DAFTAR PUSTAKA

Ardiyanti, H. (2014). *Cyber-Security Dan Tantangan Pengembangannya Di Indonesia*. 95–110.

Billo, C. G., & Chang, W. (2004). Cyber Warfare An Analysis of the means and motivations of selected nation states. *Office*, *December*, 142. http://scholar.google.com/scholar?hl=en&q=CYBER+WARFARE++AN+ANALYSIS+OF+THE+MEANS+AND+MOTIVATIONS+OF++SELECTED+NATION+STATES+&btnG=&as_sdt=1,5&as_sdtp=#0%5Cnhttp://www.mendeley.com/research/cyber-warfare-analysis-means-motivations-selected-nation-states/

Director of National Intelligence. (2014). *The National Intelligence Strategy of the US 2014*. 1–24.

Fischer, E. A. (2014). Federal Laws Relating to Cybersecurity: Overview of Major Issues, Current Laws, and Proposed Legislation. *Congressional Research Service*, *1*, 77. https://fas.org/sgp/crs/natsec/R42114.pdf

Healey, J. (2011). The Five Futures of Cyber Conflict and Cooperation. *Geo. J. Int'l Aff.*, *12*(Special), 110–118.

Ii, L. W., Tsuchiya, M., & Repko, R. (2017). *Improving Cybersecurity Cooperation between the Governments of the United States and Japan*.

Issn, J. K., & Bagi, S. (2009). *Aa Bambang A.S., 2 Idealisa Fitriana*. 1–15.

Janczewski, L. J., & Caelli, W. (2020). National Cyber Security Organisation. *Cyber Conflicts and Small States*, 87–196. https://doi.org/10.4324/9781315575650-14

Müller, H. (2013). Security Cooperation. *Handbook of International Relations*, *October*, 607–634. https://doi.org/10.4135/9781446247587.n24

Obama, B. (2011). *International Strategy for Cyberspace*. 26. https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

Ottis, R. (2008). Analysis of the 2007 cyber attacks against estonia from the information warfare perspective. *7th European Conference on Information*

Warfare and Security 2008, ECIW 2008, April, 163–168.

Pawlak, P. (2016). Confidence-Building Measures in Cyberspace : Current Debates and Trends. *International Cyber Norms: Legal, Policy & Industry Perspectives*, *20*(April 2015), 129–153.

Pawlak, P., European Commission, I. contributing to S. and P., European Commission’s Directorate-General for International Cooperation and Development, U. "Security, EUISS Task Force for Cyber Capacity Building., & Institute for Security Studies (Paris, F. (2018). *Operational Guidance for the EU’s international cooperation on cyber capacity building*. https://doi.org/10.2815/38445

Rizal, M., & Yani, Y. (2016). Cybersecurity Policy and Its Implementation in Indonesia. *JAS (Journal of ASEAN Studies)*, *4*(1), 61. https://doi.org/10.21512/jas.v4i1.967

Rollins, J., & Henning, A. C. (2010). Comprehensive national cybersecurity initiative: Legal authorities and policy considerations. *Internet Policies and Issues*, *6*, 65–89.

Thomas M. Chen. (2007). An Assessment of the Department of Defense Strategy For Operating in Cyberspace. In *Strategic Studies Institute: Vol. I*. http://www.carlisle.army.mil/ssi

Tobergte, D. R., & Curtis, S. (2013). DOD Strategy for Operating in Cyberspace. *Journal of Chemical Information and Modeling*, *53*(9), 1689–1699.

United States Department of Defense. (2017). *Joint Publication 3-20 Security Cooperation*. *May*, 142. http://www.dtic.mil/doctrine/new_pubs/jp3_20_20172305.pdf

Setiyawan, Anang. (2019). *National Cybersecurity Policy In The U.s and Indonesia.* UNTAG Law Review (ULREV). Volume 3, Issue 1, May 2019, PP 71-87

Buku Putih Pertahanan Indonesia 2014, Kementerian Pertahanan Republik Indonesia.

