Études internationales

US *National Cybersecurity. International Politics, Concepts and Organization*, Damien VAN PUYVELDE et Aaron F. BRANTLY, 2017, New York, Routledge, 238 p.

Quentin Delors

Volume 49, Number 2, Spring 2018

URI: https://id.erudit.org/iderudit/1055699ar
DOI: https://doi.org/10.7202/1055699ar

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

Delors, Q. (2018). Review of [US *National Cybersecurity. International Politics, Concepts and Organization*, Damien VAN PUYVELDE et Aaron F. BRANTLY, 2017, New York, Routledge, 238 p.] *Études internationales*, *49*(2), 435–437. https://doi.org/10.7202/1055699ar

Une course à la robotisation est donc lancée entre les plus grandes nations. L'équilibre stratégique entre les puissances pourrait en être bouleversé. Les pays en avance dans le domaine de l'intelligence artificielle pourraient ainsi devenir les chefs de file de demain. Se posent néanmoins en arrière-plan des considérations éthiques, quant à la possibilité pour une machine de tuer sans autorisation humaine, qui semblent échapper au débat citoyen. Cet ouvrage a le mérite de rendre accessibles les connaissances essentielles à la compréhension de la robotique militaire, sa nature, son utilisation et ses conséquences.

La principale lacune de ce livre réside dans l'absence de bibliographie qui ne permet pas au lecteur d'approfondir les éléments abordés tout au long de l'ouvrage. Nous pouvons également regretter que l'auteur prenne position de manière aussi franche sur les systèmes autonomes plutôt que de fournir davantage de détails sur les positions des différents antagonistes. Par sa simplicité et son accessibilité, l'ouvrage encouragera chaque citoyen à participer au débat public sur l'utilité des politiques nationales de défense. C'est, finalement, l'un des principaux objectifs de celui-ci : la contestation de la mainmise des problématiques militaires aux seuls spécialistes de la question.

Pierre COLAUTTI
Hautes études internationales
Université Laval
Québec, Canada

US National Cybersecurity. International Politics, Concepts and Organization

Damien VAN PUYVELDE et Aaron F. BRANTLY, 2017, New York Routledge, 238 p.

Les récentes attaques informatiques contre des systèmes d'information nationaux stratégiques en Ukraine, ou encore les soupçons d'ingérence russe durant la campagne présidentielle américaine par les systèmes informatiques, démontrent plus que jamais l'importance de traiter ces sujets techniques au regard des relations internationales. Sous la direction de Damien Van Puyvelde (professeur assistant à l'Université du Texas à El Paso) et Aaron Brantly (professeur assistant à l'Université de Géorgie), *US National Cybersecurity : International Politics, Concepts and Organization* s'attelle à cette tâche en s'appuyant sur une approche multidisciplinaire. En s'intéressant particulièrement à la sécurité des systèmes d'information d'importance vitale aux États-Unis, liés aux infrastructures nucléaires ou militaires, l'ouvrage montre l'efficacité de la politique sécuritaire américaine en matière de cyberinformation et replace les différentes politiques engagées jusqu'ici dans le contexte des relations internationales. Il évoque plusieurs notions clés, des plus classiques, comme la dissuasion militaire, aux plus actuelles, comme le terrorisme.

Les différents contributeurs à ce livre viennent d'horizons

divers, qu'il s'agisse d'universitaires, de travailleurs de la société civile ou d'acteurs au cœur même de ces politiques (notamment des militaires), apportant ainsi des éclairages variés qui permettent d'aborder cette problématique de manière transdisciplinaire.

Globalement, le livre est organisé autour de trois thèmes majeurs abordant la problématique centrale de la cybersécurité. Alors que le premier thème s'inscrit dans une approche macroscopique pour tenter d'établir un cadre qui fait aujourd'hui défaut à la cybersécurité, la deuxième partie du livre s'intéresse surtout aux différentes approches afférentes à la cybersécurité (militaires, médicales ou, encore, liées à l'innovation). Enfin, la troisième partie porte sur les politiques en place aux États-Unis dans une perspective comparative avec leurs alliés.

