Introduction

Pourquoi un ouvrage de méthodologie ?

Avant que n'apparaisse la notion de cybersécurité, il était question dans les années 1960 de sécurité des ordinateurs ou de sécurité informatique (*computer security*), « protection des programmes d'ordinateurs et des données contre tout accès non autorisé » [PAY 83]. Dans les années 1990, la notion de « cybersécurité » apparaît. Elle désigne alors principalement la protection des ordinateurs dans sa dimension technique, et certains y voient même déjà l'un des enjeux majeurs des politiques de sécurité pour les décennies à venir : « One of the biggest challenges for strategic leaders in the 21st century will be cyber security – protecting computers and the links between them » [JOH 95]. Dans l'essentiel de la littérature, les technologies « cyber » ou « informatiques » sont avant tout des objets imparfaits, qu'il faut réparer pour produire de la sécurité. Mais la cybersécurité a un objet plus large que l'ordinateur : la sécurité du cyberespace.

Depuis une dizaine d'années, les sciences humaines et sociales (SHS) s'intéressent à la cybersécurité. Ont ainsi été proposées des lectures politiques [DEI 10, QUI 12, CAV 19], juridiques [GRA 04], stratégiques, économiques... Des revues dédiées à l'étude de la cybersécurité offrent aux disciplines des sciences humaines et sociales les espaces d'expression de recherches procédant d'horizons multiples. Citons le *Journal of Cybersecurity* (Oxford University Press)[1], le *Journal of Cybersecurity Research* (JCR)[2], l'*International Journal of Cybersecurity Intelligence and Cybercrime* (IJCIC)[3],

---

Introduction rédigée par Daniel VENTRE, Hugo LOISEAU et Hartmut ADEN.

1. https://academic.oup.com/cybersecurity/pages/About.
2. https://clutejournals.com/index.php/JCR.
3. https://vc.bridgew.edu/ijcic/.

le *National Journal of Cyber Security Law*[4], le *Journal of Intelligence and Cyber Security*[5], pour n'en citer que quelques-uns. La plupart de ces revues académiques n'ont été créées que récemment. La cybersécurité est quoi qu'il en soit sinon déjà devenue, du moins en train de devenir, un objet à part entière de recherches en sciences humaines et sociales. Nonobstant ce constat, les recherches apparaissent encore relativement éparses, hétérogènes, chaque discipline à l'intérieur des SHS appréhendant les problématiques et posant les questions de recherche selon ses approches propres, à l'aide de son appareil théorique et méthodologique.

Notre contribution à cette vague de productions internationales sur la cybersécurité résidera dans une réflexion sur les aspects méthodologiques en sciences humaines et sociales pour la recherche en cybersécurité. Cet ouvrage pose donc la question centrale suivante : quelles méthodes et quels outils théoriques peuvent mobiliser les chercheurs des sciences humaines et sociales pour traiter de la cybersécurité ? Cette dimension méthodologique nous est apparue essentielle à plusieurs titres.

– Les publications produites ces dernières années s'intéressent généralement assez peu à la dimension méthodologique. Les ouvrages et articles de recherche abordent bien sûr dans le cadre formel de leurs développements, cette dimension méthodologique. Mais elle est généralement centrée sur le traitement de l'objet de la publication particulière. Il n'existe que peu d'efforts à ce jour pour proposer une réflexion centrée sur les questions de méthode et de théories spécifiques aux sciences humaines et sociales.

– Le thème de la cybersécurité peut dérouter de prime abord les jeunes chercheurs (et parfois moins jeunes). L'objet qu'est la cybersécurité semble imposer, de fait, la mobilisation et la maîtrise de connaissances multiples (celles du domaine propre au chercheur en SHS, combinées à des savoirs en informatique, en réseaux, en communication, etc.). C'est donc là une question de construction des savoirs indispensables au chercheur, donc de méthodologie.

– Dès lors qu'elle sera définie, expliquée, déconstruite, la cybersécurité apparaîtra rapidement comme un objet complexe, aux multiples composantes qui seront autant d'objets de recherche (la cybercriminalité, les cyberattaques, la cybermenace, le cyberrisque, les enjeux du renseignement dans le cyberespace, etc.). Chacun de ces objets pourra nécessiter des connaissances particulières, des cadres théoriques distincts et des méthodologies adaptées. Les différents chapitres composant cet ouvrage démontrent de façon éloquente la complexité de l'objet cybersécurité.

4. http://stmjournals.com/Journal-of-Cybersecurity-Law.html.

5. https://www.academicapress.com/journals.

– Par ailleurs, une autre question fort importante se pose dès lors que l'on considère la cybersécurité comme étant composite et complexe : quelle peut ou quelle doit y être la place de la multidisciplinarité ou de l'interdisciplinarité dans son étude ? En tant que discipline, la cybersécurité subit deux pressions fertiles pour son développement. La première est bien entendu la volonté de spécialisation des chercheurs qui se reconnaissent dans cette discipline (en termes de connaissances, de méthodes ou de techniques) afin de distinguer l'objet cybersécurité de la multitude d'objets ou de dimensions la composant dans le réel, mais aussi la capacité de démarquer ce champ de recherche des autres champs qui lui sont contigus tels que la sécurité informatique, la protection des données, le génie informatique, etc.

