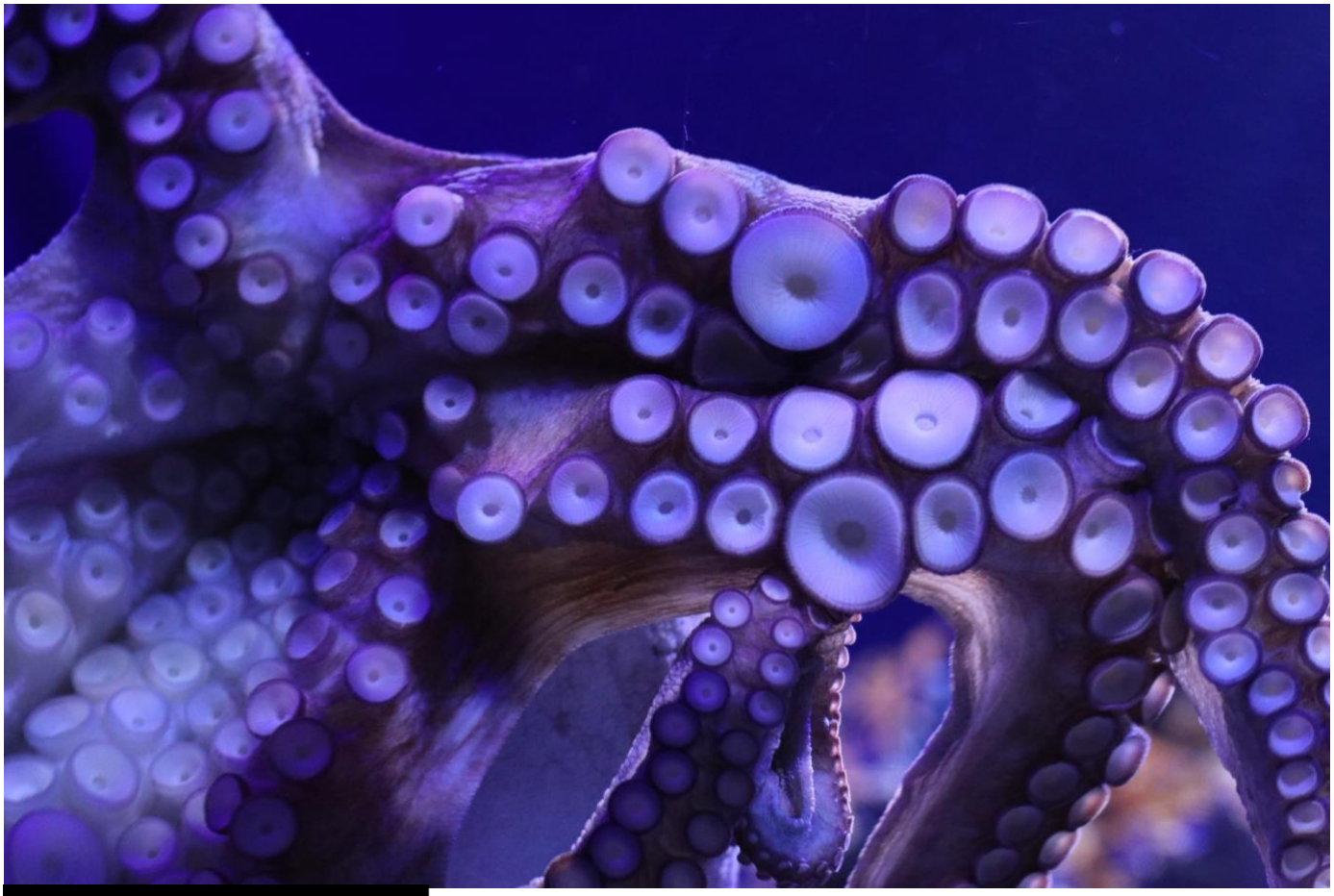
Mise à jour :
décembre 2023

Pour contribuer	Github
Pour s'informer	LinkedIn
Pour s'informer (bis)	BlueSky
Pour adhérer	Hello Asso