Zainal A. Hasibuan, (2013). *Indonesia National Cyber Security Strategy: Security and Sovereignty in Indonesia Cyberspace*. Dewan Teknologi Informasi dan komunikasi Nasional.

Schmitt, M. N. (1998). *Computer network attack and the use of force in international law: thoughts on a normative framework*. Colum. J. Transnat'l L., 37, 885.

Charles G. Billo, Welton Chang. (2004). *Cyber Warfare An Analysis Of The Means And Motivations Of Selected Nation States*. The Institute for Security Technology Studies at DartLoIth College.

Chen, T.M., (2013). *An assessment of the department of defense strategy for operating in cyberspace*. Army War College Carlisle Barracks Pa Strategic Studies Institute.

https://www.dhs.gov/cybersecurity (Diakses 23 November 2021)

National Cyber Investigative Joint Task Force — FBI (Diakses 23 November 2021)

Ardiyanti, H. (2014). *Cyber-Security Dan Tantangan Pengembangannya Di Indonesia*. 95–110.

Billo, C. G., & Chang, W. (2004). Cyber Warfare An Analysis of the means and motivations of selected nation states. *Office*, *December*, 142. http://scholar.google.com/scholar?hl=en&q=CYBER+WARFARE++AN+ANALYSIS+OF+THE+MEANS+AND+MOTIVATIONS+OF++SELECTED+NATION+STATES+&btnG=&as_sdt=1,5&as_sdtp=#0%5Cnhttp://www.mendeley.com/research/cyber-warfare-analysis-means-motivations-selected-nation-states/

Director of National Intelligence. (2014). *The National Intelligence Strategy of the US 2014*. 1–24.

Fischer, E. A. (2014). Federal Laws Relating to Cybersecurity: Overview of Major Issues, Current Laws, and Proposed Legislation. *Congressional Research Service*, *1*, 77. https://fas.org/sgp/crs/natsec/R42114.pdf

Healey, J. (2011). The Five Futures of Cyber Conflict and Cooperation. *Geo. J. Int'l Aff.*, *12*(Special), 110–118.

Ii, L. W., Tsuchiya, M., & Repko, R. (2017). *Improving Cybersecurity Cooperation between the Governments of the United States and Japan*.

Issn, J. K., & Bagi, S. (2009). *Aa Bambang A.S., 2 Idealisa Fitriana*. 1–15.

Janczewski, L. J., & Caelli, W. (2020). National Cyber Security Organisation. *Cyber Conflicts and Small States*, 87–196.

https://doi.org/10.4324/9781315575650-14

Müller, H. (2013). Security Cooperation. *Handbook of International Relations*, *October*, 607–634. https://doi.org/10.4135/9781446247587.n24

Obama, B. (2011). *International Strategy for Cyberspace*. 26. https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

Ottis, R. (2008). Analysis of the 2007 cyber attacks against estonia from the information warfare perspective. *7th European Conference on Information Warfare and Security 2008, ECIW 2008, April*, 163–168.

Pawlak, P. (2016). Confidence-Building Measures in Cyberspace : Current Debates and Trends. *International Cyber Norms: Legal, Policy & Industry Perspectives*, *20*(April 2015), 129–153.

Pawlak, P., European Commission, I. contributing to S. and P., European Commission's Directorate-General for International Cooperation and Development, U. "Security, EUISS Task Force for Cyber Capacity Building., & Institute for Security Studies (Paris, F. (2018). *Operational Guidance for the EU's international cooperation on cyber capacity building*. https://doi.org/10.2815/38445

Rizal, M., & Yani, Y. (2016). Cybersecurity Policy and Its Implementation in Indonesia. *JAS (Journal of ASEAN Studies)*, *4*(1), 61. https://doi.org/10.21512/jas.v4i1.967

Rollins, J., & Henning, A. C. (2010). Comprehensive national cybersecurity initiative: Legal authorities and policy considerations. *Internet Policies and Issues*, *6*, 65–89.

