BIBLIOGRAPHY

Armerding, T. (2017). *How likely is a 'digital Pearl Harbor' attack on critical infrastructure.* Naked Security by Sophos. Retrieved 22 June 2022, from https://www.forbes.com/global/2004/0920/104_print.html?sh=1b514b9129c3

Altheide, D. (2006). *Terrorism and the Politics of Fear* (1st ed). Alta Mira Press.

Bendrath, R. (2003). The American Cyber-Angst and the Real World – Any Link?. In R. Latham, *Bombs and Bandwidth: The Emerging Relationship between Emerging Technology and Security*. The New Press.

Bush, G. (2001). *President Bush's speech on the U.S. PATRIOT Act*. Washington, D.C. Retrieved 1 June 2022 from https://www.commonlit.org/en/texts/president-bush-on-the-patriot-acts.

Carlisle, M. (2021). *How 9/11 Radically Expanded the Power of the U.S. Government*. TIME. Retrieved 21 June 2022, from https://time.com/6096903/september-11-legal-history/.

Centre for the Study of Terrorism and Irregular Warfare. (1999). *Cyberterror: Prospects and Implications*. Monterey.

Conway, M. (2004). Cyberterrorism: media myth or a clear and present danger?. In J. Irwin, *War and virtual war: the challenges to communities*. Rodopi.

Deibert, R. (2002). *Information Technologies and Global Politics: The Changing Scope of Power and Governance* (p. 23), State University of New York, Albany.

Deutch, J. (1996). *Statement before the U.S. Senate Governmental Affairs Committee, Permanent Subcommittee on Investigations*. Washington, D.C.

Denning, D. (2002). Is Cyber Terror Next?. In C. Calhoun, P. Price & A. Timmer, *Understanding September*. The New Press.

Dunn Cavelty, M. (2007). *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age* (1st ed., p. 95). Routledge.

Dunn Cavelty, M. (2005). A Comparative Analysis of Cybersecurity Initiatives Worldwide. In *WSIS Thematic Meeting on Cybersecurity* (p. 13). Zurich; Centre for Security Studies, Swiss Federal Institute of Technology (ETH Zurich). Retrieved 24 June 2022, from https://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Comparative_Analysis_Cybersecurity_Initiatives_Worldwide.pdf

Emery, N. E. (2005). The Myth of Cyberterrorism. *Journal of Information Warfare*, 4(1), 80–89.

Eroukhmanoff, C. (2018). *Securitisation Theory: An Introduction*. E-International Relations. Retrieved 15 November 2020, from https://www.e-ir.info/2018/01/14/securitisation-theory-an-introduction/.

Federal Bureau of Investigation. (2002). *Terrorism 2002-2005*. Washington, D.C.

Federal Register. (2002). *Executive Order 13228 - Establishing the Office of Homeland Security and the Homeland Security Council*. Washington, D.C.

Floyd, R. (2020). Securitisation and the function of functional actors. *Critical Studies on Security, 9*(2), 81-97.

Gellman, B. (2002). *Cyber-Attacks by Al Qaeda Feared; Terrorists at Threshold of Using Internet as Tool of Bloodshed, Experts Say*. The Washington Post. Retrieved 20 June 2022, from https://www.washingtonpost.com/archive/politics/2002/06/27/cyber-attacks-by-al-qaeda-feared/5d9d6b05-fe79-432f-8245-7c8e9bb45813/.

Gregg, G. (n.d.). *George W. Bush: Foreign Affairs*. The Miller Centre. Retrieved 21 June 2022, from https://millercenter.org/president/gwbush/foreign-affairs.

Hansen, L., & Nissenbaum, H. (2009). Digital Disaster, Cyber Security, and the Copenhagen School. *International Studies Quarterly*, 53 (4), 1155-1175.

Homeland Security Department. The National Archives and Records Administration. Retrieved 15 June 2022, from https://www.federalregister.gov/agencies/homeland-security-department.

Jantunen, S., & Huhtinen, A.-M. (2011). American perspectives on cyber and security: Coining the linguistic tradition. *Journal of Information Warfare*, 10(3), 1–15.

Klein, J. (2018). Deterring and Dissuading Cyberterrorism. *Air and Space Power Journal-Africa and Francophonie*, 9(1), 21-34.

Latham, R. (2005). *Bombs and Bandwidth: The Emerging Relationship Between Information Technology and Security* (p. 18). The New Press.

Lawson, S. (2016). *Cyber Doom is Still the Wrong Rallying Cry for Better Cybersecurity*. Sean Lawson. Retrieved 23 June 2022, from https://www.seanlawson.net/2016/12/cyber-doom-cybersecurity/.

Lawson, S., & Middleton, M. (2019). Cyber Pearl Harbour: Analogy, fear, and the framing of cyber security threats in the United States, 1991-2016. *First Monday*, *24*(3).

Lenzner, R., & Vardi, N. (2004). *Cyber-nightmare*. Forbes. Retrieved 20 June 2022, from https://www.forbes.com/global/2004/0920/104_print.html?sh=1b514b9129c3

McCullagh, C. (2002). *Media Power: A Sociological Introduction* (1st ed). Macmillan Education UK.

Milone, M. (2002). Hacktivism: Securing the National Infrastructure. *The Business Lawyer*, 58(1), 383-413.

Mowery, S. (2013). *Defining Cyber and Focusing the Military's Role in Cyberspace* (Post Graduate). United States Army War College.

National Academies of Sciences, Engineering, and Medicine. (1991). *Computers at Risk: Safe Computing in the Information Age* (1st ed.). National Academy Press.

Raghavan, T. (2003). In Fear of Cyberterrorism: An Analysis of the Congressional Response. *Journal of Law, Technology and Policy*, 2003(1), 297-311.