Pad Bibliographie Cyber

Taken from M82 pad: `urlz.fr/j3c3`. Twitter account: `https://twitter.com/M82_project`

References

[1] Will Allsopp. *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 oeuvre par des attaquants.

[2] Nicolas Arpagian. *La cyberguerre, la guerre numérique a commencé.* Vuibert, 2009.

[3] Nicolas Arpagian. *La cybersécurité.* PUF, 2018.

[4] Nicolas Arpagian. *Frontières.com.* L'Observatoire, 2022.

[5] John Arquilla. *Bitskrieg, the new challenge of cyberwarfare.* Polity, 2021.

[6] John Arquilla and David Ronfeldt. *Networks and Netwar : the Future of Terror, Crime and Militancy.* Rand, 2002. URL: `https://www.jstor.org/stable/10.7249/mr1382osd`.

[7] Ladistlav Bittman. *The Deception Game.* Ballantine Books, 1981.

[8] Ladistlav Bittman. *The KGB and Soviet Disinformation: An Insider's View.* Brassey's Inc, 1985.

[9] Olivier Blondeau. *Devenir Média - L'activisme sur Internet, entre défection et expérimentation.* Edition Amsterdam, 2007.

[10] Olivier Blondeau and Florent Latrive. *Libres enfants du savoir Numérique. Anthologie du Libre.* Editions de L'Eclat, 2000. Liber.

[11] Stéphane Bortzmeyer. *Cyberstructure, l'Internet un espace politique.* C&F Editions, 2018.

[12] Bertrand Boyer. *Cyberstratégie, l'art de la guerre numérique.* NUVIS, 2012.

[13] Bertrand Boyer. *Cybertactique, Conduire la guerre numérique.* NUVIS, 2014.

[14] Bertrand Boyer. *Guérilla 2.0, guerres irrégulières dans le cyberespace.* École de Guerre, 2020.

[15] Susan Brenner. *Cyberthreats, the emerging fault lineson the Nation State.* Oxford University Press, 2009.

[16] Gérald Bronner. *Apocalypse cognitive.* PUF, https://amzn.to/3TkNACJ, 2021.

[17] William Bryant. *International Conflict and Cyberspace superiority.* Routledge, 2016.

[18] Russell Buchan. *Cyberespionage and international law.* Hart Publishing, 2018.

[19] Ben Buchanan. *The Cybersecurity Dilemna : Hacking, Trust and Fear Between Nations.* C Hurst Co Publishers, 2019.

[20] Ben Buchanan. *The Hacker and the state: The New Normal of Geopolitics.* Harvard University Press, 2020.

[21] Franck Bulinge. *De l'espionnage au renseignement.* Vuibert, 2012.

[22] Jeffrey Carr. *Inside Cyber Warfare, mapping the cyber underworld.* O'Reilly, 2009.

[23] Amaël Cattaruzza, Didier Danet, and Stéphane Taillat. *La cyberféfense, politique de l'espace numérique.* Armand Colin, 2018.

[24] David Chavalarias. *Toxic Data.* Flammarion, 2022.

[25] Tom Clancy. *Cybermenace.* Albin Michel, 2013.

[26] Richard Clarke and Robert Knake. *Cyberwar: the next Threat to National Security and what to do about it.* Ecco Press, 2010.

[27] Jean Nestor Dahj. *Mastering Cyber Intelligence: Gain comprehensive knowledge and skills to conduct threat intelligence for effective system defense.* Packt Publishing, 2022.

[28] Yuri Diogénes and 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.

[29] Stéphane Dosse and Aymeric Bonnemaison. *Attention cyber ! Vers le combat cyber-electronique.* Economica, 2014.

[30] Stéphane Dosse and Olivier Kempf. *Stratégie dans le Cyberespace.* L'esprit du livre, 2011.

[31] Stéphane Dosse, Olivier Kempf, and Christian Malis. *Cyberespace, nouveau domaine de la pensée stratégique.* Economica, 2013.

[32] Marc Elsberg. *Black-out: demain il sera trop tard.* Piranha, 2015.

[33] Eric Freyssinet. *La cybercriminalité en mouvement.* Hermes Science Publications, 2012.

[34] Pierre Gastineau and 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.

[35] Jean-Louis Gergorin and Léo Isacc-Dognin. *Cyber, la guerre permanente.* Les éditions du Cerf, 2018.

[36] Andy Greenberg. *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers.* Doubleday, 2019.