Thomas M. Chen. (2007). An Assessment of the Department of Defense Strategy For Operating in Cyberspace. In *Strategic Studies Institute: Vol. I*. http://www.carlisle.army.mil/ssi

Tobergte, D. R., & Curtis, S. (2013). DOD Strategy for Operating in Cyberspace. *Journal of Chemical Information and Modeling*, *53*(9), 1689–1699.

United States Department of Defense. (2017). *Joint Publication 3-20 Security Cooperation*. *May*, 142. http://www.dtic.mil/doctrine/new_pubs/jp3_20_20172305.pdf

Ardiyanti, H. (1986). *Cyber-Security Dan Tantangan Pengembangannya Di Indonesia*. 95–110.

Kurlantzick, J. (2018). *Keeping the U . S . -Indonesia Relationship Moving Forward*. *81*, 1–47

Ardiyanti, H. (2014). *Cyber-Security Dan Tantangan Pengembangannya Di Indonesia*. 95–110.

Billo, C. G., & Chang, W. (2004). Cyber Warfare An Analysis of the means and motivations of selected nation states. *Office*, *December*, 142. http://scholar.google.com/scholar?hl=en&q=CYBER+WARFARE++AN+ANALYSIS+OF+THE+MEANS+AND+MOTIVATIONS+OF++SELECTED+NATION+STATES+&btnG=&as_sdt=1,5&as_sdtp=#0%5Cnhttp://www.mendeley.com/research/cyber-warfare-analysis-means-motivations-selected-nation-states/

Director of National Intelligence. (2014). *The National Intelligence Strategy of the US 2014*. 1–24.

Fischer, E. A. (2014). Federal Laws Relating to Cybersecurity: Overview of Major Issues, Current Laws, and Proposed Legislation. *Congressional Research Service*, *1*, 77. https://fas.org/sgp/crs/natsec/R42114.pdf

Healey, J. (2011). The Five Futures of Cyber Conflict and Cooperation. *Geo. J. Int’l Aff.*, *12*(Special), 110–118.

Ii, L. W., Tsuchiya, M., & Repko, R. (2017). *Improving Cybersecurity Cooperation between the Governments of the United States and Japan*.

Issn, J. K., & Bagi, S. (2009). *Aa Bambang A.S., 2 Idealisa Fitriana*. 1–15.

Janczewski, L. J., & Caelli, W. (2020). National Cyber Security Organisation. *Cyber Conflicts and Small States*, 87–196. https://doi.org/10.4324/9781315575650-14

Müller, H. (2013). Security Cooperation. *Handbook of International Relations*, *October*, 607–634. https://doi.org/10.4135/9781446247587.n24

Obama, B. (2011). *International Strategy for Cyberspace*. 26. https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

Ottis, R. (2008). Analysis of the 2007 cyber attacks against estonia from the information warfare perspective. *7th European Conference on Information Warfare and Security 2008, ECIW 2008*, *April*, 163–168.

Pawlak, P. (2016). Confidence-Building Measures in Cyberspace : Current Debates and Trends. *International Cyber Norms: Legal, Policy & Industry Perspectives*, *20*(April 2015), 129–153.

Pawlak, P., European Commission, I. contributing to S. and P., European Commission’s Directorate-General for International Cooperation and Development, U. "Security, EUISS Task Force for Cyber Capacity Building., & Institute for Security Studies (Paris, F. (2018). *Operational Guidance for the EU’s international cooperation on cyber capacity building*. https://doi.org/10.2815/38445

Rizal, M., & Yani, Y. (2016). Cybersecurity Policy and Its Implementation in Indonesia. *JAS (Journal of ASEAN Studies)*, *4*(1), 61. https://doi.org/10.21512/jas.v4i1.967

Rollins, J., & Henning, A. C. (2010). Comprehensive national cybersecurity initiative: Legal authorities and policy considerations. *Internet Policies and Issues*, *6*, 65–89.

Thomas M. Chen. (2007). An Assessment of the Department of Defense Strategy For Operating in Cyberspace. In *Strategic Studies Institute: Vol. I*. http://www.carlisle.army.mil/ssi

Tobergte, D. R., & Curtis, S. (2013). DOD Strategy for Operating in Cyberspace. *Journal of Chemical Information and Modeling*, *53*(9), 1689–1699.

