# BIBLIOGRAPHIE
## cyberdéfense, cybersécurité, guerre de l'information

## Édition février 2023

Pour contribuer **Le pad**
Pour s'informer **Le Twitter**
Pour participer à la biblio **Le Telegram**
Pour nous lire **Le blog**


1. Abiteboul, Serge et Jean Cattan. *Nous sommes les réseaux sociaux*. Odile Jacob. 2022.
2. ADAIR, Steven, Michael LIGH, Blake HARTSTEIN, et al. *Malware analyst's Cookbook*. Wiley. 2011.

Une référence pour s'initier à l'analyse de codes malveillants.

3. AGENCE NATIONALE DE LA SECURITE DES SYSTEMES D'INFORMATION. *Maîtrise du risque numérique, l'atout confiance*. Agence nationale de la sécurité des systèmes d'information. 2019.
4. 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.

5. ANDERSON, Chris. *La longue traine*. Pearson. 2012.
6. ARPAGIAN, Nicolas. *Frontières.com*. L'Observatoire. 2022.
7. ARPAGIAN, Nicolas. *La cybersécurité*. PUF. 2018.

8. ARPAGIAN, Nicolas. La cyberguerre, la guerre numérique a commencé. Vuibert. 2009.
9. ARQUILLA, John. *Bitskrieg, the new challenge of cyberwarfare*. Polity. 2021.
10. ARQUILLA, John et David RONFELDT. *Networks and Netwar: the Future of Terror, Crime and Militancy*. Rand. 2002.
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. BILLOIS, Jérome et Nicolas COUGOT. *Cyberattaques, les dessous d'une menace mondiale*. Hachette. 2022.
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.
20. BOYER, Bertrand. *Guérilla 2.0, guerres irrégulières dans le cyberespace*. École de Guerre. 2020.
21. BOYER, Bertrand. *Cybertactique, conduire la guerre numérique*. NUVIS. 2014.
22. BOYER, Bertrand. *Cyberstratégie, l'art de la guerre numérique*. NUVIS. 2012.
23. BRENNER, Susan. *Cyberthreats, the emerging fault line of the Nation State*. Oxford University Press. 2009.
24. BRONNER, Gérald. *Apocalypse cognitive*. PUF. 2021.
25. BRUNTON, Finn et Helen NISSENBAUM. *Obfuscation: a User's Guide for Privacy and Protest*. The MIT Press. 2015.

26. BRYANT, William. *International Conflict and Cyberspace superiority*. Routledge. 2016.
27. BUCHAN, Russell. *Cyberespionage and international law*. Hart Publishing. 2018.
28. BUCHANAN, Ben. *The Hacker and the state: the New Normal of Geopolitics*. Harvard University Press. 2020.
29. BUCHANAN, Ben. *The Cybersecurity Dilemna: Hacking, Trust and Fear Between Nations*. C Hurst Co Publishers. 2019.
30. BULINGE, Franck. *De l'espionnage au renseignement*. Vuibert. 2012.
31. CARDON, Dominique. *À quoi rêvent les algorithmes : nos vies à l'heure des Big data*. Média Diffusion. 2015.
32. CARR, Jeffrey. *Inside Cyber Warfare, mapping the cyber underworld*. O'Reilly. 2009.
33. CATTARUZZA, Amaël, Didier DANET, et Stéphane TAILLAT. *La cyberféfense, politique de l'espace numérique*. Armand Colin. 2023.
2ème édition. Mise à jour en 2023.
34. CHAVALARIAS, David. *Toxic Data*. Flammarion. 2022.
35. CHESNEY, Robert et Max SMEETS. *Deter, Disrupt, or Deceive*. Georgetown University Press. 2023.
36. CLANCY, Tom. *Cybermenace*. Albin Michel. 2013.
37. CLARKE, Richard et Robert KNAKE. *Cyberwar: the next Threat to National Security and what to do about it*. Ecco Press. 2010.
38. CLOUGH, Jonathan. *Principles of cybercrime*. Cambridge University Press. 2015.
39. DAHJ, Jean Nestor. *Mastering Cyber Intelligence: Gain comprehensive knowledge and skills to conduct threat intelligence for effective system defense*. Packt Publishing. 2022.
40. DELERUE, François. *Cyberoperations and International Law*. Cambridge University Press. 2020.
41. DENARDIS, Laura. *The Internet in everything*. Yale University Press. 2020.