BIBLIOGRAPHIE

Cyberdéfense, cybersécurité, guerre de l'information

1. ABITEBOUL, Serge et Jean CATTAN. *Nous sommes les réseaux sociaux*. Odile Jacob. 2022.
2. ALLSOPP, Will. *Advanced penetration testing*. Wiley. 2017. *Même si les techniques de ce livre sont connues, il constitue une vue intéressante sur les potentiels vecteurs d'infection et d'ingénierie sociale pouvant être mis en œuvre par des attaquants.*
3. ANDERSON, Chris. *La longue traine*. Pearson. 2012. *Livre un brin prophétique devenu un classique, Chris Anderson, rédacteur en chef de* Wired*, nous démontre comment Internet modifie en profondeur les mécanismes de l'économie.*
4. ANDRESS, Jason et Steve WINTERFELD. *The Basics of Cyber Warfare: Understanding the Fundamentals of Cyber Warfare in Theory and Practice*. Newnes. 2012. Disponible prêt adhérents M82. *Un livre "ancien" qui a le mérite de présenter les bases de la construction des doctrines de cyberdéfense. L'ouvrage replace le concept de cyberguerre dans le corpus stratégique et la continuité des concepts militaires.*
5. ARPAGIAN, Nicolas. *Frontières.com*. L'Observatoire. 2022.
6. ARPAGIAN, Nicolas. *La cybersécurité*. PUF. 2018.
7. ARPAGIAN, Nicolas. *La cyberguerre, la guerre numérique a commencé*. Vuibert. 2009.
8. ARQUILLA, John. *Bitskrieg, the new challenge of cyberwarfare*. Polity. 2021. *Disponible prêt adhérents M82. Livre qui revient sur 20 ans d'évolution du concept de cyberguerre sans vraiment changer la ligne défendue par l'auteur depuis son article "Cyberwar is coming".*
9. ARQUILLA, John et David RONFELDT. *Networks and Netwars: the Future of Terror, Crime and Militancy*. Rand. 2001.
10. ARTICLE 19. *Connaissez-vous vraiment internet ? Protocoles, sécurité, censure, gouvernance...* Éditions Eyrolles. 2022. Disponible prêt adhérents M82. *Un très bon livre pour les débutants.*
11. ARUTUNYAN, Anna. *Hybrid Warriors, Proxies, Freelancers and Moscow's Struggle for Ukraine*. Hurst Publisher. 2022.
12. AUSTIN, Greg. *Cybersecurity in China: the next wave*. Springer. 2018.
13. BADOUARD, Romain. *Le désenchantement de l'internet. Désinformation, rumeur et propagande*. FYP éditions. 2017.
14. BENKLER, Yochai, Robert FARIS, et Hal ROBERTS. *Network propaganda: Manipulation, disinformation, and radicalization in American politics*. Oxford University Press. 2018.
1. BILLOIS, Gérôme et Nicolas COUGOT. *Cyberattaques, les dessous d'une menace mondiale*. Hachette. 2022. *La qualité d'un consultant réside souvent dans sa capacité à expliquer des choses complexes de manière accessible. C'est justement ce qu'arrive à faire Gérôme Billois avec cet ouvrage complet et au design soigné. Vous y trouverez des récits sur les différents types de cyberattaques, des explications sur les enjeux de la cyber sécurité pour les états, les entreprises et les individus ainsi que des portraits de professionnels représentant la grande diversité des métiers. Ce libre est le B.A.-BA pour tout nouvel entrant dans le domaine de la cybersécurité et notamment ceux qui se destinent à une carrière dans le conseil.*
15. BITTMAN, Ladistlav. *The KGB and Soviet Disinformation: An Insider's View*. Brassey's Inc. 1985.
16. BITTMAN, Ladistlav. *The Deception Game*. Ballantine Books. 1981.
17. BLONDEAU, Olivier. *Devenir média. L'activisme sur Internet, entre défection et expérimentation*. Édition Amsterdam. 2007.
18. BLONDEAU, Olivier et Florent LATRIVE. *Libres enfants du savoir numérique. Anthologie du libre*. Éditions de L'Éclat. 2000.
19. BORTZMEYER, Stéphane. *Cyberstructure, l'Internet un espace politique*. C&F Editions. 2018. *Écrit par un expert des questions d'internet et travaillant pour l'AFNIC (organisme gestionnaire du registre des noms de domaine en .fr), ce livre se divise en deux parties. La première se concentre sur le fonctionnement d'internet : les protocoles, les applications web, les organismes de gouvernance et quelques*

sujets particuliers tels que les crypto monnaies. La deuxième partie est dédiée à une réflexion sur les aspects politiques d'internet : doit-on limiter le chiffrement ? Les concepts de sécurité et vie privée sont-ils opposés ? Quelles technologies choisir pour l'internet de demain ?

