Introduction

Étudier le cyberespace à l'international

Pourquoi faut-il appréhender le cyberespace d'un point de vue réflexif ? Celui-ci n'étant pas une réalité naturelle ou sociale mais un système partagé construit dans le temps par une multitude d'acteurs, son caractère hybride – puisqu'il possède une composante technologique et une composante sociale – ne permet pas d'utiliser les repères habituels que les sciences sociales emploient pour étudier le monde social. Par ailleurs, les acteurs du cyberespace sont bavards et doctrinaires et produisent eux-mêmes une foule de concepts stratégiques plus ou moins nouveaux (et bien souvent d'un faible apport) mais qui obscurcissent la compréhension de la situation[1]. L'effort de réflexivité paraît d'autant plus nécessaire. Appréhender le cyber suppose donc une approche tenant compte à la fois des dimensions sociale et technologique ainsi qu'une capacité à se tenir à distance des multiples discours des acteurs, deux conditions indispensables afin d'en faire un objet d'étude authentique. L'enjeu de cet ouvrage est précisément d'essayer de contribuer à cette réflexion essentielle, qui n'en est qu'à ses débuts[2]. Il nous faut donc énoncer à destination du lecteur quels sont les choix et les perspectives qui guident ce livre.

Introduction rédigée par Sébastien-Yves LAURENT.

1. Lire Pierre Musso, « Le Web : nouveau territoire et vieux concepts », *Annales des Mines. Réalités industrielles*, novembre 2010, n° 4, 2010, p. 75-83.

2. Il n'en est que plus important de souligner le rôle des pionniers : Hugo Loiseau et Elena Waldispuehl, *Cyberespace et science politique, de la méthode au terrain, du virtuel au réel*, Québec, Presses de l'Université de Québec, 2017, et Hugo Loiseau, Daniel Ventre et Hartmut Aden, *La cybersécurité en sciences humaines et sociales : méthodologies de recherche*, ISTE Editions, Londres, 2021.

Les neuf chapitres de ce volume donnent à voir une dimension globale, et en cela originale, du cyberespace. En effet, il nous a semblé utile de ne pas limiter le propos, comme c'est parfois le cas, à une vision irénique valorisant seulement la dimension collaborative ou, à l'inverse, à une vision cynique réduisant le cyberespace à un espace conflictuel. Dans l'esprit de notre perspective globale, nous avons fait le choix du titre *Conflits, crimes et régulations dans le cyberespace*. Cet ouvrage ne s'inscrit pas directement dans le débat sans fin entre les partisans de la guerre[3] et ceux qui rejettent cette posture[4]. Nous constatons qu'il y a des confrontations dans le cyberespace, par des acteurs civils et militaires, pour des finalités diverses qui ne sont pas toujours de court terme. Aujourd'hui, l'état des connaissances tend fortement à dépasser les pronostics apocalyptiques des années 1990 et 2000 et à relativiser la quantité et la portée des affrontements entre acteurs étatiques, l'essentiel d'entre eux relevant d'activités de vol de données, c'est-à-dire d'espionnage[5]. Ainsi, nous avons fait le choix de les qualifier de « crimes » ou de « conflits » pour éviter délibérément le terme de guerre[6], qui nous paraît excessif et produit immédiatement un effet de sécuritisation.

Les dix auteurs que nous remercions vivement[7] pour leur contribution ont été invités à donner dans leur texte une définition claire de ce qu'ils entendaient par cyberespace. Cela est bien sûr d'importance car, en ce domaine, la diversité l'emporte ; ainsi, en 2018, le CCD COE (centre d'excellence de cyberdéfense coopérative de l'Otan) de Tallinn recensait 29 définitions du cyberespace[8]. Nous faisons le choix d'adopter à l'orée de ce volume la définition étatsunienne de la National Military Strategy for Cyberspace Operations de 2006 car elle nous paraît neutre : « […] an operational domain characterized by the use of electronics and the electromagnetic spectrum to create, store, modify and exchange information *via* networked information systems and associated physical infrastructures »[9]. Les auteurs réunis ici, qu'ils soient juristes ou politistes, adhèrent

3. Alex Calvo, « Cyberwar is war: a critique of "hacking can reduce real-world Violence" », *Small Wars Journal*, juin 2014 [En ligne]. Disponible à l'adresse : www.smallwarsjournal.com/jrnl/art/cyberwar-is-war.