United States Department of Defense. (2017). *Joint Publication 3-20 Security Cooperation*. *May*, 142. http://www.dtic.mil/doctrine/new_pubs/jp3_20_20172305.pdf

Weimann, G. (2004). Cyberterrorism: How Real is the Threat? *Media Asia*, *29*(3), 149–154. https://doi.org/10.1080/01296612.2002.11726680

Schjolberg, S. (2006). Terrorism in Cyberspace–Myth or reality? *Terrorism*, *1998*(December 2005), 1–20. http://www.cybercrimelaw.net/documents/Terrorism_in_cyberspace.pdf

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. https://doi.org/10.25041/fiatjustisia.v13no4.1735

Dorothy E. Denning, Professor, Naval Postgraduate School, (2000). USA: Testimony before the Special Oversight Panel on Terrorism, Committee on Armed Services, U.S. House of Representatives.

Keith Lourdeau, Deputy Assistant Director, Cyber Division, (2004). FBI: Terrorism, Technology, and Homeland Security. Testimony before the Senate Judiciary Subcommittee.

See the International Handbook on Critical Information Infrastructure Protection (CIIP) 2006 Vol. II, page 14

Wilson, Clay. (2008). Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress. Congressional Research Service (CRS). Januray. 7-5700.

Brunst, Phillip. (2009). Terrorism and the Internet: New Threats Posed by Cyberterrorism and Terrorist Use of the Internet. A War on Terror? : The European Stance on a New Threat, Changing Laws and Human Rights Implications, 51-78 (2009). 10.1007/978-0-387-89291-7-3.

Taliharm, A.-M. (2010). Cyberterrorism: in Theory or in Practice? *Defence Against Terrorism Review*, *3*(2), 59–74. http://www.tmmm.tsk.tr/publication/datr/volume6/05-Cyberterrorism_in_Theory_or_in_Practice.pdf

Gabriela Luca, (2017). “Manifestations of Contemporary Terrorism: Cyber-terrorism”, Research and Science Today, pp. 20–25.

Kuehl, D. T. (2011). From cyberspace to cyberpower: Defining the problem. *Cyberpower and National Security*, 24–42.

Nye, J. S. (2018). Cyber power. *Routledge Handbook of Russian Foreign Policy*, *May*, 182–198. https://doi.org/10.4324/9781315536934

Ziolkowski, K. (2013). Peacetime cyber espionage: New tendencies in public international law. In *Peacetime Regime for State Activities in Cyberspace*. https://s3.amazonaws.com/academia.edu.documents/40986873/Peacetime-Regime_for_state_activities_in_cyberspace.pdf?response-content-disposition=inline%3B filename%3DPeacetime-

Regime_for_state_activities_in.pdf&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credent

Klimburg, A. (2011). Mobilising cyber power. *Survival*, *53*(1), 41–60. https://doi.org/10.1080/00396338.2011.555595

https://www.youtube.com/watch?v=CI19w3yYMMQ&ab_channel=RiskGroupLLC (diakses 24 November 2021)

Ardiyanti, H. (2014). *Cyber-Security Dan Tantangan Pengembangannya Di Indonesia*. 95–110.

Billo, C. G., & Chang, W. (2004). Cyber Warfare An Analysis of the means and motivations of selected nation states. *Office*, *December*, 142. http://scholar.google.com/scholar?hl=en&q=CYBER+WARFARE++AN+ANALYSIS+OF+THE+MEANS+AND+MOTIVATIONS+OF++SELECTED+NATION+STATES+&btnG=&as_sdt=1,5&as_sdtp=#0%5Cnhttp://www.mendeley.com/research/cyber-warfare-analysis-means-motivations-selected-nation-states/

Director of National Intelligence. (2014). *The National Intelligence Strategy of the US 2014*. 1–24.