20. BOYER, Bertrand. *Guérilla 2.0, guerres irrégulières dans le cyberespace*. École de Guerre. 2020. *Disponible prêt adhérents M82.*
21. BOYER, Bertrand. *Dictionnaire de la Cybersécurité et des réseaux*. NUVIS. 2015. *Disponible prêt adhérents M82.*
22. BOYER, Bertrand. *Cybertactique, conduire la guerre numérique*. NUVIS. 2014. *Disponible prêt adhérents M82.*
23. BOYER, Bertrand. *Cyberstratégie, l'art de la guerre numérique*. NUVIS. 2012. *Disponible prêt adhérents M82.*
24. BRADDOCK, Kurt. *Weaponized words: The strategic role of persuasion in violent radicalization and counter-radicalization*. Cambridge University Press. 2020.
25. BRANTLY, Aaron Franklin. *The decision to attack: military and intelligence cyber decision-making*. University of Georgia Press. 2016. vol.5.
26. BRENNER, Susan W. *Cyberthreats, the emerging fault line of the Nation State*. Oxford University Press. 2009.
27. BRONNER, Gérald. *Apocalypse cognitive*. PUF. 2021.
28. BRUNTON, Finn et Helen NISSENBAUM. *Obfuscation: A User's Guide for Privacy and Protest*. The MIT Press. 2015.
29. BRYANT, William D. *International Conflict and Cyberspace superiority*. Routledge. 2016.
30. BUCHAN, Russell. *Cyberespionage and international law*. Hart Publishing. 2018.
31. BUCHANAN, Ben. *The Hacker and the state: The New Normal of Geopolitics*. Harvard University Press. 2020. *Une des 5 références sur le sujet selon le Modern Warfare Institute de West Point.*
32. BUCHANAN, Ben. *The Cybersecurity Dilemna: Hacking, Trust and Fear Between Nations*. Oxford University Press. 2016.
33. BULINGE, Franck. *De l'espionnage au renseignement*. Vuibert. 2012.
34. CARDON, Dominique. *A quoi rêvent les algorithmes : nos vies à l'heure des Big data*. Média Diffusion. 2015.
35. CARR, Jeffrey. *Inside Cyber Warfare, mapping the cyber underworld*. O'Reilly. 2009.
36. CARRIER, Brian. *File System Forensic Analysis*. Addison-Wesley Professional. 2005.
37. CATTARUZZA, Amaël. *Géopolitique des données numériques. Pouvoirs et confilts à l'heure du Big Data*. éditions le Cavalier bleu. 2019.
38. CATTARUZZA, Amaël, Didier DANET, et Stéphane TAILLAT. *La cyberféfense, politique de l'espace numérique*. Armand Colin. 2023. *2ème édition. Mise à jour en 2023. Cet ouvrage collectif analyse la cyberdéfense sous le prisme des relations internationales. Les auteurs présentent l'état des connaissances scientifiques dans des sujets variés tel que le concept de guerre cyber, les enjeux de souveraineté numérique, le positionnement des grands pays cyber (États-Unis, Chine, Russie), le droit international appliqué au numérique… Plus théorique que pratique, cet ouvrage est un indispensable pour les étudiants ayant un projet de mémoire en lien avec la cyberdéfense. Disponible prêt adhérents M82.*
39. CHAVALARIAS, David. *Toxic Data*. Flammarion. 2022. *Un des ouvrages les plus abordables pour comprendre le travail d'analyse des réseaux sociaux. Disponible prêt adhérents M82.*
40. CHESNEY, Robert et Max SMEETS. *Deter, Disrupt, or Deceive, Assessing Cyber Conflict as an Intelligence Contest*. Georgetown University Press. 2023.
41. CHOPIN, Olivier et Benjamin OUDET. *Renseignement et sécurité-2e éd.* Armand Colin. 2019.
42. CHOUCRI, Nazli et David D. CLARK. *International Relations in the Cyber Age. The Co-Evolution Dilemma*. The MIT Press. 2019.
43. CIALDINI, Robert B. *Influence et manipulation : l'art de la persuasion*. First. 2021. P*arfait pour apprendre les*

techniques que les médias, le marketing, utilisent tous les jours sans qu'on s'en rende compte. Un point de départ pour la conduite d'opération HUMINT.