[37] Jean Guyaux. *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.

[38] Marc Hecker and Thomas Rid. *War 2.0: Irregular Warfare in the information Age.* Praeger, 2009.

[39] Romain Hennion and Anissa Maklhouf. *La cybersécurité.* Eyrolles, 2018.

[40] Joseph Henrotin. *L'art d la guerre à l'age des réseaux*. ISTE éditions, 2017.

[41] François-Bernard Huyghe, Olivier Kempf, and Nicolas Mazzucchi. *Gagner les cyberconflits, au-delà du technique*. Economica, 2015.

[42] Mikko Hypponen. *If it's smart, it's vulnerable*. Wiley, 2022.

[43] Lech Janczewsky and Colarik Andrew. *Cyber warfare and Cyberterrorism*. Information Science Reference, 2007.

[44] Fred Kaplan. *Dark Territory: The Secret History of Cyber War*. Simon and Schuster, 2016.

[45] Olivier Kempf. *Introduction à la cyberstratégie*. Economica, 2012.

[46] Alexander Klimburg. *The Darkening Web: The War for Cyberspace*. Penguin Press, 2017.

[47] Franklin Kramer, Stuart Starr, and Larry Wentz. *Cyberpower and National Security. National Defense*. University Press and potomac books, 2009.

[48] Arnaud Le Dez. *Tactique cyber, le combat numérique*. Economica, 2019. Préface du Général Olivier BONNET DE PAILLERETS.

[49] Xavier Leonetti and Christiane Féral-Schull. *Cybersécurité Mode d'emploi*. PUF, 2022.

[50] Yasha Levine. *Surveillance Valley, The Secret Military History of the Internet*. Public Affairs, 2018.

[51] Qiao Liang and Wang Xiangsui. *La guerre hors limites*. Les éditions du Cerf, 1999. Incontournable (entre autres) sur la pensée cyber chinoise.

[52] Martin Libicki. *Conquest in cyberspace: national security and information*. Cambridge University Press, 2007.

[53] Martin Libicki. *Cyberdeterrence and Cyberwar*. RAND Project Air force, 2009.

[54] Bilyana Lilly. *Russian Information Warfare*. Naval Institute Press, 2022.

[55] David Lonsdale. *The Nature of War in the Information Age*. Frank Cass, 2004.

[56] Tim Maurer. *Cyber Mercenaries : The State, Hackers, and Power*. Cambridge University Press, 2018.

[57] Joseph Menn. *Cult of the Dead Cow*. PublicAffairs, 2019.

[58] Kevin Mitnick. *The Art of Deception - Controlling the Human Element of Security*. John Wiley & Sons, 2003.

[59] Kevin Mitnick. *The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders and Deceivers*. John Wiley & Sons, 2005.

[60] Kevin Mitnick. *Ghost in the Wires: My Adventures as the World's Most Wanted Hacker*. Back Bay Books, 2012.

[61] Matthew Monte. *Network Attacks and Exploitation*. Wiley, 2015.

[62] Daniel Moore. *Offensive Cyber Operations*. Hurst, 2022. https://www.hurstpublishers.com/book/offensive-cyber-operations/.

[63] Martin Motte. *La mesure de la force*. Taillandier, 2018.

[64] Agence nationale de la sécurité des systèmes d'information. *Maîtrise du risque numérique, l'atout confiance.* Agence nationale de la sécurité des systèmes d'information, 2019. URL: `https://www.ssi.gouv.fr/uploads/2019/11/anssi_amrae-guide-maitrise_risque_numerique-atout_confiance.pdf`.

[65] Joseph Nye. *Cyberpower.* Harvard University, 2010.

[66] Groupe Pandoras. *cybersécurité - méthode de gestion de crise.* VA-EDITIONS, 2021.

[67] Nicole Pelroth. *This is How they Tell me the World Ends: the Cyberweapons Arms Race.* Bloomsburry Publishing, 2021.

[68] Pierre Penalba. *Cyber crimes: Un flic 2.0 raconte.* Albin Michel, 2021.

[69] Cédric Pernet. *Sécurité et espionnage informatique.* Eyrolles, 2014.

[70] Myriam Quemener and Joël Ferry. *Cybercriminalité : défi mondial et réponse.* Economica, 2007.

[71] Laurane Raimondo. *Les fondamentaux de la gestion de crise cyber.* Ellipses, 2022.

