Literature Review Outline

Topic: State-Sponsored Cyberterrorism in Global Politics

1. **Introduction**
    a. Description of cyberterrorism and its importance to computer science (Veerasamy, 2020; Gao et al., 2021; Petr, 2022)
    b. Historical context of cyberterrorism (Ramadhan, 2020; Zinchenko, 2022; Salih et al., 2023)
    c. Argument: Cyberterrorism both benefits and harms major global powers (Abdallah et al., 2019; Odeh, 2019; Adetunji et al., 2022; Abdel-Aal & Atwa, 2023; Banks, 2017; Helms et al., 2012)
2. **Definition of Terms**
    a. Cyberterrorism (Gao et al., 2021; Veerasamy, 2020; Ma'arif et al., 2023; Onat et al., 2021; Jacobsen, 2022)
    b. Cyber Warfare (Pais et al., 2022; Asbas & Tuzlukaya, 2023)
    c. Cyber Espionage (Dilek & Talih, 2022; Heriyanto, 2019; Kaster & Ensign, 2022)
3. **Cyberterrorism**
    a. Destruction of computing systems, networks, and data (Veerasamy, 2020; Gao et al., 2021; Petr, 2022; Al Asyari, 2022)
4. **Cyber Warfare**
    a. Use of computing systems for warfare (Pais et al., 2022; Asbas & Tuzlukaya, 2023; Ashraf & Kayani, 2023)
5. **Cyber Espionage**
    a. Theft of data and intellectual property (Dilek & Talih, 2022; Heriyanto, 2019; Kaster & Ensign, 2022; Rivera et al., 2021; Hore & Rauchaudhuri, 2020)
6. **State-Sponsored Cyberterrorism**
    a. United States of America (Moore, 2022; Kaminski, 2020; Mohee, 2022; Ardita et al., 2023)
    b. Russia (Fidler, 2017; Topor & Tabachnik, 2021; Priyono, 2022; Strucl, 2023; Kondratov & Johansson-Nogues, 2022)
    c. China (Mohamed et al., 2023; Ardita et al., 2023; Jiang, 2019; Alperovitch, 2011)
    d. Iran (Freilich et al., 2023; Moore, 2022; Alashti et al., 2022)
    e. North Korea (Hwang & Choi, 2021; Gulyas, 2021; Man-sik & Sung-gu, 2017)
    f. Israel (Saada & Turan, 2021; Freilich et al., 2023; Kaster & Ensign, 2022; Pirvu, 2021; Kaminski, 2020)
7. **Countermeasures and Policy Responses**
    a. International Cooperation (Khater, 2023; Zinchenko, 2022; Salih et al., 2023; Saadat, 2020)
        i. EU (Al Asyari, 2022; Milkowski, 2022; Kondrotas, 2022; European Council, 2022; Baker-Beall & Mott, 2021)
        ii. UN (Khater, 2023; Kadir, 2020; Kadir et al., 2019; United Nations, 2022; UNODC, N.D.; Broeders et al., 2021; Housen-Couriel et al., 2022)

        iii. NATO (Ferent & Preja, 2023; Mosoiu et al., 2020; Tosbotn & Cusumano, 2020)
    b. Challenges (Baldassarre, 2023; Grobbelaar, 2022; Al Asyari, 2022)

8. **Future Directions**
    a. Emerging Threats (Al Asyari, 2022; Grobbelaar, 2022; Abdallah et al., 2019)
        i. AI (Bianchi et al., 2023; Montasari, 2023, Yamin et al., 2021)
        ii. Quantum Computing (Kilber et al., 2021; Johnson et al., 2019; Easa et al., 2023; Ford, 2023)

9. **Conclusion**
    a. How does current literature contribute?
    b. Strengths of current literature
    c. Weaknesses of current literature
        i. Often outdated as events are talked about mostly when they occur
    d. Gaps in current literature
        i. Little research on how countries benefit from cyberterrorism
    e. Areas of future research

Bibliography

Veerasamy, N. (2020) *Chapter 2 - Cyberterrorism - the spectre that is the convergence of the physical and virtual worlds.* Academic Press. DOI: https://doi.org/10.1016/B978-0-12-816203-3.00002-2 [Accessed 24 March 2024].

Gao, M., Dong, Y., Qiao, X. & Fan, S. (2021) The Study of the Plight of Cyberterrorism and Its Way Out. *The Frontiers of Society, Science and Technology* 3(1): 93-98. DOI: https://dx.doi.org/10.25236/FSST.2021.030115 [Accessed 24 March 2024].