Fischer, E. A. (2014). Federal Laws Relating to Cybersecurity: Overview of Major Issues, Current Laws, and Proposed Legislation. *Congressional Research Service*, *1*, 77. https://fas.org/sgp/crs/natsec/R42114.pdf

Healey, J. (2011). The Five Futures of Cyber Conflict and Cooperation. *Geo. J. Int'l Aff.*, *12*(Special), 110–118.

Ii, L. W., Tsuchiya, M., & Repko, R. (2017). *Improving Cybersecurity Cooperation between the Governments of the United States and Japan*.

Issn, J. K., & Bagi, S. (2009). *Aa Bambang A.S., 2 Idealisa Fitriana*. 1–15.

Janczewski, L. J., & Caelli, W. (2020). National Cyber Security Organisation. *Cyber Conflicts and Small States*, 87–196. https://doi.org/10.4324/9781315575650-14

Müller, H. (2013). Security Cooperation. *Handbook of International Relations*, *October*, 607–634. https://doi.org/10.4135/9781446247587.n24

Obama, B. (2011). *International Strategy for Cyberspace*. 26. https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strat egy_for_cyberspace.pdf

Ottis, R. (2008). Analysis of the 2007 cyber attacks against estonia from the information warfare perspective. *7th European Conference on Information Warfare and Security 2008*, *ECIW 2008*, *April*, 163–168.

Pawlak, P. (2016). Confidence-Building Measures in Cyberspace : Current Debates and Trends. *International Cyber Norms: Legal, Policy & Industry Perspectives*, *20*(April 2015), 129–153.

Pawlak, P., European Commission, I. contributing to S. and P., European Commission’s Directorate-General for International Cooperation and Development, U. "Security, EUISS Task Force for Cyber Capacity Building., & Institute for Security Studies (Paris, F. (2018). *Operational Guidance for the EU’s international cooperation on cyber capacity building*. https://doi.org/10.2815/38445

Rizal, M., & Yani, Y. (2016). Cybersecurity Policy and Its Implementation in Indonesia. *JAS (Journal of ASEAN Studies)*, *4*(1), 61. https://doi.org/10.21512/jas.v4i1.967

Rollins, J., & Henning, A. C. (2010). Comprehensive national cybersecurity initiative: Legal authorities and policy considerations. *Internet Policies and Issues*, *6*, 65–89.

Thomas M. Chen. (2007). An Assessment of the Department of Defense Strategy For Operating in Cyberspace. In *Strategic Studies Institute: Vol. I*. http://www.carlisle.army.mil/ssi

Tobergte, D. R., & Curtis, S. (2013). DOD Strategy for Operating in Cyberspace. *Journal of Chemical Information and Modeling*, *53*(9), 1689–1699.

United States Department of Defense. (2017). *Joint Publication 3-20 Security Cooperation*. *May*, 142. http://www.dtic.mil/doctrine/new_pubs/jp3_20_20172305.pdf

Moh. Nazir. 1988. Metodologi Penelitian. Jakarta: Ghalia Indonesia.

Bryman, A. (2012). Social Research Method (4th Edition). New York: Oxford University Press.

Bryman, A. (2012). Social Research Methods . New York: Oxford University Press Inc.

Hasan, M. Iqbal, Pokok-pokok Materi Metodologi Penelitian dan Aplikasinya, Ghalia Indonesia, Bogor, 2002.

Ardiyanti, H. (2014). *Cyber-Security Dan Tantangan Pengembangannya Di Indonesia*. 95–110.

Billo, C. G., & Chang, W. (2004). Cyber Warfare An Analysis of the means and motivations of selected nation states. *Office*, *December*, 142. http://scholar.google.com/scholar?hl=en&q=CYBER+WARFARE++AN+ANALYSIS+OF+THE+MEANS+AND+MOTIVATIONS+OF++SELECTED+NATION+STATES+&btnG=&as_sdt=1,5&as_sdtp=#0%5Cnhttp://www.mendeley.com/research/cyber-warfare-analysis-means-motivations-selected-nation-states/

Director of National Intelligence. (2014). *The National Intelligence Strategy of the US 2014*. 1–24.