44. CLANCY, Tom. *Cybermenace*. Albin Michel. 2013.
45. CLARKE, Richard et Robert KNAKE. *Cyberwar: the next Threat to National Security and what to do about it*. HarperCollins. 2010.
46. CLOUGH, Jonathan. *Principles of cybercrime*. Cambridge University Press. 2015.
47. COELHO, Ophélie. Éditions de l'Atelier. 2023. *Disponible prêt adhérents M82.*
48. COLON, David. *La guerre de l'information*. Tallandier. 2023. *Disponible prêt adhérents M82.*
49. CRISTIANO, Fabio, Dennis BROEDERS, François DELERUE, et al. *Intelligence artificielle et conflit international dans le cyberespace*. Taylor & Francis. 2023.
50. CUKIER, Kenneth, Viktor MAYER-SCHÖNBERGER, et Francis DE VERICOURT. *Framers: Human advantage in an age of technology and turmoil*. Penguin. 2022.
51. DAHJ, Jean Nestor. *Mastering Cyber Intelligence: Gain comprehensive knowledge and skills to conduct threat intelligence for effective system defense*. Packt Publishing. 2022.
52. DEHGHANTANHA, Ali, Mauro CONTI, et Tooska DARGAHI. *Cyber threat intelligence*. Springer. 2018. *Une bonne référence pour commencer dans la CTI.*
53. DELERUE, François. *Cyberoperations and International Law*. Cambridge University Press. 2020.
54. DENARDIS, Laura. *The Internet in everything*. Yale University Press. 2020.
55. DIOGENES, Yuri et Erdal OZKAYA. *Cybersecurity. Attack and Defense Strategies: Counter modern threats and emply state of the art tools and techniques to protect your organization*. Packt Publishing. 2019.
56. DOSSE, Stéphane et Aymeric BONNEMAISON. *Attention cyber ! Vers le combat cyber-electronique*. Économica. 2014. *Disponible prêt adhérents M82.*
57. DOSSE, Stéphane et Olivier KEMPF. *Stratégie dans le cyberespace*. L'esprit du livre. 2011.
58. DOSSE, Stéphane, Olivier KEMPF, et Christian MALIS. *Cyberespace, nouveau domaine de la pensée stratégique*. Économica. 2013. *Disponible prêt adhérents M82.*
59. DYKSTRA, Josiah, Eugene SPAFFORD, et Leigh METCALF. *Cybersecurity myths and Misconceptions*. Pearson Education. 2023.
60. EGLOFF, Florian J. *Semi-State Actors in Cybersecurity*. Oxford University Press Inc. 2022.
61. ELSBERG, Marc. *Black-out : demain il sera trop tard*. LGF. 2016. *Roman d'anticipation.*
62. ENGEBRETSON, Patrick. *Les bases du hacking*. Pearson. 2017. *Vous souhaitez concrètement comprendre comment se déroule une cyberattaque ? Alors ce guide est fait pour vous ! Patrick Engebretson, professeur américain en sécurité informatique, va vous présenter chaque étape d'une attaque (reconnaissance, scan, exploitation, maintien d'accès) à l'aide d'un cas d'étude. Grâce à ses conseils, aux outils gratuits et aux lignes de commande présentées vous serez en mesure de refaire l'attaque depuis votre ordinateur personnel. Bien que ce livre comporte des éléments techniques, il reste accessible dans sa grande majorité à tous.*
63. FAILLET, Caroline. *L'art de la guerre digitale, survivre et dominer à l'ère du numérique*. Dunod. 2016.
64. FERGUSON, Niels, Bruce SCHNEIER, et Tadayoshi KOHNO. *Cryptography Engineering: design principles and practical applications*. John Wiley & Sons. 2011.
65. FOSTER, James JF. *Digital influence mercenaries, profits and power through information warfare*. US Naval Institute Press. 2022. *Étude sur les acteurs d'influence privés avec une présentation de leurs méthodes et effets sur la population ciblée.*
66. FOURASTIER, Yannick et Ludovic PIETRE-CAMBACEDES. *Cybersécurité des installations industrielles : défendre ses systèmes numériques*. Cépaduès. 2015. *Destiné aux acteurs de la sécurité informatique dans le domaine des systèmes industriels.*

67. FREYSSINET, Eric. *La cybercriminalité en mouvement*. Hermes Science Publications. 2012.
68. FUTTER, Andrew. *Hacking The Bomb: Cyber Threats and Nuclear Weapons*. Georgetown University Press. 2018.
69. GALEOTTI, Mark. *The Weaponisation of Everything: A Field Guide to the New Way of War*. Yale University Press. 2022.
70. GASTINEAU, Pierre et Philippe VASSET. *Armes de déstabilisation massive. Enquête sur le business des fuites de données*. Fayard. 2017. *Enquête sur les groupes d'attaquants et entreprises privées spécialisées dans l'exfiltration de données et la publication ou revente de celles-ci à des fins lucratives ou de déstabilisation.*
71. GERGORIN, Jean-Louis et Léo ISACC-DOGNIN. *Cyber, la guerre permanente*. Les éditions du Cerf. 2018.
72. GOLDSTEIN, Guy-Philippe. *Babel minute zéro*. Folio Policier. 2010.
73. GOTTSCHALL, Jonathan. *The Storytelling Animal: How Stories Make Us Human*. Houghton Mifflin Harcourt. 2013. *Une des 5 références sur le sujet selon le Modern Warfare Institute de West Point.*
74. GREENBERG, Andy. *Les criminels de la cryptomonnaie. Traque au cœur du Dark Web*. Saint-Simon. 2022. *Traduction française par Henri Froment du livre Tracers in the Dark. Livre d'enquête consacré à l'utilisation des crypto-monnaies par des groupes cyber-criminels.*
75. GREENBERG, Andy. *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*. Anchor. 2019.
76. GUEGUEN, Nicolas. *Psychologie la manipulation et la soumission*. Dunod. 2021. *Une recherche universitaire sur la manipulation et la soumission un bon follow up a* Petit traité de manipulation à l'usage des honnêtes gens.
77. GUISNEL, Jean. *Guerres dans le cyberespace : services secrets et Internet*. La Découverte. 1995. *Un des premiers livres français d'investigation sur le monde du hacking, particulièrement sur les groupes US Legion of Doom (LoD) et Masters of Deception (MoD).*
78. GUYAUX, Jean. *L'espion des sciences : les arcanes et les arnaques scientifiques du contre-espionnage*. Flammarion. 2002. *Le général Jean Guyaux a été détaché comme conseiller scientifique à la direction de la Surveillance du territoire (DST) de 1984 et 1995. Ces mémoires comprennent une partie parlant de la DST face à l'émergence de la piraterie informatique et la surveillance d'internet.*
79. HARREL, Yannick. *La cyberstratégie russe*. NUVIS. 2013.
80. HECKER, Marc et Thomas RID. *War 2.0: Irregular Warfare in the information Age*. Praeger. 2009.
81. HEMEZ, Rémy. *Les opérations de déception, ruse et stratagèmes de guerre*. Perrin. 2022. *Ouvrage un peu éloigné du cyber mais on en parle quand même dans la partie sur la déception. Très intéressant et très complet sur l'histoire des ruses de guerre. Toujours utile en cybersécurité. Disponible prêt adhérents M82.*
82. HENNING, Lahmann. *Unilateral Remedies to Cyber Operations*. Cambridge University Press. 2020.
83. HENNION, Romain et Anissa MAKHLOUF. *La cybersécurité*. Eyrolles. 2018.
84. HENROTIN, Joseph. *L'art de la guerre à l'age des réseaux*. ISTE éditions. 2017.
85. HENROTIN, Joseph. *Techno-guérilla et guerre hybride : le pire des deux mondes*. Nuvis. 2014.
86. HERMAN, Michael. *Intelligence Services in the Information Age*. Routledge. 2002.
87. HEUER, Richards J. *Psychology of Intelligence Analysis*. Center for the Study of Intelligence. 1999. *Un indispensable pour tout analyste traitant de la donnée en vue de fournir du renseignement.*
88. HUBBARD, Douglas W et Richard SEIERSEN. *How to measure anything in cybersecurity risk*. John Wiley & Sons. 2023.
89. HUYGHE, François-Bernard. *La désinformation, les armes du faux*. Armand Colin. 2016.
90. HUYGHE, François-Bernard, Olivier KEMPF, et Nicolas MAZZUCCHI. *Gagner les cyberconflits, au-delà du technique*. Economica. 2015. *Un essai*