– La deuxième pression pousse la discipline à élargir ses horizons vers les SHS puisqu'il est dorénavant acquis que la cybersécurité est aussi un phénomène social. Cette pression pousse donc la recherche vers l'interdisciplinarité ou la multidisciplinarité pour tenir compte des dimensions humaines et sociales de la cybersécurité.

– La cybersécurité intéresse-t-elle toutes les disciplines des SHS ? Cette question sous-entend que les aspects humains et sociaux de la cybersécurité sont potentiellement transversaux lorsque les SHS abordent la cybersécurité. Autrement dit, autant des théories, des méthodes, des cadres analytiques que des variables issues de la psychologie, de l'anthropologie, de la sociologie ou de toutes autres disciplines des SHS peuvent contribuer de quelque façon à expliquer ou comprendre le phénomène de la cybersécurité. Mobiliser ces différents outils de recherche et ce patrimoine méthodologique semble profitable pour une analyse intégrée de la cybersécurité et une richesse de connaissances insoupçonnée.

– Quels avantages la cybersécurité tire-t-elle de sa rencontre avec les sciences humaines et sociales ? La réponse à cette question repose sur ce qui caractérise les sciences humaines et sociales et finalement les distingue des autres sciences. La principale distinction réside dans leurs capacités d'analyser de façon qualitative et quantitative les phénomènes humains complexes. De ce fait, une multitude d'outils et d'approches méthodologiques existent et permettent, notamment, d'affiner les connaissances en cybersécurité et de fortement nuancer le technodéterminisme (ou le « solutionnisme » comme le nomme Morozov [MOR 14]). Cette double capacité qualitative et quantitative permet aux SHS de dévoiler des enjeux de cybersécurité de trois façons. Tout d'abord de façon macro où la globalité du phénomène de cybersécurité est dévoilée dans ses aspects structurels, systémiques et environnementaux. Par exemple, la géopolitique internationale qui est transformée par l'importance que prend la cybersécurité dans les rapports internationaux de nos jours [DOU 14]. De façon méso, par la suite, où les processus de prise de décision, le rôle des différents acteurs institutionnels et des organisations privées sont mis en exergue. Il suffit de

penser à la formulation d'une politique étrangère ou de défense qui ne peut faire abstraction des menaces hybrides en termes de cybersécurité. Enfin, de façon micro où l'unicité et la particularité du même phénomène de cybersécurité sont rendues observables dans le comportement ou la pensée de l'individu telle la victime d'une campagne de *phishing* par exemple. L'apport des SHS se révèle aussi dans leurs capacités de générer des débats de société autour des questions de cybersécurité et de forcer la discipline à vulgariser ses notions de base. La transmission du savoir et la conscientisation sociale à propos des enjeux de cybersécurité s'en trouvent donc facilitées. Enfin, elles permettent de contextualiser les problèmes ou les risques reliés à la cybersécurité en donnant une profondeur historique à la réflexion ou aux débats par ailleurs impossibles à trouver.

– Une dernière question s'impose à notre avis sur les plans méthodologique et théorique : faut-il mobiliser les cadres théoriques préexistants ou est-il possible d'envisager le renouvellement de ces derniers ? La nature de l'objet cybersécurité favorise certes la multidisciplinarité, mais crée néanmoins deux obstacles à son analyse. D'une part, la cybersécurité associe une dimension technique à une dimension humaine qui fait de cet objet de recherche un objet hybride et complexe tel que mentionné précédemment. D'ailleurs, peu de cadres théoriques ou méthodologiques existent, en ce moment, pour traiter l'entièreté des dimensions humaine et technique de la cybersécurité afin d'avoir un point de vue holiste ou intégré sur la cybersécurité. D'autre part, la célérité du développement informatique (dimension technique) et de l'adoption des nouvelles technologies (dimension humaine) rend les cadres d'analyse existants rapidement obsolètes. Or, ces deux obstacles doivent être pris en compte dans la mobilisation des cadres théoriques, existants, mais aussi, et surtout, dans le développement de nouveaux cadres d'analyse complets. Pour y arriver, une étude sur les méthodes de recherche et sur les outils théoriques des sciences humaines et sociales dans l'étude de la cybersécurité nous semblait nécessaire.

Les contributions à l'ouvrage

Les six chapitres de l'ouvrage offrent des perspectives différentes sur des aspects particuliers de la cybersécurité et proposent quelques réponses aux différentes questions exposées précédemment.