Petr, K. (2022) Cyberterrorism as the Most Important Threat to the National Security of the Russian Federation and its Main Warnings. *National Security and Strategic Planning* 1(37): 23-28. DOI: https://www.doi.org/10.37468/2307-1400-2022-1-23-28 [Accessed 24 March 2024].

Pais, S. L., Shrihstha, S. R. M., Shruthi, C. S. & Poojari, S. (2022) Cyber Warfare: Espionage, Botnet. *International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)* 2(2): 271-274. DOI: https://www.doi.org/10.48175/ijarsct-5819 [Accessed 01 April 2024].

Asbas, C. & Tuzlukaya S. E. (2023) Cyberwarfare: War Activities in Cyberspace. *Handbook of Research on War Policies, Strategies, and Cyber Wars*: 1-18. DOI: https://www.doi.org/10.4018/978-1-6684-6741-1.ch007 [Accessed 01 April 2024].

Dilek, E. & Talih, O. (2022) ‘Overview of Cyber Espionage Incidents and Analysis of Tackling Methods’, 2022 15th International Conference on Information Security and Cryptography (ISCTURKEY). Ankara, Turkey. 19-20 October 2022. IEEE. 55-60. DOI: https://doi.org/10.1109/ISCTURKEY56345.2022.9931893 [Accessed 01 April 2024].

Heriyanto, D. S. N. (2019) International Regulatory Vacuum of Cyber Espionage. *Advances in Social Science, Education and Humanities Research* 436: 106-111. DOI: https://doi.org/10.2991/assehr.k.200529.022 [Accessed 01 April 2024].

Al Asyari, H. (2022) The Evolution of Cyberterrorism: Perspectives And Progress From The European Union And Association of Southeast Asian Nation. *Jurnal Hukum Ius Quia Iustum* 29(1): 1-23. DOI: https://www.doi.org/10.20885/iustum.vol29.iss1.art1 [Accessed 24 March 2024].

Grobbelaar, A. (2022) Cyberterrorism In Africa - Exaggerated Threat Or Worthy Foe? *Future, Research, and Expectations in Science, Knowledge, and Aspirations* 1(1): 257-266. DOI: https://doi.org/10.7251/ZNUBL2201257G [Accessed 24 March 2024].

Ramadhan, I. (2020) Cyber-Terrorism in The Context of Proselytizing, Coordination, Security, and Mobility. *Journal of Islamic World and Politics* 4(2): 179-197. DOI: https://www.doi.org/10.18196/JIWP.4252 [Accessed 02 April 2024].

Zinchenko, O. (2022) Cyberattacks as a Tool of Destructive Influence of Cyberterrorism. *International Journal of Science, Technology and Society* 10(2): 23-26. DOI: https://www.doi.org/10.11648/j.ijsts.20221002.11 [Accessed 02 April 2024].

Salih, A. J. & Al Azzam, F. A. (2023) A Competent Approach to the Training of Lawyers in “Cyberterrorism”. *Pedagogy and Education Management Review* 1(11): 29-43. DOI: https://www.doi.org/10.36690/2733-2039-2023-1-29 [Accessed 02 April 2024].

Abdallah, J. A., Awang, M. B. B. & Ahamd, A. A. (2019) Cyberterrorism as a Threat to International Peace and Security: A Critical Discourse. *Scholars International Journal of Law, Crime and Justice*: 314-317. DOI: https://www.doi.org/10.36348/SIJLCJ.2019.V02I10.004 [Accessed 02 April 2024].

Odeh, A. (2019) A Review of the Economic Benefits of Cyber Terrorism. *Applying Methods of Scientific Inquiry Into Intelligence, Security, and Counterterrorism.* DOI: https://www.doi.org/10.4018/978-1-5225-8976-1.CH006 [Accessed 02 April 2024].

Adetunji, C. O., Olugbemi, O. T., Anani, O. A., Hefft, D. I., Wilson, N., Olayinka, A. S. & Ukhurebor, K. E. (2022) *AI, Edge and IoT-based Smart Agriculture: Chapter 27 - Cyberespionage: Socioeconomic implications on sustainable food security.* Academic Press. DOI: https://doi.org/10.1016/B978-0-12-823694-9.00011-6 [Accessed 02 April 2024].

