. Le livre de Gallaher et de ses collègues s'adresse plus au lectorat de l'analyse des politiques publiques qu'à celui des études internationales. Ce livre enrichit avantageusement la littérature sur l'analyse de prise de décision relativement à la menace cybernétique à l'intérieur des institutions publiques et des entreprises privées. Il rassemble à la lumière d'un cadre théorique original une multitude de connaissances techniques, administratives, technologiques et politiques autrement dispersées.

Sans en faire un résumé exhaustif, disons que ce livre porte sur trois éléments essentiels qui synthétisent de façon pertinente l'ensemble de son contenu. Il s'agit de l'approche théorique de la cybersécurité par l'analyse de la prise de décision, de la diversité des

pratiques organisationnelles par rapport à la cybersécurité qui a été révélée par les auteurs et du rôle des gouvernements dans la sécurisation du cyberespace. L'objectif général de l'ouvrage est de présenter la première analyse systématique du développement des enjeux inhérents au cyberespace et du rôle qu'ont à jouer les gouvernements dans la préservation des infrastructures critiques. À cette fin, les auteurs amorcent leur ouvrage par la création d'une approche théorique originale. Cette approche est axée sur les études de cas tirées des rencontres avec une centaine d'entreprises ou d'institutions publiques situées aux États-Unis et des entrevues de leurs dirigeants. À partir de la somme d'informations générée par ces rencontres, les auteurs établissent une série de tendances et de stratégies qu'adoptent les institutions visitées en matière de sécurisation des infrastructures liées au cyberespace. À l'aide de l'interprétation des tendances et des stratégies, autrement dit de leurs forces et de leurs faiblesses, les auteurs proposent plusieurs recommandations et politiques publiques aux différents acteurs du milieu. Par exemple, les auteurs exposent au quatrième chapitre les deux stratégies générales habituellement adoptées par les institutions, la stratégie d'investissement et celle de la mise en œuvre, et les deux grandes tendances observées, l'approche proactive et l'approche réactive en matière de cybersécurité. En vertu de la gestion du risque et de la tolérance à ce même risque, les dirigeants et les techniciens responsables de la sécurité informatique doivent composer avec de nombreuses contraintes, dont le budget et l'ampleur de l'institution, dans leur stratégie de sécurité cybernétique. De plus, les auteurs ont remarqué que, même si les institutions qui sont proactives en matière de cybersécurité sont moins vulnérables aux menaces en provenance du cyberespace, la majorité des institutions préfèrent adopter un comportement réactif, car c'est beaucoup plus rentable financièrement. La principale conclusion du livre propose que la cybersécurité est un bien public qui laisse voir deux failles de marché importantes : 1) l'absence d'informations fiables et peu onéreuses sur lesquelles les institutions peuvent baser leurs décisions en matière de cybersécurité et 2) les coûts externes d'une brèche de sécurité qui rejaillissent sur les autres institutions et les consommateurs. Les principales recommandations des auteurs pour les gouvernements ont pour objectif d'éliminer ou de diminuer ces deux failles qui freinent le développement de la cybersécurité. Entre autres, ils recommandent d'améliorer le financement des organismes étasuniens chargés de l'élaboration de normes de sécurité communes, la collecte et la distribution d'informations gratuites et accessibles à propos de la cybersécurité, de même que la redistribution des coûts de la sécurité parmi l'ensemble des acteurs concernés. Toutes ces recommandations ont pour but de favoriser l'investissement privé dans la sécurisation des réseaux. Par la suite, dans la seconde partie du livre, les auteurs font valoir leurs recommandations au moyen de quatre études de cas portant sur l'implantation de normes et de protocoles de sécurité dans diverses institutions aux États-Unis.

Il s'agit d'un livre original qui est très complet à propos des risques associés aux développements du cyberespace et des vulnérabilités des réseaux de communication contemporains, notamment Internet. Les auteurs passent en revue tous les protocoles existant aux États-Unis et signalent les faiblesses

générales en matière de cybersécurité dans ce pays. Les conséquences sur la cybersécurité des tensions entre le secteur public et le secteur privé, le premier régulant l'autre, sont bien expliquées tout au long de l'ouvrage. Toutefois, un reproche qu'il est possible de faire concerne l'approche adoptée par les auteurs, qui concentrent leur analyse exclusivement sur les États-Unis. Cette approche est paradoxale, car la nature même du cyberespace est décentralisée et internationale. Par exemple, ils ne font aucunement référence aux normes ISO qui ont été établies par l'Organisation internationale de normalisation. Ils évacuent la dimension internationale et l'aspect, plus intéressant pour les internationalistes et les politologues, de l'impact du cyberespace et de la vulnérabilité des systèmes informatiques dans l'occurrence des guerres et le déplacement des conflits dans une dimension supplémentaire aux théâtres conflictuels habituels. Les auteurs ne s'inspirent pas des études sur la sécurité et proposent une vision presque exclusivement managériale du phénomène, ce qui diminue la portée explicative des conclusions du livre. Enfin, l'ouvrage tombe parfois dans des descriptions très techniques, à la limite du superflu, qui peuvent faire perdre le fil conducteur du chapitre ou de la partie concernée et qui amoindrissent la force de l'argumentation qui y est développée.

Hugo LOISEAU

École de politique appliquée
Université de Sherbrooke

War as Business. Technological Change and Military Service Contracting

Armin KRISHNAN, 2008, Aldershot, Ashgate Publishing, 207 p.

Parmi les transformations qu'a connues la politique globale depuis la fin des années 1990, certaines ont pris plus de temps à apparaître sur le radar des chercheurs en études de la sécurité. La privatisation de la sécurité, de la guerre et des *services* permettant la conduite des opérations militaires a fait partie de ces zones d'ombre. Pas plus les analyses discursives que les théories critiques en économie politique internationale n'ont accordé un grand intérêt à ces processus durant les années 1990. Toutefois, leur croissance soutenue a reçu une attention plus systématique depuis la guerre en Irak. Cela, malgré le fait que l'ampleur du phénomène ne soit pas toujours aisément quantifiable. L'ouvrage d'Armin Krishnan cherche à éclairer cette zone d'ombre. *War as Business. Technological Change and Military Service Contracting* est une contribution aux études de la sécurité qui propose d'analyser la privatisation du secteur des services liés à la sécurité et à la défense. L'ouvrage contribue également à l'économie politique et aux études stratégiques.

War as Business cherche à étayer la thèse selon laquelle le rythme singulier de la croissance du recours à la privatisation des services militaires repose sur la croissance de la complexité des technologies militaires. Une partie de l'introduction de l'ouvrage effectue un survol succinct de cette croissance de la guerre, du Vietnam à aujourd'hui, en passant par les doctrines stratégiques américaine (*AirLand Battle* et *Follow-on-Forces Attack*) et soviétique, la guerre du Kippour (1973) et la guerre du Golfe (1991).