particulièrement accessible qui propose une réflexion sur comment progressivement les algorithmes ont bouleversé notre quotidien. Disponible prêt adhérents M82.

91. HYPPÖNEN, Mikko. *If it's smart, it's vulnerable*. Wiley. 2022.
92. JAMIESON, Kathleen Hall. *Cyberwar: how Russian hackers and trolls helped elect a president: what we don't, can't, and do know*. Oxford University Press. 2020.
93. JANCZEWSKI, Lech et Andrew COLARIK. *Cyber warfare and Cyberterrorism*. IGI Global. 2007.
94. JANKOWICZ, Nina. *How to lose the Information War: Russia, Fake News and the Future of Conflict*. Bloomsbury Publishing. 2020.
95. JEAN, Aurélie. *De l'autre côté de la machine*. L'Observatoire. 2019. *Disponible prêt adhérents M82.*
96. JOULE, Robert-Vincent, Jean-Léon BEAUVOIS, et Jean Claude DESCHAMPS. *Petit traité de manipulation à l'usage des honnêtes gens*. Presses universitaires de Grenoble Grenoble. 1987.
97. KAISER, Brittany. *Targeted*. Harper Collins Publishers. 2019.
98. KAPLAN, Fred. *Dark Territory: The Secret History of Cyber War*. Simon and Schuster. 2016.
99. KEMPF, Olivier. *Introduction à la cyberstratégie*. Economica. 2012. *Disponible prêt adhérents M82.*
100. KITCHIN, Rob. *The Data Revolution: Big Data, Open Data, Data Infrastructures and Their Consequences*. SAGE. 2014.
101. KLIMBURG, Alexander. *The Darkening Web: The War for Cyberspace*. Penguin Press. 2018.
102. KRAMER, Franklin, Stuart STARR, et Larry WENTZ. *Cyberpower and National Security. National Defense*. Georgetown University Press. 2009.
103. LAFOURCADE, Pascal et Cristina ONETE. *20 énigmes ludiques pour se perfectionner en cryptographie*. Dunod. 2023. *À écouter, l'épisode de NoLimit Sécu : https://www.nolimitsecu.fr/20-enigmes-ludiques-pour-se-perfectionner-en-cryptographie/*
104. LAMDAN, Sarah. *Data cartels: The companies that control and monopolize our information*. Stanford University Press. 2022.
105. LAMY, Stéphanie. *Agora toxica*. éditions du détour. 2022. *Disponible prêt adhérents M82.*
106. LAURENT, Sébastien-Yves. *Conflits, crimes et régulations dans le cyberespace*. ISTE Group. 2021. vol.4.
107. LE DEZ, Arnaud. *Tactique cyber, le combat numérique*. Economica. 2019.
108. LEBRUMENT, Fabien, Chantal et Soyez. *Louis Pouzin, l'un des péres de l'internet*. Economica. 2018. *Un éclairage sur un français à l'origine de l'Internet, une figure des débuts des réseaux.*
109. LEE, Marin. *Cyber Threat Intelligence*. Wiley. 2023.
110. LEJEUNE, Yannick et EPITA. *Big, fast, Open Data : décrire, décrypter et prédire le monde : l'avènement des données*. FYP. 2014.
111. LEONETTI, Xavier et Christiane FERAL-SCHULL. *Cybersécurité mode d'emploi : entreprise, monde numérique et protection des données personnelles : 57 fiches réflexes*. PUF. 2022.
112. LESSIG, Lawrence. *Code: And other laws of cyberspace*. ReadHowYouWant. com. 2009.
113. LEVINE, Yasha. *Surveillance Valley, The Secret Military History of the Internet*. Public Affairs. 2018.
114. LIANG, Qiao et Wang XIANGSUI. *La guerre hors limites*. Les éditions du Cerf. 1999. *Incontournable (entre autres) sur la pensée cyber chinoise.*
115. LIBICKI, Martin. *Cyberdeterrence and Cyberwar*. RAND Corporation. 2009.
116. LIBICKI, Martin. *Conquest in cyberspace: national security and information*. Cambridge University Press. 2007.
117. LIGH, Michael, Steven ADAIR, Blake HARTSTEIN, et al. *Malware analyst's cookbook and DVD: tools and techniques for fighting malicious code*. Wiley Publishing. 2010.
118. LILLY, Bilyana. *Russian Information Warfare: assault on democracies in the cyber wild west*. Naval Institute Press. 2022.
119. LIMONIER, Kevin. *Ru.net*. édition de l'Inventaire. 2018.

