DAFTAR PUSTAKA

Ballbach, E. J. (2022). The sanctions regime of the European Union against North Korea. *SWP Research Paper*. https://doi.org/10.18449/2022RP04

Bendiek, A., & Pawlak, P. (2019). The EU's Cyber Diplomacy Toolbox: Towards deterrence by denial? *European Union Institute for Security Studies (EUISS).*

Bendiek, A., & Schulze, M. (2021). Advancing the EU's cyber posture. *European Union Institute for Security Studies (EUISS).*

Bodansky, D. (2005). The international climate change regime. In *Perspectives on climate change: Science, economics, politics, ethics*. Emerald Group Publishing Limited.

Bourhriba, O. (2024, November 29). Digital transformation in the maritime industry. *Observer Research Foundation.* https://www.orfonline.org/expert-speak/digital-transformation-in-the-maritime-industry

Buzan, B., Wæver, O., & de Wilde, J. (1998). *Security: A new framework for analysis*. Lynne Rienner Publishers.

Capano, D. E. (2023). NotPetya attacking Maersk. In *How NotPetya accidentally took down global shipping giant Maersk* (pp. 39–41). Elsevier. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85169000270

Carrapico, H., & Barrinha, A. (2017). European Union cybersecurity as an emerging research and policy field. *European Political Science, 16*(3), 328–336.

Cîrnu, C. E., Rotuna, C., & Vasiloiu, I. C. (2023). Comparative analysis on cyber diplomacy in EU and US. *Romanian Cyber Security Journal*, *5*, 77–86.

Colatin, S. D. (n.d.). Si vis cyber pacem, para sanctiones: The EU Cyber Diplomacy Toolbox in action. *NATO CCDCOE.* https://ccdcoe.org/library/publications/si-vis-cyber-pacem-para-sanctiones-the-eu-cyber-diplomacy-toolbox-in-action/

Council of the European Union. (2015). *Council conclusions on cyber diplomacy.* https://data.consilium.europa.eu/doc/document/ST-6122-2015-INIT/en/pdf

Council of the European Union. (2017). *CDT guideline: Draft implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities.*

Council of the European Union. (2020). *Council Decision (CFSP) 2020/1127 concerning restrictive measures against cyber-attacks threatening the Union or its Member States.*

Council of the European Union. (2021). *Declaration by the High Representative on behalf of the EU on malicious cyber activities (Ghostwriter).*

Council of the European Union. (2023). *Revised implementing guidelines of the Cyber Diplomacy Toolbox* (pp. 1–26). https://data.consilium.europa.eu/doc/document/ST-10289-2023-INIT/en/pdf

Cyber Diplomacy Toolbox. (n.d.). What is cyber diplomacy? Retrieved from https://www.cyber-diplomacy-toolbox.com/Cyber_Diplomacy.html

DNV Group. (n.d.). Maritime cyber security. *DNV.* https://www.dnv.com/maritime/insights/topics/maritime-cyber-security/regulations/

Dominguez, G. (2025). EU and Japan aim for deeper defense cooperation in high-tech arena. *Japan Times.* https://www.japantimes.co.jp/news/2025/07/23/japan/politics/eu-japan-defense-kaja-kallas/

Düzenli, H., et al. (2024). Maritime cybersecurity exercises in the EU: Enhancing collective preparedness. *Journal of Maritime Policy & Management.*

ENISA. (2022). *Cyber Europe 2022 Exercise Report*. European Union Agency for Cybersecurity.

European Commission. (2016). *Directive (EU) 2016/1148 on security of network and information systems (NIS Directive).*

European Commission. (2019). *EU Cybersecurity Act.*

European Commission. (2020). *Directive (EU) 2020/35 on measures for a high common* *level of cybersecurity across the Union (NIS2 Directive).*

European Commission. (2021). *EU Statement at the United Nations Group of Governmental Experts (UNGGE) on Developments in the Field of ICTs.*

European Commission. (n.d.). EU cybersecurity policies. https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies

European Council. (2025). Chemical weapons: EU sanctions three entities in the Russian Armed Forces over use of chemical weapons in Ukraine. https://www.consilium.europa.eu/en/press/press-releases/2025/05/20/chemical-weapons-eu-sanctions-three-entities-in-the-russian-armed-forces-over-use-of-chemical-weapons-in-ukraine/

European External Action Service. (2020). *EU imposes first ever cyber sanctions.*

European Maritime Safety Agency. (2022). *Maritime cybersecurity guidelines.*

European Policy Centre. (2019). *Responding to cyberattacks: Prospects for the EU Cyber Diplomacy Toolbox.* https://www.epc.eu/publication/Responding-to-cyberattacks-EU-Cyber-Diplomacy-Toolbox-218414/

European Union Council. (2023). *Revised European Union Maritime Security Strategy (EUMSS).*

European Union Institute for Security Studies (EUISS). (2023). *EU cyber diplomacy and the global order.*

European Union Law. (2019). *Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States.* https://eur-lex.europa.eu/eli/dec/2019/797/oj/eng

Fitton, O., Prince, D., Germond, B., & Lacy, M. (2015). The future of maritime cyber security. *Lancaster University Papers*, 8, 1–20.