Fischer, E. A. (2014). Federal Laws Relating to Cybersecurity: Overview of Major Issues, Current Laws, and Proposed Legislation. *Congressional Research Service*, *1*, 77. https://fas.org/sgp/crs/natsec/R42114.pdf

Healey, J. (2011). The Five Futures of Cyber Conflict and Cooperation. *Geo. J. Int'l Aff.*, *12*(Special), 110–118.

Ii, L. W., Tsuchiya, M., & Repko, R. (2017). *Improving Cybersecurity Cooperation between the Governments of the United States and Japan*.

Issn, J. K., & Bagi, S. (2009). *Aa Bambang A.S., 2 Idealisa Fitriana*. 1–15.

Janczewski, L. J., & Caelli, W. (2020). National Cyber Security Organisation. *Cyber Conflicts and Small States*, 87–196. https://doi.org/10.4324/9781315575650-14

Müller, H. (2013). Security Cooperation. *Handbook of International Relations*, *October*, 607–634. https://doi.org/10.4135/9781446247587.n24

Obama, B. (2011). *International Strategy for Cyberspace*. 26. https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

Ottis, R. (2008). Analysis of the 2007 cyber attacks against estonia from the information warfare perspective. *7th European Conference on Information Warfare and Security 2008, ECIW 2008*, *April*, 163–168.

Pawlak, P. (2016). Confidence-Building Measures in Cyberspace : Current Debates and Trends. *International Cyber Norms: Legal, Policy & Industry Perspectives*, *20*(April 2015), 129–153.

Pawlak, P., European Commission, I. contributing to S. and P., European Commission’s Directorate-General for International Cooperation and Development, U. "Security, EUISS Task Force for Cyber Capacity Building., & Institute for Security Studies (Paris, F. (2018). *Operational Guidance for the EU’s international cooperation on cyber capacity building*. https://doi.org/10.2815/38445

Rizal, M., & Yani, Y. (2016). Cybersecurity Policy and Its Implementation in Indonesia. *JAS (Journal of ASEAN Studies)*, *4*(1), 61. https://doi.org/10.21512/jas.v4i1.967

Rollins, J., & Henning, A. C. (2010). Comprehensive national cybersecurity initiative: Legal authorities and policy considerations. *Internet Policies and Issues*, *6*, 65–89.

Thomas M. Chen. (2007). An Assessment of the Department of Defense Strategy For Operating in Cyberspace. In *Strategic Studies Institute: Vol. I*. http://www.carlisle.army.mil/ssi

Tobergte, D. R., & Curtis, S. (2013). DOD Strategy for Operating in Cyberspace. *Journal of Chemical Information and Modeling*, *53*(9), 1689–1699.

United States Department of Defense. (2017). *Joint Publication 3-20 Security Cooperation*. *May*, 142. http://www.dtic.mil/doctrine/new_pubs/jp3_20_20172305.pdf

https://www.marshallcenter.org/en/publications/marshall-center-papers/cooperative-security-new-horizons-international-order/cooperative-security-theory-practice (diakses 7 Januari 2022)

https://www.cisa.gov/uscert/ncas/tips/ST04-001 (diakses 7 Januari 2022)

Amoroso, E. 2006. Cyber Security. New Jersey: Silicon Press

ITU. 2009. Overview of Cybersecurity. Recommendation ITU-T X.1205. Geneva: International Telecommunication Union (ITU). http://www.itu.int/rec/T-REC-X.1205-200804-I/en

DHS. 2014. A Glossary of Common Cybersecurity Terminology. National Initiative for Cybersecurity Careers and Studies: Department of Homeland Security. October 1, 2014: http://niccs.us-cert.gov/glossary#letter_c

Cisco Mid-Year Security Report 2016: The Rise of Ransomware Cisco 2016 Midyear Cybersecurity Report

The Ministry of Defense of the Republic of Indonesia. (2013). A Road Map to Cyber Defense National Strategy. Jakarta: The Ministry of Defense of the Republic of Indonesia.

The Department of Defense of the Republic of Indonesia. (2008). Indonesian Defense White Paper. Jakarta: The Departement of Defense of the Republic of Indonesia.