Abdel-Aal, R. A. & Atwa, R. (2023) Cyber Wars and Their Impact on International Security. *International Affairs and Global Strategy* 99: 38-54. DOI: https://www.doi.org/10.7176/iags/99-05 [Accessed 02 April 2024].

Banks, W. C. (2017) Cyber Espionage and Electronic Surveillance: Beyond the Media Coverage. *Emory Law Journal* 66(3): 513-525. Available from: https://scholarlycommons.law.emory.edu/elj/vol66/iss3/3?utm_source=scholarlycommons.law.emory.edu%2Felj%2Fvol66%2Fiss3%2F3&utm_medium=PDF&utm_campaign=PDFCoverPages [Accessed 02 April 2024].

Helms, R., Costanza, S. E. & Johnson, N. (2012) Crouching tiger or phantom dragon? Examining the discourse on global cyber-terror. *Security Journal* 25: 57-75. DOI: https://www.doi.org/10.1057/SJ.2011.6 [Accessed 02 April 2024].

Bianchi, S., Paternoster, C., Tsikrika, T., Kozhuharova, D., Mancuso, M., Kalpakis, G., Vrochidis, S. & Jaeger, B. (2023) ‘Artificial Intelligence to Counter Cyber-Terrorism’, *The International Conference on Cybersecurity and Cybercrime*. Melbourne, Australia. 17-19 October 2023. DOI: https://doi.org/10.19107/CYBERCON.2023.02 [Accessed 02 April 2024].

Montasari, R. (2023) *Countering Cyberterrorism - The Confluence of Artificial Intelligence, Cyber Forensics and Digital Policing in US and UK National Cybersecurity*. Springer. DOI: https://www.doi.org/10.1007/978-3-031-21920-7 [Accessed 02 April 2024].

Yamin, M. M., Ullah, M., Ullah, H. & Katt, B. (2021) Weaponized AI for cyber attacks. *Journal of Information Security and Applications* 57: 1-14. DOI: https://doi.org/10.1016/j.jisa.2020.102722 [Accessed 02 April 2024].

Kilber, N., Kaestle, D. & Wagner, S. (2021) ‘Cybersecurity for Quantum Computing’. *2nd Quantum Software Engineering and Technology Workshop - IEEE International Conference on Quantum Computing and Engineering*. Virtual. 18-22 October 2021. Available from: https://arxiv.org/pdf/2110.14701.pdf [Accessed 02 April 2024].

Johnson, N. F., Gomez-Ruiz, F. J., Rodriguez, F. J. & Quiroga, L. (2019) *Quantum Terrorism: Collective Vulnerability of Global Quantum Systems*: 1-14. Available from: https://arxiv.org/pdf/1901.08873.pdf [Accessed 02 April 2024].

Easa, R. J., Yahya, A. S. & Ahmad, E. K. (2023) Protection from A Quantum Computer Cyber-Attack: survey. *Applied Sciences and Technology* 5: 1-12. DOI: https://doi.org/10.47577/technium.v5i.8293 [Accessed 02 April 2024].

Ford, P. (2023) The Quantum Cybersecurity Threat May Arrive Sooner Than You Think. *Computer* 56(2): 134-136. DOI: https://doi.org/10.1109/MC.2022.3227657 [Accessed 02 April 2024].

Khater, M. (2023) International Perspective on Securing Cyberspace Against Terrorist Acts. *International Journal of Sociotechnology and Knowledge Development* 15(1): 1-8. DOI: https://www.doi.org/10.4018/ijskd.318706 [Accessed 03 April 2024].

Saadat, S. Y. (2020) International cooperation for counter-terrorism: a strategic perspective. *Journal of Policing, Intelligence and Counter Terrorism* 15(1): 83-93. DOI: https://doi.org/10.1080/18335330.2020.1732451 [Accessed 03 April 2024].

Milkowski, T. (2022) The European Union and Terrorist Threats: The Next Step (Part 1). *Annuals of the Administration and Law* 4(22): 105-116. DOI: https://www.doi.org/10.5604/01.3001.0016.3318 [Accessed 03 April 2024].

Kondrotas, L. (2022) European Union policy and the use of the normative power regarding cybersecurity. *Analisis Juridico-Politico* 4(7): 141-168. DOI: https://doi.org/10.22490/26655489.5504 [Accessed 03 April 2024].