Harris, R. (2021a, November 25). How big a problem is maritime cyber security? *Ocean Technologies Group*. https://oceantg.com/blog/the-problem-of-maritime-cyber-security/

Industrial Cyber. (2025). ENISA launches EU Vulnerability Database to strengthen cybersecurity under NIS2 Directive, boost cyber resilience. https://industrialcyber.co/vulnerabilities/enisa-launches-eu-vulnerability-database-to-strengthen-cybersecurity-under-nis2-directive-boost-cyber-resilience/

Khausar, M., & Ras, A. R. (2023). Establishment of the Cyber Diplomacy Toolbox (CDT) as a joint diplomatic response of the European Union against the threat of cyber-attack activity. *Politicon: Jurnal Ilmu Politik, 5*(1), 29–58.

Khausar, M., & Ras, A. R. (2023, March 29). Establishment of the Cyber Diplomacy Toolbox (CDT) as a joint diplomatic response of the European Union against the threat of cyber-attack activity. *Politicon: Jurnal Ilmu Politik*. https://journal.uinsgd.ac.id/index.php/politicon/article/view/14833/8855

Kost, E. (2025, June 25). The difference between a regulation and cyber framework. *UpGuard*. https://www.upguard.com/blog/regulation-vs-cyber-framework

Krasner, S. D. (1982). Structural causes and regime consequences: Regimes as intervening variables. *International Organization, 36*(2), 185–205. https://doi.org/10.1017/S0020818300018920

Lavadoux, F. (2021). EU cyber diplomacy 101. *EIPA Blog*. https://www.eipa.eu/blog/eu-cyber-diplomacy-101/

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cybersecurity: Emerging trends and recent developments. *Energy Reports, 7*, 8176–8186.

Marine Digital. (n.d.). The importance of cybersecurity in the maritime industry. Retrieved from https://marinedigital.com/article_importance_of_cybersecurity

Maulana, Y. I., & Fajar, I. (2023). Analysis of cyber diplomacy and its challenges for the digital era community. *IAIC Transactions on Sustainable Digital Innovation (ITSDI), 4*(2), 169–177. https://doi.org/10.34306/itsdi.v4i2.587

Miadzvetskaya, Y., & Wessel, R. A. (2022). The European Union's cyber diplomacy: Institutions, processes, and instruments. *Journal of Common Market Studies, 60*(4), 902–918.

Miadzvetskaya, Y., & Wessel, R. A. (2022). The externalisation of the EU's cybersecurity regime: The cyber diplomacy toolbox. *European Papers, 7*(1), 413–438. https://doi.org/10.15166/2499-8249/570

Moret, E., & Pawlak, P. (2017). The EU Cyber Diplomacy Toolbox: Towards a cyber sanctions regime? *European Union Institute for Security Studies (EUISS).*

Pernik, P. (2018). EU cyber diplomacy: A tool for peace, security and stability in cyberspace. *NATO CCDCOE Publications.*

Potter, E. H. (2002). *Cyber-diplomacy: Managing foreign policy in the twenty-first century*. McGill-Queen's Press.

Reuters. (2025). EU warns of GPS jamming threats to merchant ships in the Eastern Mediterranean. *Reuters.*

Ribeiro, A. (2025). European Commission rolls out ProtectEU strategy to boost internal security, resilience against hybrid threats. *Industrial Cyber.* https://industrialcyber.co/regulation-standards-and-compliance/european-commission-rolls-out-protecteu-strategy-to-boost-internal-security-resilience-against-hybrid-threats/

Rid, T. (2020). *Cyber war will not take place*. Oxford University Press.

Schulze, M. (2021). Attribution: A major challenge for EU cyber sanctions. *Stiftung Wissenschaft und Politik.* https://www.swp-berlin.org/10.18449/2021RP11/

The EU Cyber Diplomacy Toolbox. (n.d.). Retrieved from https://www.cyber-diplomacy-toolbox.com

Thumfart, J. (2022). The (Il)legitimacy of cybersecurity: An application of just securitization theory to cybersecurity based on the principle of subsidiarity. *Applied Cybersecurity & Internet Governance, 1*(1), 1–24.

Vanberghen, C. (2025). The digital battlefield: EU-China cybersecurity diplomacy in the 21st century – Part I. *Friends of Europe.* https://www.friendsofeurope.org/insights/critical-thinking-the-digital-battlefield-eu-china-cybersecurity-diplomacy-in-the-21st-century-part-i/