ASEAN Secretariat. (2013). ASEAN's Cooperation on Cybersecurity and against Cybercrime. Octopus Conference: Cooperation Against Cybercrime Strasbourg, France: Council of Europe.

Aaron Boyd, '2014 FISMA reduces paperwork, codifies management structure', Federal Times, 2014 https://www.federaltimes.com/management/2014/12/16/2014-fisma-reduces-paperwork-codifies-management-structure/ (Diakses 23 Mei 2022)

Ariesta, M. (2019). Keamanan Siber Jadi Perhatian Khusus Indonesia dan Australia. Keamanan Siber Jadi Perhatian Khusus Indonesia dan Australia - Medcom.id (Diakses 24 Mei 2022)

US Department of State. (2022). U.S. Relations With Indonesia. U.S. Relations With Indonesia - United States Department of State (Diakses 24 Mei, 2022)

The Indonesian National Cyber and Crypto Agency. 2020. Annual Report 2020: Cybersecurity Monitoring, Jakarta: BSSN, 11.

Laila Afifa. 2021. "6 Major Data Breach Cases in Indonesia in Past 1.5 Years," Tempo. https://en.tempo.co/read/1501851/6-major-data-breach-cases-in-indonesia-in-past-1-5-years (Diakses 5 Juni 2022)

Gera . (2018). LIPI: Dibutuhkan Badan Cyber Nasional Indonesia. Retrieved fromVoa Indonesia. https://www.voaindonesia.com/a/lipi-dibutuhkan-badan-cyber-nasional-di-indonesia-/2591870.html (Diakses 6 Juni 2022)

Astuti, S. A. (2015). Law Enforcement of Cyber Terorism in Indonesia.

Rechtsidee, *2*(2), 157–178. https://doi.org/10.21070/jihr.v2i2.82

Eichensehr, K. E. (2019). Symposium on cyber attribution decentralized cyberattack attribution. *AJIL Unbound*, *113*(2014), 213–217. https://doi.org/10.1017/aju.2019.33

Fatihah, C. Y. N. (2021). *Cybersecurity , Sovereignty , and Indonesia ' s Foreign Policy*.

Fatihah, C. Y. N. (2022). *Indonesia Law Review Establishing A Legitimate Indonesia ' s Government Electronic Surveillance Regulation : A Comparison with The U . S . Legal Practices Establishing A Legitimate Indonesia ' s Government Electronic Surveillance*. *11*(2).

Gill, P., Stewart, K., Treasure, E., & Chadwick, B. (2008). Methods of data collection in qualitative research: Interviews and focus groups. *British Dental Journal*, *204*(6), 291–295. https://doi.org/10.1038/bdj.2008.192

Gupta, A., & Wolf, J. (2018). An Examination of Cybersecurity Knowledge Transfer: Teaching, Research, and Website Security at U.S. Colleges and Universities. *Journal of Cybersecurity Education, Research and Practice, 2018*(2), 4.

Hatta, M., Rajamanickam, R., Abdullah, D., Hartono, H., Saleh, A. A., Djanggih, H., Bunga, M., Wahab, M., Susena, K. C., Abbas, I., Aswari, A., & Sriadhi, S. (2018). Internet and Terrorism in Indonesia. *Journal of Physics: Conference Series*, *1114*(1). https://doi.org/10.1088/1742-6596/1114/1/012080

Hoadley, S. (1988). Security Cooperation in the South Pacific. *Regional Cooperation in the Pacific Era*, 15.

Johnson, C., Badger, L., Waltermire, D., Snyder, J., & Skorupka, C. (2016). Guide to Cyber Threat Information Sharing. *NIST Special Publication*, 800–150. http://dx.doi.org/10.6028/NIST.SP.800-150

Juned, M., Samhudi, G. R., & Akhli, R. A. (2022). *The Social Impact of Expanding the Indonesian Military Mandate on Counter-terrorism Implikasi Sosial Perluasan Tugas Tentara Nasional Indonesia dalam Kontra Terorisme*. *13*(1), 105–115.