42. 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.
43. DOSSE, Stéphane et Aymeric BONNEMAISON. *Attention cyber ! Vers le combat cyber-electronique*. Économica. 2014.
44. DOSSE, Stéphane et Olivier KEMPF. *Stratégie dans le cyberespace*. L'esprit du livre. 2011.
45. DOSSE, Stéphane, Olivier KEMPF, et Christian MALIS. *Cyberespace, nouveau domaine de la pensée stratégique*. Économica. 2013.
46. DYKSTRA, Josiah, Metcalf LEIGH, et Eugene SPAFFORD. *Cybersecurity myths and Misconceptions*. Pearson Education. 2023.
47. ELSBERG, Marc. *Black-out : demain il sera trop tard*. LGF. 2016.
48. FAILLET, Caroline. *L'art de la guerre digitale, survivre et dominer à l'ère du numérique*. Dunod. 2016.
49. FOSTER, James. Digital influence mercenaries, profits and power through information warfare. US Naval Institute Press. 2022.
50. FREYSSINET, Eric. *La cybercriminalité en mouvement*. Hermes Science Publications. 2012.
51. FUTTER, Andrew. *Hacking The Bomb: Cyber Threats and Nuclear Weapons*. Georgetown University Press. 2018.
52. GALEOTTI, Mark. *The Weaponisation of Everything: a Field Guide to the New Way of War*. Yale University Press. 2022.
53. 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.
54. GERGORIN, Jean-Louis et Léo ISACC-DOGNIN. *Cyber, la guerre permanente*. Les éditions du Cerf. 2018.
55. GOLDSTEIN, Guy-Philippe. *Babel minute zéro*. Galimard. 2010.

56. GREENBERG, Andy. *Sandworm: a New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*. Doubleday. 2019.
57. GROUPE PANDORAS. *Cybersécurité : méthode de gestion de crise*. VA-EDITIONS. 2021.
58. 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)
59. 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.
60. HARREL, Yannick. *La cyberstratégie russe*. NUVIS. 2013.
61. HECKER, Marc et Thomas RID. *War 2.0: Irregular Warfare in the information Age*. Praeger. 2009.
62. HENNING, Lahmann. *Unilateral Remedies to Cyber Operations*. Cambridge University Press. 2020.
63. HENNION, Romain et Anissa MAKLHOUF. *La cybersécurité*. Eyrolles. 2018.
64. HENROTIN, Joseph. *L'art de la guerre à l'age des réseaux*. ISTE éditions. 2017.
65. HUBBARD, Douglas W et Richard SEIERSEN. *How to measure anything in cybersecurity risk*. John Wiley & Sons. 2023.
66. HUYGHE, François-Bernard. *La désinformation, les armes du faux*. Armand Colin. 2016.
67. HUYGHE, François-Bernard, Olivier KEMPF, et Nicolas MAZZUCCHI. *Gagner les cyberconflits, au-delà du technique*. Economica. 2015.
68. HYPPONEN, Mikko. *If it's smart, it's vulnerable*. Wiley. 2022.

69. JANCZEWSKY, Lech et Andrew COLARIK. *Cyber warfare and Cyberterrorism*. Information Science Reference. 2007.
70. JANKOWICZ, Nina. *How to lose the Information War*. Bloomsbury. 2020.
71. KAPLAN, Fred. *Dark Territory: the Secret History of Cyber War*. Simon and Schuster. 2016.
72. KEMPF, Olivier. *Introduction à la cyberstratégie*. Economica. 2012.
73. KITCHIN, Rob. *The Data Revolution: Big Data, Open Data, Data Infrastructures and Their Consequences*. SAGE. 2014.
74. KLIMBURG, Alexander. *The Darkening Web: The War for Cyberspace*. Penguin Press. 2017.
75. KRAMER, Franklin, Stuart STARR, et Larry WENTZ. *Cyberpower and National Security. National Defense*. University Press and potomac books. 2009.
76. LAURENT, Sébastien-Yves. *Conflits, crimes et régulations dans le cyberespace*. ISTE Group. 2021. vol.4.
77. LE DEZ, Arnaud. *Tactique cyber, le combat numérique*. Économica. 2019.
78. LEONETTI, Xavier et Christiane FÉRAL-SCHULL. *Cybersécurité mode d'emploi*. PUF. 2022.
79. LESSIG, Lawrence. *Code: And other laws of cyberspace*. ReadHowYouWant. com. 2009.
80. LEVINE, Yasha. Surveillance Valley. *The Secret Military History of the Internet*. Public Affairs. 2018.
81. LIANG, Qiao et Wang XIANGSUI. *La guerre hors limites*. Les éditions du Cerf. 1999.
Incontournable (entre autres) sur la pensée cyber chinoise.
82. LIBICKI, Martin. *Cyberdeterrence and Cyberwar*. RAND Project Air force. 2009.
83. LIBICKI, Martin. *Conquest in cyberspace: national security and information*. Cambridge University Press. 2007.
84. LILLY, Bilyana. *Russian Information Warfare*. Naval Institute Press. 2022.
85. LIMONIER, Kevin. *Ru.net*. Éditions de l'Inventaire. 2018.