Dans le chapitre 1, Hugo Loiseau aborde la scientificité des études sur la cybersécurité. Celle-ci demande encore à être définie et démontrée en sciences humaines et sociales. Parmi le foisonnement des recherches en cybersécurité, toutes sciences confondues, peu d'études se consacrent aux problèmes méthodologiques et scientifiques de cette discipline naissante. En effet, en sciences humaines et sociales, sur le

plan épistémologique, les études sur la cybersécurité nécessitent une critique méthodologique pour améliorer leur scientificité et leur crédibilité face aux sciences informatiques et au génie. Dans ce chapitre, les méthodes de recherche, l'accès aux données et le développement d'une discipline de cybersécurité en sciences humaines et sociales sont ainsi évalués. L'objectif du chapitre est de poser les bases épistémologiques pour proposer une définition opérationnalisable de l'objet « cybersécurité » pour les sciences humaines et sociales.

Daniel Ventre traite spécifiquement de la définition et de la manière d'exprimer et saisir les concepts. La définition, la typologie, la taxonomie et l'ontologie (regroupées dans l'acronyme DTTO) peuvent être mobilisées pour dire la cybersécurité, la représenter, la comprendre, dessiner son domaine, son périmètre. La littérature postule le plus souvent l'absence de DTTO consensuelle. Dans le chapitre 2, l'auteur tente d'identifier des tendances suffisamment fortes et significatives dans chacune des approches de la cybersécurité, pour que le postulat puisse être remis en question.

Hartmut Aden analyse dans le chapitre 3 les tensions et les synergies entre la cybersécurité et la protection des données dans la perspective des sciences juridiques et de l'analyse des politiques publiques, avec une attention particulière sur leurs liens transdisciplinaires. Il montre que la combinaison des méthodes juridiques d'interprétation des normes émergeant dans le champ de la cybersécurité et des méthodes qualitatives et quantitatives de sciences sociales utilisées pour l'analyse des politiques publiques peut contribuer à mieux comprendre les diverses facettes des tensions et des synergies entre la cybersécurité et la protection des données.

Joseph Fitsanakis s'intéresse dans le chapitre 4 aux méthodes, aux outils, aux théories que le chercheur peut mobiliser et aux obstacles spécifiques qu'il peut rencontrer dans l'étude des enjeux du cyberespionnage soutenu par les États. Il propose un état de l'art des recherches actuellement menées sur le sujet en sciences humaines et sociales, et qui se concentrent sur les dimensions stratégiques, tactiques et opérationnelles du phénomène. Il identifie et discute les outils théoriques, conceptuels pertinents pour mener ces recherches.

Le chapitre 5 proposé par Brett van Niekerk et Trishana Ramluckan illustre la manière dont la recherche qualitative peut être utile aux recherches sur la cybersécurité. Y est proposée une analyse de la législation sur la cybercriminalité et des stratégies nationales de cybersécurité, réalisée à l'aide de l'application NVivo. L'objectif de ce chapitre est d'évaluer la pertinence d'une analyse qualitative de documents pour une recherche portant sur la guerre de l'information et/ou la cybersécurité.

Elena Waldispuehl s'intéresse dans le chapitre 6 aux violences antiféministes en ligne sous deux angles. D'une part, elle y discute de la définition et des enjeux de

cybersécurité des activistes féministes à travers leur sentiment de sécurité en ligne. D'autre part, il y est question des enjeux de cybersécurité (menaces cyber et mesures de prévention) qui pèsent sur la chercheuse, qui s'identifie aussi comme féministe dans ses pratiques de recherche.

Bibliographie

[CAV 19] CAVELTY M.D., EGLOFF F.J., "The politics of cybersecurity: Balancing different roles of the state", *St Antony's International Review*, vol. 15, no. 1, pp. 37–57, 2019.

[DEI 10] DEIBERT R.J., ROHOZINSKI R., "Risking security: Policies and paradoxes of cyberspace security", *International Political Sociology*, vol. 4, no. 1, pp. 15–32, March 2010.

[DOU 14] DOUZET F., "La géopolitique pour comprendre le cyberespace", *Hérodote*, vol. 1, nos 152–153, pp. 3–21, 2014.

[GRA 04] GRADY M.F., PARISI F., "The law and economics of cybersecurity: An introduction", *George Mason University School of Law, Working Paper Series*, Paper 12, 2004.

[JOH 95] JOHNSEN W.T., JOHNSON II D.V., KIEVIT J.O. *et al.*, *The Principles of War in the 21st Century: Strategic Considerations*, Department of Defense, U.S. Army War College, Carlisle Barracks, USA, August 1, 1995.

[MOR 14] MOROZOV E., *Pour tout résoudre, cliquez ici : l'aberration du solutionnisme technologique*, Limoges, Fyp éditions, 2014.

[PAY 83] PAYTON J., ASBURY A.J., "Computer security", *British Medical Journal*, vol. 287, pp. 965–967, 1983.

Cette bibliographie est identique à celle de l'ouvrage correspondant en anglais publié par ISTE.