120. LONSDALE, David J. *The Nature of War in the Information Age: Clausewitzian future*. Frank Cass. 2004.
121. MAURER, Tim. *Cyber Mercenaries : The State, Hackers, and Power*. Cambridge University Press. 2018.
122. MENN, Joseph. *Cult of the Dead Cow: how the original hacking Supergroup might just save the world*. PublicAffairs. 2019.
123. MITNICK, Kevin. *Ghost in the Wires: My Adventures as the World's Most Wanted Hacker*. Back Bay Books. 2012.
124. MITNICK, Kevin D et William L SIMON. *The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders and Deceivers*. John Wiley & Sons. 2005. *Disponible prêt adhérents M82.*
125. MITNICK, Kevin D et William L SIMON. *The Art of Deception: Controlling the Human Element of Security*. John Wiley & Sons. 2003.
126. MONTE, Matthew. *Network Attacks and Exploitation*. Wiley. 2015.
127. MOORE, Daniel. *Offensive Cyber Operations*. Hurst. 2022.
128. MOREL, Camille. *Les câbles sous-marins*. CNRS. 2023. *Excellent ouvrage sur une thématique centrale pour comprendre les enjeux du numérique. Disponible prêt adhérents M82.*
129. MOTTE, Martin. *La mesure de la force*. Taillandier. 2018. *Ouvrage qui ne traite pas uniquement de cyber mais de stratégie au sens large, un chapitre couvre les enjeux du combat à l'ère numérique.*
130. NYE, Joseph. *Cyberpower*. Harvard University. 2010.
131. O'HARA, Kieron et Wendy HALL. *Four Internets: Data, Geopolitics, and the Governance of Cyberspace*. Oxford University Press. 2021.
132. PANDORAS, Groupe. *cybersécurité : méthode de gestion de crise*. VA-ÉDITIONS. 2021.
133. PATINO, Bruno. *Tempête dans le bocal, la nouvelle civilisation du poisson rouge*. Grasset. 2022.
134. PATINO, Bruno. *La civilisation du poisson rouge. Petit traité sur le marché de l'attention*. Grasset. 2019.
135. PAYNE, Kenneth. *I, Warbot: The Dawn of Artificially Intelligent Conflict*. Oxford University Press. 2021.
136. PENALBA, Pierre. *Cyber crimes : un flic 2.0 raconte*. Albin Michel. 2020.
137. PERKOVICH, George et Levite ARIEL. *Understanding Cyber conflict: 14 analogies*. Georgetown University Press. 2017.
138. PERLROTH, Nicole. *This is How they Tell me the World Ends: the Cyberweapons Arms Race*. Bloomsburry Publishing. 2021.
139. PERNET, Cédric. *Sécurité et espionnage informatique*. Eyrolles. 2014. *Maitriser sa sécurité signifie que l'on doit comprendre les menaces auxquelles il faut faire face et c'est justement l'objet de ce livre consacré aux APT. Les APT, pour Advanced Persistent Threats, sont les menaces du haut du spectre (étatiques ou criminelles). L'auteur va ainsi définir ce terme qui fait débat au sein de la communauté cyber avant d'en décrire les différentes phases. L'exposé est enrichi d'exemples concrets et aborde certains aspects techniques. Il ne couvre cependant pas les actions à mener pour répondre à ce type de menace (la réponse à incident). Pour les débutants, il est intéressant de noter que si les APT sont des menaces avec un impact potentiel élevé, il ne s'agit pas forcément des attaques les plus sophistiquées techniquement.*
140. PETROV, Victor. *Balkan Cyberia: Cold War Computing, Bulgarian Modernization, and the Information Age behind the Iron Curtain*. MIT Press. 2023.
141. PHARO, Patrick. *Les data contre la liberté*. PUF. 2022.
142. PILLOU, Jean-Philippe, Jean-François et Bay. *Tout sur la sécurité informatique*. Dunod. 2020. *Excellent ouvrage généraliste pour bien débuter avec les bases du domaine.*
143. POMERANTSEV, Peter. *This Is Not Propaganda : Adventures in the War Against Reality*. Faber & Faber. 2019.
144. PORCHE, Isaac. *Cyberwarfare: An Introduction to Information-Age Conflict*. Artech House. 2019.