86. LONSDALE, David. *The Nature of War in the Information Age*. Frank Cass. 2004.
87. MAURER, Tim. *Cyber Mercenaries: The State, Hackers, and Power*. Cambridge University Press. 2018.
88. MENN, Joseph. *Cult of the Dead Cow*. PublicAffairs. 2019.
89. MERCIER, Arnaud et Nathalie PIGNARD-CHEYNEL (eds.). *#Info : commenter et partager l'actualité sur Twitter et Facebook*. Fondation Maison des sciences de l'Homme. 2018.
90. MITNICK, Kevin. *Ghost in the Wires: my Adventures as the World's Most Wanted Hacker*. Back Bay Books. 2012.
91. MITNICK, Kevin. *The Art of Intrusion: the Real Stories Behind the Exploits of Hackers, Intruders and Deceivers*. John Wiley & Sons. 2005.
92. MITNICK, Kevin. *The Art of Deception. Controlling the Human Element of Security*. John Wiley & Sons. 2003.
93. MONTE, Matthew. *Network Attacks and Exploitation*. Wiley. 2015.
94. MOORE, Daniel. *Offensive Cyber Operations*. Hurst. 2022.
95. MOTTE, Martin. *La mesure de la force*. Taillandier. 2018.
96. NYE, Joseph. *Cyberpower*. Harvard University. 2010.
97. PATINO, Bruno. *Tempête dans le bocal, la nouvelle civilisation du poisson rouge*. Grasset et Fasquelle. 2022.
98. PATINO, Bruno. *La civilisation du poisson rouge, Petit traité sur le marché de l'attention*. Grasset et Fasquelle. 2019.
99. PAYNE, Kenneth. *I, Warbot: the Dawn of Artificially Intelligent Conflict*. Hurst Publishers. 2021.
100. PELROTH, Nicole. *This is How they Tell me the World Ends: the Cyberweapons Arms Race*. Bloomsburry Publishing. 2021.
101. PENALBA, Pierre. *Cyber crimes : un flic 2.0 raconte*. Albin Michel. 2021.
102. PERKOVICH, George et Levite ARIEL. *Understanding Cyber conflict: 14 analogies*. Georgetown University Press. 2017.
103. PERNET, Cédric. *Sécurité et espionnage informatique*. Eyrolles. 2014.
104. PHARO, Patrick. *Les data, contre la liberté*. PUF. 2022.

105. PORCHE, Isaac. *Cyberwarfare: an Introduction to Information-Age Conflict*. Artech House. 2019.

106. QUEMENER, Myriam et Joël FERRY. *Cybercriminalité : défi mondial et réponse*. Economica. 2007.

107. RAIMONDO, Laurane. *Les fondamentaux de la gestion de crise cyber*. Ellipses. 2022.

108. RASCAGNERES, Sébastien, Paul et Larinier. *Cybersécurité et malwares. Détection, analyse et threat Intelligence*. ENI. 2022.

4ème édition (2022) d'un livre de référence sur le sujet.

109. RATTRAY, Gregory. *Strategic warfare in cyberspace*. Mass MIT Press. 2001.

110. 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.

111. RID, Thomas. *Active Measures: The Secret History of Disinformation and Political Warfare*. Profile Books Ltd. 2020.