Un pan entier de l'ouvrage est consacré à une analyse transdisciplinaire des relations internationales pour donner des pistes d'analyse de cybersécurité. Ainsi, les réponses aux cybermenaces sont abordées du point de vue des normes légales internationales. Les réponses légales qui peuvent être données par le gouvernement américain en cas d'attaques touchant ses infrastructures n'étant pas clairement identifiées, l'ouvrage propose des pistes juridiques vers lesquelles les normes pourraient évoluer. Ainsi, le gouvernement américain devrait s'appuyer légalement sur les conséquences des actions d'acteurs non étatiques pour mener ses opérations et dresser un cadre légal plus contraignant pour empêcher des opérations illégales dans son cyberespace.

Plus classiquement, certains contributeurs tentent d'apporter une expertise sur l'adaptation des techniques de dissuasion militaire pour répondre aux cybermenaces du nouveau millénaire. Toutefois, un véritable changement dans l'approche militaire traditionnelle s'opère, notamment en raison de la difficulté à définir l'objet, ce qui complique l'évaluation de l'efficacité des politiques mises en place. En conséquence, plusieurs auteurs proposent des pistes de solution qui vont au-delà de la simple question militaire dans un contexte de guerre asymétrique en évoquant la place grandissante de l'innovation dans l'adoption de mesures adaptées, en regardant, pour l'armée américaine, les politiques innovatrices mises en place par de grands groupes privés. Dans cette mesure, ils tentent des approches de plus en plus originales pour lutter contre les menaces en s'appuyant par exemple sur l'essor du « big data », mais aussi en s'inspirant des techniques de lutte contre les épidémies. En lien avec les tendances politiques actuelles, Damien Van Puyvelde rappelle l'importance des partenariats publics-privés pour répondre aux menaces posées aux deux parties, qui partagent parfois les mêmes systèmes d'information, puisque le secteur privé peut être

fournisseur du secteur public, dans l'objectif de coordonner au mieux les actions.

Les États-Unis à eux seuls ne pourront pas mettre en place une politique de lutte contre les activités cybercriminelles. Toutefois, différentes puissances mondiales, à l'image de la Chine ou de la Russie, seraient peu enclines à fixer avec les États-Unis des normes contraignantes communes en matière de sécurité de l'Internet. Dans ce cadre, l'ouvrage aborde les politiques américaines en matière de cybersécurité à la lumière de ce qui a été mis en place par les alliés des États-Unis, en se concentrant sur la structure choisie au Royaume-Uni. L'importance de la coopération internationale dans la lutte contre la cybercriminalité est largement soulignée.

En conclusion, l'ouvrage aborde de manière progressiste la question de la cybercriminalité au sein des relations internationales et constitue aujourd'hui un outil adapté pour aborder cette question d'une manière macroscopique, mais précise. Au-delà de la critique des politiques existantes par les différents auteurs, ceux-ci proposent des axes d'orientation pour les futures politiques en s'appuyant sur la théorie des Relations internationales dans d'autres domaines, notamment en matière de dissuasion militaire, mais aussi sur la comparaison des politiques des alliés des États-Unis. Toutefois, il aurait été intéressant de mener une étude plus approfondie des acteurs qui menacent aujourd'hui les États-Unis, notamment pour les lecteurs novices. Ainsi, un travail de synthèse des principales menaces et des parties prenantes, en début d'ouvrage, aurait été nécessaire. Le vocabulaire utilisé par les différents acteurs est tout de même défini au fil des chapitres avec un niveau de détail plus ou moins suffisant. Par ailleurs, si ce travail de synthèse des différents termes utilisés avait été réalisé, il aurait permis d'éviter les nombreuses répétitions chez les principaux auteurs au fil des chapitres. D'un point de vue théorique, l'ouvrage provoque une prise de conscience de ces problématiques, bien que l'on puisse regretter que l'ouvrage se concentre uniquement sur le cas des États-Unis, étant donné la nature intrinsèquement mondialisée du sujet traité. Néanmoins, cette limitation du cadre d'étude s'avère nécessaire afin de baliser le travail de recherche et d'optimiser la qualité de celui-ci, d'autant que l'étude comparative permet habilement d'aller au-delà du seul contexte américain.

Quentin DELORS
Faculté des sciences de l'administration
Université Laval
Québec, Canada

Pourquoi la dissuasion ?

Nicolas ROCHE, 2017, Paris Presses Universitaires de France, 545 p.

Au-delà de la formulation du titre de cet ouvrage – interrogation ou argumentation –, cet essai