4. Erik Gartzke, « The Myth of Cyberwar: bringing war in cyberspace back down to earth », *International security*, vol. 38, n° 2, p. 41-73, automne 2013.

5. Brandon Valeriano et Ryan C. Maness, « How we stopped worrying about cyber doom and started collecting data », *Politics and governance*, vol. 6, n° 5, p. 781-799, 2018.

6. Pour une mise en contexte dans la littérature, voir Robert Gorwa et Max Smeets, « Cyber conflict in political science: a review of methods and literature », ISA, Toronto, mars 2019.

7. L'auteur tient à remercier également Michel Courty pour le façonnement du manuscrit.

8. Brad Bigelow, « The Topography of Cyberspace and Its Consequences for Operations », *10th International Conference on Cyber Conflict*, NATO CCD COE Publications, p. 125, 2018.

9. Citée par Daniel T. Kuehl, « From Cyberspace to Cyberpower: Defining the Problem », dans Franklin D. Kramer, Stuart H. Starr, Larry Wentz (dir.), *Cyberpower and National Security*, Washington, National Defense University Press, p. 27, 2009.

également à la perspective d'étudier l'objet cyberespace comme un système sociotechnique, c'est-à-dire comme un ensemble d'unités sociales en interactions dynamiques, organisées autour des technologies de l'information et de la communication, ce qui oriente vers l'étude des sciences et technologies (STS)[10].

Enfin, ce livre s'inscrit clairement dans une perspective internationaliste[11] : ses auteurs pensent que l'étude du cyberespace ne peut être circonscrite aux seules limites d'un pays, en raison de la nature distribuée du système structurant le cyberespace et de la mobilité constante des données. Ce constat n'invalide pas cependant la possibilité d'étudier les politiques publiques cyber (voir chapitre 2). Adoptant cette approche internationale, nous précisons que l'on ne reviendra pas ici sur le débat théorique consistant à savoir si le cyberespace est une composante du système international ou s'il constitue un système propre et autonome[12]. Dans le paradigme de recherche que nous avons rappelé, ce sont ici les enjeux internationaux du cyber qui sont mis en avant (voir chapitres 1 et 8) ainsi que deux pays, les États-Unis (voir chapitres 1, 2, 6 et 9) et la France (voir chapitres 3, 5 et 8). La diversité des acteurs du cyber – étatiques, non-étatiques et individuels – est évoquée dans l'ensemble des chapitres du livre, mais l'approche choisie met toutefois l'accent sur les deux premiers.

Conflits, crimes et régulations dans le cyberespace insiste, d'une part, sur les acteurs du cyberétatique, ce que l'on peut appeler les bureaucraties cyber (chapitres 2, 8 et 9) et, d'autre part, sur les outils du cyberétatique, à savoir les normes (droit national et international), dans les chapitres 4, 5 et 7, ainsi que les concepts stratégiques utilisés par les différents acteurs (cybersécurité, cyberdéfense, souveraineté numérique[13]). Notre approche ici est donc celle du niveau « méso », peu fréquente car les approches internationalistes du cyber dans la littérature académique de l'anglosphère tendent plutôt à prendre en compte des entités « macro » (États, organisations internationales, etc.). C'est ainsi que cet ouvrage entend contribuer au débat académique global sur les questions cyber.

10. Voir deux exemples particulièrement réussis : Thierry Balzacq et Myriam Dunn Cavelty, « A Theory of actor network for cyber-security », *European Journal of International Security*, vol. 1-2, p. 176-198, 2016, et Myriam Dunn Cavelty, « Cybersecurity research meets science and technology studies », *Politics and governance*, vol. 6, n° 2, p. 22-30, 2018.

11. Voir Robert Reardon et Nazli Choucri, « The Role of Cyberspace in International Relations: a view of the literature », ISA, San Diego, avril 2012.

12. Voir Sébastien-Yves Laurent, « Ce que le cyber (ne) fait (pas) aux relations internationales », *Études internationales*, 2021.

13. Voir Pauline Türk et Christian Vallar, *La Souveraineté numérique. Le concept, les enjeux*, Mare & Martin, Paris, 2017.