145. QUEMENER, Myriam et Joël FERRY. *Cybercriminalité : défi mondial et réponse*. Economica. 2007.
146. QUESARD, Céline, Maud et Marangé. *Les guerres de l'information à l'ère numérique*. PUF. 2021.
147. RAIMONDO, Laurane. *Les fondamentaux de la gestion de crise cyber*. Ellipses. 2022.
148. RAINS, Tim. *Cybersecurity Threats, Malware Trends, and Strategies: Discover risk mitigation strategies for modern threats to your organization*. Packt Publishing Ltd. 2023.
149. RAINS, Tim. *Cybersecurity Threats, Malware Trends, and Strategies: Learn to mitigate exploits, malware, phishing, and other social engineering attacks*. Packt Publishing Ltd. 2020.
150. RASCAGNERES, Paul et Sébastien LARINIER. *Cybersécurité et Malwares. Détection, analyse et Threat Intelligence*. ENI. 2022. *4ème édition (2022) d'un livre de référence sur le sujet.*
151. RATTRAY, Gregory. *Strategic warfare in cyberspace*. Mass MIT Press. 2001.
152. RAUFAST, Pierre. *Habemus piratam*. Forges Vulcain. 2022. *Un très bon roman français dans le domaine cyber/hacking, auteur membre de l'équipe SSI chez Michelin.*
153. RID, Thomas. *Active Measures: The Secret History of Disinformation and Political Warfare*. Profile Books Ltd. 2020. *Fait partie des 5 recommandations de lecture sur le sujet par le Modern Warfare Institue de West Point.*
154. RID, Thomas. *Cyber War will not take place*. Oxford University Press. 2013. *Excellent livre qui ne perd rien de son actualité, fait partie des 5 recommandations de lecture sur le sujet par le Modern Warfare Institue de West Point*
155. ROBERTS, Scott J. et Rebekah BROWN. *Intelligence-Driven Incident Response*. O'Reilly Media. 2023. *Un livre sur le renseignement appliqué à la réponse à incident, donc la CTI.*
156. ROCCIA, Thomas. *Visual Threat Intelligence, An illustrated Guide For Threat Researchers*. 2023. *Livre numérique pour l'instant, disponible au lien suivant https://store.securitybreak.io/threatintel*
157. ROGER, Grimes. *Hacking the Hacker: Learn From the Experts Who Take Down Hackers*. Wiley. 2017.
158. ROSCINI, Marco. *Cyber Operations and the Use of Force in International Law*. Oxford University Press. 2014.
159. ROUX, Thierry. *L'art de la guerre cyber : vers une intelligence des crises*. Nunkee Editions. 2020.
160. SALAMON, Yann. *Cybersécurité et Cyberdéfense : enjeux stratégiques*. Ellipses. 2020. *S'adressant à un panel de publics divers, cet ouvrage balaie un large panorama de sujets structurants liés à la sécurité numérique. Prenant comme point de départ la compréhension du cyberespace, il en décrit quelques propriétés importantes : tendances, enjeux, caractéristiques « topologiques », acteurs en présence.*
161. SALOBIR, Eric. *Dieu et la silicon valley*. Buchet Chastel. 2020. *Disponible prêt adhérents M82.*
162. SANGER, David. *The Perfect Weapon: War, Sabotage and Fear in the Cyber Age*. Crown. 2018.
163. SANGER, David. *Confront and Conceal: Obama's secret wars and surprising use of American power*. Crown. 2012. *Un livre à lire pour comprendre l'histoire récente des conflits numériques et la conduite de cette guerre par l'administration Obama.*
164. SARFRAZ, Muhammad. *Cybersecurity Threats with New Perspectives*. BoD–Books on Demand. 2021.
165. SCHMITT, Michael N. et Liis VIHUL. *Tallinn manual 2.0 on the international law applicable to cyber operations*. Cambridge university press. 2017.
166. SCHNEIER, Bruce. *Secrets and Lies: Digital Security in a Networked World*. John Wiley & Sons. 2004.
167. SCHNEIER, Bruce. *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. John Wiley & Sons. 1996.
168. SCHRADIE, Jen. *L'illusion de la démocratie numérique. Internet est-il de droite ?* Quanto. 2022.