112. RID, Thomas. *Cyber War will not take place*. Oxford University Press. 2013.

113. ROUX, Thierry. *L'art de la guerre cyber : vers une intelligence des crises*. Nunkee Editions. 2020.

114. 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.

115. SANGER, David. *The Perfect Weapon: War, Sabotage and Fear in the Cyber Age*. Crown. 2019.

116. SANGER, David. *Confront and Conceal: Obama's secret wars*. Crown. 2012.

117. SCHMITT, Michael N. et Liis VIHUL. *Tallinn manual 2.0 on the international law applicable to cyber operations*. Cambridge university press. 2017.

118. SCHNEIER, Bruce. *Cryptography Engineering*. John Wiley & Sons. 2010.
119. SCHNEIER, Bruce. *Secrets and Lies: Digital Security in a Networked World*. John Wiley & Sons. 2004.
120. SCHNEIER, Bruce. *Applied Cryptography*. John Wiley & Sons. 1996.
121. SEJEAN, Michel. *Code de la Cybersécurité*. Lefevre Dalloz. 2022.
122. SHIMOMURA, Tsutotmu et John MARKOFF. *Cybertraque. La chasse au pirate informatique le plus célèbre des Etats-Unis*. Plon. 1998.
Traduction FR de "Katching Kevin", récit du hack et de la traque de Kevin Mitnick en 1995.
123. SHIRKY, Clay. *Cognitive Surplus: Creativity and Generosity in a Connected Age*. Penguin Press. 2010.
124. SIKORSKI, Michael et Andrew HONIG. *Practical Malware Analysis: the Hands-On Guide to Dissecting Malicious Software*. No Starch Press. 2012.
125. SINGER, P.W et August COLE. *La flotte fantôme*. Folio. 2022.
126. SMEETS, Max. *No Shortcuts. Why States Struggle to Develop a Military Cyber-Force*. Hurst. 2022.
127. STAMBOLIYSKA, Rayna. *La face cachée d'internet : hackers*. Larousse. 2017.
128. STEVENS, Tim. *Cyber security and the politics of time*. Cambridge University Press. 2016.
129. STOLL, Clifford. *The Cuckoo's Egg*. New York: Doubleday. 1989.
130. TARISSAN, Fabien. *Au cœur des réseaux, des sciences aux citoyens*. Le Pommier. 2019.
131. TRIANDAFILLIDOU, Olga. *Cybermenaces, un état de siège*. alsyse-news.com. 2019.
132. TRIFFAULT, Alexandre. *The Little Black Book of Lockpicking: Lock opening and Bypass techniques for Security Professionals*. Amazon. 2021.
133. TROIA, Vinny. *Hunting Cyber Criminals: A Hacker's Guide to Online Intelligence Gathering Tools and Techniques*. Sybex Inc. 2020.
134. VAN PUYVELDE, Damien et Aaron F. BRANTLY. *Cybersecurity. Politics, Governance and Conflict in Cyberspace*. Polity. 2019.

135. VENTRE, Daniel. *Information Warfare*. ISTE Wiley. 2016.

136. VENTRE, Daniel. *Cyberattaque et cyberdéfense*. Lavoisier. 2011.

137. VENTRE, Daniel. *Cyberguerre et guerre de l'information. Stratégie, règles et enjeux*. Lavoisier. 2010.

138. VENTRE, Daniel. *La guerre de l'information*. Lavoisier. 2007.u

139. VOLKOFF, Vladimir. *La désinformation : arme de guerre*. L'Age d'homme. 2004.

140. ZALEWSKI, Michal. *The Tangled Web: A Guide to Securing Modern Web Applications*. No Starch Press. 2011.

141. ZALEWSKI, Michal. Menaces sur le réseau. Sécurité informatique : guide pratique des attaques passives et indirectes. Pearson. 2008.
Superbe livre pout s'initier à la sécurité informatique au niveau réseau/protocolaire. Version FR du livre publié en 2005 "Silence on the Wire".

142. ZEGART, Amy. *Spies, Lies, and Algorithms: the History and Future of American Intelligence*. Princeton. 2022.

143. ZETTER, Kim. *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. Crown. 2014.

144. ZUBOFF, Shoshana. *The Age of Surveillance Capitalism: the Fight for a Human Future at the New Frontier of Power*. Profile Books Ltd. 2019.