Kadir, N. K. (2020) Cyberterrorism's Dilemma: Renewal of Conventional Terrorism. *International Journal of Global Community* 3(2): 97-110. Available from: https://journal.riksawan.com/index.php/IJGC-RI/article/view/68 [Accessed 03 April 2024].

Kadir, N. K., Judhariksawan, J. & Maskun, M. (2019) Terrorism and Cyberspace: A Phenomenon of Cyber-Terrorism as Transnational Crimes. *Fiat Justisia: Jurnal Ilmu Hukum* 13(4): 333-344. DOI: https://doi.org/10.25041/fiatjustisia.v13no4.1735 [Accessed 03 April 2024].

United Nations (2022) Cybersecurity and New Technologies. Available from: https://www.un.org/counterterrorism/cct/programme-projects/cybersecurity#:~:text=At%20the%20end%20of%20October,media%2C%20and%20online%20terrorist%20financing. [Accessed 03 April 2024].

UNODC (N.D.) Cyberterrorism. Available from: https://www.unodc.org/e4j/zh/cybercrime/module-14/key-issues/cyberterrorism.html [Accessed 03 April 2024].

European Council (2022) Cybersecurity: how the EU tackles cyber threats. Available from: https://www.consilium.europa.eu/en/policies/cybersecurity/ [Accessed 03 April 2024].

Baker-Beall, C. & Mott, G. (2021) Understanding the European Union's Perception of the Threat of Cyberterrorism: A Discursive Analysis. *Journal of Common Market Studies* 60(4): 1086-1105. DOI: https://doi.org/10.1111/jcms.13300 [Accessed 03 April 2024].

Broeders, D., Cristiano, F. & Weggemans, D. (2021) Too Close for Comfort: Cyber Terrorism and Information Security across National Policies and International Diplomacy. *Studies in Conflict & Terrorism* 46(12): 2426-2453. DOI: https://doi.org/10.1080/1057610X.2021.1928887 [Accessed 03 April 2024].

Housen-Couriel, D., Ganor, B., Yaakov, U. B., Weinberg, S. & Beri, D. (2022) *The International Cyber Terrorism Regulation Project*. Online. Royal United Services Institute of Defence and

Security Studies. Available from: https://static.rusi.org/20190731_grntt_paper_09.pdf [Accessed 03 April 2024]

Ferent, D. & Preja, C. (2023) NATO's involvement in cyber defence. *Intelligence Info* 2(1): 1-6. DOI: https://www.doi.org/10.58679/ii30227 [Accessed 03 April 2024].

Mosoiu, O., Balaceanu, I. & Mihai, E. (2020) Cyber Terrorism and the Effect of the Russian Attacks on Democratic States in East Europe. *Scientific Journal of Silesian University of Technology* 106: 131-139. DOI: https://www.doi.org/10.20858/SJSUTST.2020.106.11 [Accessed 03 April 2024].

Tosbotn, R. A. & Cusumano, E. (2019) *The Changing Global Order - NATO in a Changing World*. Online: Springer. DOI: https://www.doi.org/10.1007/978-3-030-21603-0_16 [Accessed 03 April 2024].

Ma'arif, S., Ibda, H., Ahmadi, F., Qosim, N. & Muanayah, N. A. (2023) Islamic moderation in education and the phenomenon of cyberterrorism: a systematic literature review. *Indonesian Journal of Electrical Engineering and Computer Science* 31(3): 1523-1533. Available from: https://d1wqtxts1xzle7.cloudfront.net/105712835/17562-libre.pdf?1694641839=&response-content-disposition=inline%3B+filename%3DIslamic_moderation_in_education_and_the.pdf&Expires=1712177740&Signature=Ck4foeJzdyxzyyJadUIHa8zsXDxuwqgse7UOunVqKKCUF7HhJUeLIxZTrHKcX-WyDT1ZHBjnZYIMM9TsPdBbEcB2cyCw6SDxD8cn9Fj5jpWQ-rAuwgxOX0XRoIpZdkjULSpDCfpWr5fEZ0~jkk5RmdJKW3FPWSx48D6AwRKeTHHkVBdmKVuLB480ejBzzK7Xspv2qE1K0hfNQL5tQFaWw1dQ0DLr8zesXWk3g4BQQwhoBMz~DI~YRYemtjtCj3sU7b9JUWjyxHjX0gYm3QA5kneaxRSycfpb~g1yhPZYvxRNuxUO~wLqr41mIn~1ObHAxl6qwUpInKhqAadxiYgOqg__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA [Accessed 03 April 2024].