[72] Gregory Rattray. *Strategic warfare in cyberspace.* Mass MIT Press, 2001.

[73] Pierre Raufast. *Habemus piratam.* Forges Vulcain, 2022. Un très bon roman français dans le domaine Cyber/Hacking, auteur membre de l'équipe SSI chez Michelin.

[74] Thomas Rid. *Cyber War will not take place.* Oxford University Press, 2013.

[75] Thomas Rid. *Active Measures: The Secret History of Disinformation and Political Warfare.* Profile Books Ltd, 2020.

[76] Thomas Rid and Marc Hecker. *War 2.0. Irregular warfare in the information age.* Praeger security international, 2009.

[77] Thierry Roux. *L'art de la guerre cyber : Vers une intelligence des crises.* Nunkee Editions, 2020.

[78] Yann Salamon. *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.

[79] David Sanger. *Confront and Conceal: Obama's secret wars.* Crown, 2012.

[80] David Sanger. *The Perfect Weapon: War, Sabotage and Fear in the Cyber Age.* Crown, 2019.

[81] Michael N. Schmitt and Liis Vihul. *Tallinn manual 2.0 on the international law applicable to cyber operations.* Cambridge university press, Cambridge, Royaume-Uni, 2017.

[82] Bruce Schneier. *Applied Cryptography.* John Wiley & Sons, 1996.

[83] Bruce Schneier. *Secrets and Lies: Digital Security in a Networked World.* John Wiley & Sons, 2004.

[84] Bruce Schneier. *Cryptography Engineering.* John Wiley & Sons, 2010.

[85] Adair Seven, Hale Michael, Hartsein Blake, and Matthew Richard. *Malware analyst's Cookbook.* Wiley, 2011. Une référence pour s'initier à l'analyse de codes malveillants.

[86] Clay Shirky. *Cognitive Surplus: Creativity and Generosity in a Connected Age.* Penguin Press, 2010. In Cognitive Surplus, Internet guru Clay Shirky forecasts the thrilling changes we will all enjoy as new digital technology puts our untapped resources of talent and goodwill to use at last.

[87] Michael Sikorski and Andrew Honig. *Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software.* No Starch Press, 2012.

[88] Max Smeets. *No Shortcuts. Why States Struggle to Develop a Military Cyber-Force.* Hurst, 2022.

[89] Rayna Stamboliyska. *La face cachée d'internet: hackers.* Larousse, 2017.

[90] Clifford Stoll. *The Cuckoo's Egg.* New York: Doubleday, 1989.

[91] Michel Séjean. *Code de la Cybersécurité.* Lefevre Dalloz, 2022.

[92] Olga Triandafillidou. *Cybermenaces, Un état de siège.* alsyse-news.com, 2019.

[93] Alexandre Triffault. *The Little Black Book of Lockpicking: Lock opening and Bypass techniques for Security Professionals.* Amazon, 2021.

[94] Vinny Troia. *Hunting Cyber Criminals: A Hacker's Guide to Online Intelligence Gathering Tools and Techniques.* Sybex Inc, 2020.

[95] Damien Van Puyvelde and Aaron F. Brantly. *Cybersecurity. Politics, Governance and Conflict in Cyberspace.* Polity, 2019.

[96] Daniel Ventre. *La guerre de l'information.* Lavoisier, 2007.

[97] Daniel Ventre. *Cyberguerre et guerre de l'information. Stratégie,règles et enjeux.* Lavoisier, 2010.

[98] Daniel Ventre. *Cyberattaque et cyberdéfense.* Lavoisier, 2011.

[99] Daniel Ventre. *Information Warfare.* ISTE Wiley, 2016.

[100] Michal Zalewski. *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".

[101] Michal Zalewski. *The Tangled Web: A Guide to Securing Modern Web Applications.* No Starch Press, 2011.

[102] Amy Zegart. *Spies, Lies, and Algorithms: The History and Future of American Intelligence.* Princeton, 2022. https://press.princeton.edu/books/hardcover/9780691147130/spies-lies-and-algorithms.

[103] Kim Zetter. *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon.* Crown, 2014. The story behind the virus that sabotaged Iran's nuclear efforts and shows how its existence has ushered in a new age of warfare.

[104] Shoshana Zuboff. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power.* Profile Books Ltd, 2019. The challenges to humanity posed by the digital future, the first detailed examination of the unprecedented form of power called "surveillance capitalism," and the quest by powerful corporations to predict and control us.