169. SCOTT CARD, Orson. *Ender's Game*. Mass Market Paperback. 1985. *Ce roman de science-fiction est une des 5 références sur le sujet selon le Modern Warfare Institute de West Point.*
170. SEJEAN, Michel. *Code de la cybersécurité*. Lefevre Dalloz. 2023. *Un incontournable pour ceux qui souhaitent maitriser le droit associé à la cybersécurité.*
171. SHEVELYOV, Nicholas. *Cyber War... and Peace: Building Digital Trust Today with History as Our Guide*. Lioncrest Publishing. 2017.
172. SHIMOMURA, Tsutomu et John MARKOFF. *Cybertraque : la chasse au pirate informatique le plus célèbre des États-Unis*. Plon. 1998. *Traduction française de* Katching Kevin*, récit du hack et de la traque de Kevin Mitnick en 1995.*
173. SHIRKY, Clay. *Cognitive Surplus: Creativity and Generosity in a Connected Age*. Penguin Press. 2010.
174. SIKORSKI, Michael et Andrew HONIG. *Practical Malware Analysis: the Hands-On Guide to Dissecting Malicious Software*. No Starch Press. 2012.
175. SINGER, P.W et Emerson T BROOKING. *LikeWar: The Weaponization of Social Media*. Mariner Books. 2019.
176. SINGER, P.W et August COLE. *La flotte fantôme*. Folio. 2022. *Roman. Disponible prêt adhérents M82.*
177. SMEETS, Max. *No Shortcuts. Why States Struggle to Develop a Military Cyber-Force*. Oxford University Press. 2022.
178. STAMBOLIYSKA, Rayna. *La face cachée d'internet : hackers*. Larousse. 2017.
179. STEFFENS, Timo. *Attribution of Advanced Persistent Threat*. Springer Vieweg. 2020. *Un livre qui traite en profondeur la problématique de l'attribution, mais aussi l'ensemble des concepts clés de la CTI.*
180. STENGEL, Richard. *Information Wars: How We Lost the Global Battle Against Disinformation and What We Can Do About It*. Atlantic Monthly Press. 2019.
181. STEVENS, Tim. *Cyber security and the politics of time*. Cambridge University Press. 2016.
182. STOLL, Clifford. *The Cuckoo's Egg*. Doubleday. 1989.
183. TARISSAN, Fabien. *Au coeur des réseaux, des sciences aux citoyens*. Le Pommier. 2019.
184. THAMES, Lane et Dirk SCHAEFER. *Cybersecurity for industry 4.0*. Springer. 2017.
185. TRIFFAULT, Alexandre. *The Little Black Book of Lockpicking: Lock opening and Bypass techniques for Security Professionals*. Publication indépendante. 2021.
186. TROIA, Vinny. *Hunting Cyber Criminals: A Hacker's Guide to Online Intelligence Gathering Tools and Techniques*. John Wiley & Sons. 2020.
187. VALERIANO, Brandon et C MANESS Ryan. *Cyber war versus cyber realities: Cyber conflict in the international system*. Oxford University Press. 2015.
188. VAN PUYVELDE, Damien et Aaron F. BRANTLY. *Cybersecurity. Politics, Governance and Conflict in Cyberspace*. John Wiley & Sons. 2019.
189. VENTRE, Daniel. *Information Warfare*. Wiley. 2016.
190. VENTRE, Daniel. *Cyberattaque et cyberdéfense*. Lavoisier. 2011. *Disponible prêt adhérents M82.*
191. VENTRE, Daniel. *Cyberguerre et guerre de l'information. Stratégie, règles et enjeux*. Lavoisier. 2010.
192. VENTRE, Daniel. *La guerre de l'information*. Lavoisier. 2007.
193. VOLKOFF, Vladimir. *La désinformation : arme de guerre*. l'Age d'homme. 2004.
194. ZALEWSKI, Michal. *The Tangled Web: A Guide to Securing Modern Web Applications*. No Starch Press. 2011.
195. ZALEWSKI, Michal. *Menaces sur le réseau, Sécurité informatique : guide pratique des attaques passives et indirectes*. CampusPresse. 2008. *Superbe livre pour s'initier à la sécurité informatique au niveau réseau/protocolaire. Version française du livre publié en 2005* Silence on the Wire.
196. ZEGART, Amy. *Spies, Lies, and Algorithms: The History and Future of American Intelligence*. Princeton. 2022.
197. ZETTER, Kim. *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. Crown. 2014.

198. ZITTRAIN, Jopnathan. *The future of the Internet: And How to Stop it*. Yale University Press. 2008.
199. ZUBOFF, Shoshana. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. Profile Books Ltd. 2019.