Onat, I., Bastug, M. F., Guler, A. & Kula, S. (2021) Fears of cyberterrorism, terrorism, and terrorist attacks: an empirical comparison. *Behavioral Sciences of Terrorism and Political Aggression* 16(2): 149-165. DOI: https://doi.org/10.1080/19434472.2022.2046625 [Accessed 03 April 2024].

Jacobsen, J. T. (2022) Cyberterrorism: Four Reasons for Its Absence - So Far. *Perspectives on Terrorism* 16(5): 62-72. Available from: https://www.jstor.org/stable/27168617 [Accessed 03 April 2024].

Saada, M. A. & Turan, Y. (2021) *Israeli-Palestinian Cyber Conflict*. Kabul: Eskisehir Osmangazi Universitesi. Available from: https://dergipark.org.tr/en/pub/oguiibf/issue/60025/869178 [Accessed 03 April 2024].

Freilich, C. D., Cohen, M. S. & Siboni, G. (2023) *Israel and the Cyber Threat: How the Startup Nation Became a Global Cyber Power*. Online: Oxford Academic. DOI: https://doi.org/10.1093/oso/9780197677711.001.0001 [Accessed 03 April 2024].

Freilich, C. D., Cohen, M. S. & Siboni, G. (2023) *Israel and the Cyber Threat: The Iranian Cyber Threat*. Online: Oxford Academic. DOI: https://doi.org/10.1093/oso/9780197677711.003.0006 [Accessed 03 April 2024].

Kaster, S. D. & Ensign, P. C. (2022) Privatized espionage: NSO Group Technologies and its Pegasus spyware. *Thunderbird International Business Review* 65(3): 355-364. DOI: https://doi.org/10.1002/tie.22321 [Accessed 03 April 2024].

Pirvu, M. (2021) 'The Degradation of Human Rights and Free Press Through the Pegasus Software in the Era of Surveillance, as a Threat to International Security. A Debate of Civil Liberties and Censorship'. *Proceedings of the International Scientific Conference "Strategies XXI"*. National Defence University. 9-10 December 2021. Univeritatea Nationala de Aparare Carol I. DOI: https://www.doi.org/10.53477/2668-6511-22-29 [Accessed 03 April 2024].

Hwang, J. & Choi, K. (2021) North Korean Cyber Attacks and Policy Responses: An Interdisciplinary Theoretical Framework. *International Journal of Cybersecurity, Intelligence & Cybercrime* 4(2): 4-24. DOI: https://www.doi.org/10.52306/04020221NHPZ9033 [Accessed 03 April 2024].

Gulyas, A. (2021) "Lazarus" The North Korean Hacker Group. *2021: The Complex and Dynamic Nature of the Security Environment*: 75-83. DOI: https://doi.org/10.53477/2668-6511-22-08 [Accessed 03 April 2024].

Man-sik, S. & Sung-gu, J. (2017) Response of KOREAN Private Security against North Korean CYBER TERRORISM. *International Journal of Protection, Security & Investigation* 2(2): 11-14. DOI: https://www.doi.org/10.22471/PROTECTIVE.2017.2.2.11 [Accessed 03 April 2024].

Moore, D. (2022) *Offensive Cyber Operations: Understanding Intangible Warfare - Approximating the Iranian Threat*. Online: Oxford Academic. DOI: https://doi.org/10.1093/oso/9780197657553.003.0009 [Accessed 04 April 2024].

Moore, D. (2022) *Offensive Cyber Operations: Understanding Intangible Warfare - American Cyber Superiority*. Online: Oxford Academic. DOI: https://doi.org/10.1093/oso/9780197657553.003.0006 [Accessed 04 April 2024].

Alashti, Z. F., Bojnordi, A. J. J. & Sani, S. M. S. (2022) Toward a carnivalesque analysis of hacking: A qualitative study of Iranian hackers. *Asian Journal of Social Science* 50(2): 147-155. DOI: https://doi.org/10.1016/j.ajss.2022.01.001 [Accessed 04 April 2024].

Fiddler, D. P. (2017) The U.S. Election Hacks, Cybersecurity, and International Law. *American Journal of International Law* 110: 337-342. DOI: https://doi.org/10.1017/aju.2017.5 [Access 04 April 2024].