Kemmerer, R. A. (2003). Cybersecurity. *Department of Computer Science*

University of California Santa Barbara, *6*, 1–23.

Khan, O. H. (2015). Transfer of Technology Agreements in International Business. *Galgotias Journal of Legal Studies*, *III*(1), 1–23.

Kurlantzick, J. (2018). *Keeping the U . S . -Indonesia Relationship Moving Forward*. *81*, 1–47.

Meyer, P. (2015). Seizing the Diplomatic Initiative to Control Cyber Conflict. *Washington Quarterly*, *38*(2), 47–61. https://doi.org/10.1080/0163660X.2015.1064709

Office of the United Nations High Commissioner for Human Rights. (2008). Human Rights , Terrorism and Counter-terrorism. *Terrorism*, *32*, 1–76. https://docs.google.com/viewer?a=v&q=cache:zDkNc7Gm71cJ:www.ohchr.org/Documents/Publications/Factsheet32EN.pdf+Adding+International+Terrorism+into+the+Statute+of+the+ICC:+Definition,+Benefits+to+Justice+and+Obstacles&hl=en&gl=nl&pid=bl&srcid=ADGEESjHdkHAr

Pawlak, P. (2016). Confidence-Building Measures in Cyberspace : Current Debates and Trends. *International Cyber Norms: Legal, Policy & Industry Perspectives*, *20*(April 2015), 129–153.

Pawlak, P., European Commission, I. contributing to S. and P., European Commission’s Directorate-General for International Cooperation and Development, U. "Security, EUISS Task Force for Cyber Capacity Building., & Institute for Security Studies (Paris, F. (2018). *Operational Guidance for the EU’s international cooperation on cyber capacity building*. https://doi.org/10.2815/38445

Rizal, M., & Yani, Y. (2016). Cybersecurity Policy and Its Implementation in Indonesia. *JAS (Journal of ASEAN Studies)*, *4*(1), 61. https://doi.org/10.21512/jas.v4i1.967

Smith, E. A. (2001). *The role of tacit and explicit knowledge in the workplace*. *5*(4), 311–321.

Steenhuis, H. J. (2000). *International technology transfer: Building theory from a multiple case-study in the aircraft industry. Doctoral Thesis. 1360*.

Taichman, E. (2021). *Defend Forward & Sovereignty : How America ’ s Cyberwar Strategy Upholds International Law Defend Forward &*

Sovereignty : How America ' s Cyberwar Strategy Upholds International Law. *53*(1).

Taufik, A. F. (2021). Indonesia's cyber diplomacy strategy as a deterrence means to face the threat in the indo-pacific region. *Journal of Physics: Conference Series*, *1721*(1). https://doi.org/10.1088/1742-6596/1721/1/012048

Tirrell, W. K., & George, T. (2012). *UNITED STATES CYBERSECURITY STRATEGY , POLICY , AND ORGANIZATION : POORLY POSTURED TO COPE WITH A POST-9 / 11 SECURITY ENVIRONMENT ? A thesis presented to the Faculty of the U . S . Army Command and General Staff College in partial fulfillment of the requ*.

United Nations. (2002). United Nations system support for capacity-building. *United Nations Economic and Social Council*, *2002*(58).

Valencia, M. J. (2017). *Trump Administration ' s South China Sea Policy*. *June*, 1940.

Valeriano, B. (2015). Cyber War Versus Cyber Realities: Cyber Conflict in the International System by Brandon Valeriano and Ryan C. Maness. *Journal of Information Technology & Politics*, *12*(4), 399–401. https://doi.org/10.1080/19331681.2015.1101039

Kusamaatmadja, Mochtar. (1999). Pengantar Hukum Internasional,. 9th ed. Bandung: Putra Abardin.

Golose, Petrus Reinhard. (2015). Invasi Terrorisme Ke Cyberspace. Jakarta: YPKIK.

Nusantara, Abdul Hakim G. (2003). Undang-Undang Pemberantasan Tindak Pidana Terorisme Dalam Perspektif Negara Hukum. Bandung: Badan Pembinaan Hukum Nasional.