Kaminski, M. A. (2020) Operation “Olympic Games.” Cyber-sabotage as a tool of American intelligence aimed at counteracting the development of Iran’s nuclear programme. *Security and Defence Quarterly* 29(2): 63-71. DOI: https://doi.org/10.35467/sdq/121974 [Accessed 04 April 2024].

Mohee, A. (2022) A Realistic Analysis of the Stuxnet Cyber-attack. *American Political Science Association - International Relations* 1: 1-11. DOI: https://doi.org/10.33774/apsa-2022-qs797 [Accessed 04 April 2024].

Topor, L. & Tabachnik, A. (2021) Russian Cyber Information Warfare - International Distribution and Domestic Control. *Journal of Advanced Military Studies* 12(1): 112-127. DOI: https://www.doi.org/10.21140/MCUJ.20211201005 [Accessed 04 April 2024].

Priyono, U. (2022) Cyber Warfare as Part of Russia and Ukraine Conflict. *Jurnal Diplomasi Pertahanan* 8(2): 44-59. DOI: https://doi.org/10.33172/jdp.v8i2.1005 [Accessed 04 April 2024].

Strucl, D. (2023) Russian Aggression on Ukraine: Cyber Operations and the Influence of Cyberspace on Modern Warfare. *Contemporary Military Challenges* 24(2): 103-124. DOI: https://doi.org/10.33179/bsv.99.svi.11.cmc.24.2.6 [Accessed 04 April 2024].

Kondratov, E. & Johansson-Nogues, E. (2022) Russia’s Hybrid Interference Campaigns in France, Germany and the UK: A Challenge against Trust in Liberal Democracies? *Geopolitics* 28(5): 2169-2199. DOI: https://doi.org/10.1080/14650045.2022.2129012 [Accessed 04 April 2024].

Mohamed, N., Almazrouei, S. K., Oubelaid, A., Ahmed, A. A., Jomah, O. S. M. & Aghnaiya, A. (2023) ‘Understanding the Threat Posed by Chinese Cyber Warfare Units’. Benghazi, Libya. 21-23 May 2023. Online. IEEE. 359-364. DOI: https://doi.org/10.1109/MI-STA57575.2023.10169496 [Accessed 04 April 2024].

Ardita, N. D., Prakoso, S. G., Al Putra, F. A., Sulistiobudi, A. & Satria, R. (2023) Cyberwarfare between the United States and China 2014 - 2022: in Retrospect. *Jurnal Pertahanan: Media Informasi tentang Kajian dan Strategi Pertahanan yang Mengedepankan Identity, Nasionalism dan Integrity* 9(1): 17-29. DOI: https://www.doi.org/10.33172/jp.v9i1.1869 [Accessed 04 April 2024].

Jiang, T. (2019) From Offensive Dominance to Deterrence: China’s Evolving Strategic Thinking on Cyberwar. *Chinese Journal of International Review* 1(2): 1-23. DOI: https://doi.org/10.1142/S2630531319500021 [Accessed 04 April 2024].

Alperovitch, D. (2011) *Revealed: Operation Shady RAT*. Available from: http://contagio.deependresearch.org/APT/China/APT1_CommentCrew_CommentPanda_PLAUnit61398_TG8223/Reading/2011_Mcafee-operation-shady-rat1.pdf [Accessed 04 April 2024].

Ashraf, N. & Kayani, S. A. (2023) India’s Cyber Warfare Capabilities: Repercussions for Pakistan’s National Security. *NDU Journal* 37: 34-45. DOI: https://doi.org/10.54690/ndujournal.37.152 [Accessed 04 April 2024].

Rivera, R., Pazmino, L., Becerra, F. & Barriga, J. (2021) *Developments and Advances in Defense and Security - An Analysis of Cyber Espionage Process*. Singapore: Springer. DOI: https://www.doi.org/10.1007/978-981-16-4884-7_1 [Accessed 04 April 2024].

Hore, S. & Raychaudhuri, K. (2020) *Innovations in Computational Intelligence and Computer Vision - Cyber Espionage - An Ethical Analysis*. Singapore: Springer. DOI: https://www.doi.org/10.1007/978-981-15-6067-5_5 [Accessed 04 April 2024].

Baldassarre, S. (2023) Cyberterrorism and Religious Fundamentalism: New Challenges for Europe in the Age of Universal Internet Access. *Religions* 14(4): 1-12. DOI: https://doi.org/10.3390/rel14040458 [Accessed 04 April 2024].