

## DAFTAR PUSTAKA

- Alperovitch, Dmitri. "Revealed: Operation Shady RAT". *McAfee White Paper* (2012)
- Baezner, Marie. "Cybersecurity in Sino-American Relations". *CSS Analyses in Security Policy*. No.224. (2018)
- Budd, Christopher. "Operation Iron Tiger: Attackers Shift From East Asia to the United States". *TrendMicro*. (2015). <https://newsroom.trendmicro.com/blog/operation-iron-tiger-attackers-shift-east-asia-united-states>. (diakses 9 Maret 2019)
- Bebber, Robert. "China's Cyber Economic Warfare Threatens U.S.". *US Naval Institute*. Vol.143. No. 7. (2017)
- Bortz, Travis. "Cyberspace: United States vs China". *The Journal of High Technology Law*. <https://sites.suffolk.edu/jhtl/2014/04/04/cyberspace-united-states-v-china/> (diakses 15 Maret 2019)
- Cambridge Dictionary. <https://dictionary.cambridge.org/dictionary/english/cyber-warfare>. (diakses 11 Maret 2019)
- Center for Internet Safety. *The Ostrich Effect-In Search of A Realistic Model for Cybersecurity*. University of Canberra. <http://www.canberra.edu.au/cis/storage/CIS%20Cyber%20Whitepaper%20-%20FINAL.pdf>, (diakses 9 Maret 2019)
- Chang, Ziv, dkk. *Operation Iron Tiger: Exploring Chinese Cyber-Espionage Attacks on United States Defense Contractors*, TrendMicro Research Paper. 2015. [https://www.era1.com/CustomUploads/ca/wp/2015\\_12\\_wp\\_operation\\_iron\\_tiger.pdf](https://www.era1.com/CustomUploads/ca/wp/2015_12_wp_operation_iron_tiger.pdf), (diakses 9 Maret 2019)
- Choucri, Nazli. *Cyberpolitics in International Relations*. Cambridge : MIT Press. (2012)
- Cooper, Zach. "Understanding the Chinese Communist Party's Approach to Cyber-Enabled Economic Warfare". (Washington DC: FDD Press. 2018)

Department of Homeland Security. "Brief Documentary History of the Department of Homeland Security 2001-2008" <https://www.hsdl.org/?view&did=37027>. diakses (3 April 2019)

Digital Watch. "UN GGE". <https://dig.watch/processes/ungge> (diakses 17 April 2019)

Dunn Caveltly, Myriam. *Cyber Security*. Oxford:Oxford University Press.(2012)

Eftimiades, Nicholas. "The Impact of Chinese Espionage to United States of America". *The Diplomat*. <https://thediplomat.com/2018/12/the-impact-of-chinese-espionage-on-the-united-states/>.(diakses 11 Maret 2019)

Finkle, Jim."Hacker Group in China Linked to Big Cyber Attacks : Symantec".Reuters (2013) <https://www.reuters.com/article/us-cyberattacks-china/hacker-group-in-china-linked-to-big-cyber-attacks-symantec-idUSBRE98G0M720130917>. (diakses 12 Maret 2019)

Finnermore, Martha. dan Duncan B. Hollis. "Constructing Norms for Global Cybersecurity". *The American Journal of International Law*. Vol.110. No.3 (2016)

Fisher, Eric A. dkk., "The 2013 Cyber security Executive Order: Overview and Considerations for Congress". Congressional Research Service. (2013) <http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEB B424 /docs/Cyber-089.pdf>.

Geng, Zhao. "An Analysis of Cyberspace Rule-Making in China-US Relations".*International Relations and Diplomacy*. Vol. 6. No.1.2018. doi: 10.17265/2328-2134/2018.01.002

Gertz, Bill. "Cyber Attacks on U.S. Firms, Google Traced to Chinese".Washington Times (2010) <https://www.washingtontimes.com/news/2010/mar/24/cyber-attack-on-us-firms-google-traced-to-chinese/>. (diakses 12 Maret 2019)

Greenwald, Eric A. . "History Repeats Itself: The 60- Day Cyberspace Policy Review in Context".*Journal of National Security Law and Policy*.Vol.4.No.41

Hunker, Jeffrey."U.S. International Policy for Cybersecurity: Five Issues That Won't Go Away". *Journal of National Security Law and Policy*. Vol.47. No.197 (2010)

Hollis, Duncan B. "China and the US Strategic Construction of Cybernorms: The Process is the Product". *Aegis Paper Series*.No.1704

Kawulich, Barbara D. *Data Analysis Technique in Qualitative Research*. Georgia: State University of Georgia. 2005.

Keizer, Gregg."Shady RAT Hacking Claims Overblown, Say Security Firms".*Computer World*.(2011) <https://www.computerworld.com/article/2509930/-shady-rat--hacking-claims-overblown--say-security-firms.html>, (diakses 8 Maret 2019)

Lawrence, Susan V. "US – China Relations: An Overview of Policy Issues". *Congresional Research Service*. (2013) <https://fas.org/sgp/crs/row/R41108.pdf>, (diakses 29 Maret 2019)

Lewis, James A."Computer Espionage, Titan Rain and China".Center for Strategic and International Studies-Technology and Public Policy Program, <http://cybercampaigns.net/wp-content/uploads/2013/05/Titan-Rain-Moonlight-Maze.pdf> (diakses 6 Maret 2019 )

Liaropoulos, Andrew .“Great Power Politics in Cyberspace: U.S. and China are Drawing the Lines Between Confrontation and Cooperation”. PANORAMA of Global Security Environment (2013)

Lieberthal, Kenneth dan Peter W Singer. “Cyber Security and U.S – China Relations”. Brookings. (2012)

Lindsay, Jon R. Tai Ming Cheung, dan Derek S. Reveron. *China and Cybersecurity:Espionage, Strategy, Politics in the Digital Domain*. (USA:Oxford University Press,2015)

Louie, Celia. “U.S-China Cybersecurity Cooperation”. The Henry M. Jackson School of International Studies.(2017). <https://jsis.washington.edu/news/u-s-china-cybersecurity-cooperation/> (diakses 23 April 2019)

Powner, David. "National Cybersecurity Strategy: Key Improvements Are Needed to Strengthen the Nation's Posture". *United States Government Accountability Office*. 2009

Maurer, Tim dan Kathryn Taylor. "Outlook on International Cyber Norms: Three Avenues For Future Progress". *Carneige Endowment for International Peace*. 2018. <https://carnegieendowment.org/2018/03/02/outlook-on-international-cyber-norms-three-avenues-for-future-progress-pub-75704> (diakses 17 April 2019)

Matusitz, Jonathan. "Cyberterrorism: A Description from Multiple Perspectives". *International Journal of Information Technology*. Vol.16. No.1 (2010)

Mas'ood, Mohtar. *Ilmu Hubungan Internasional: Disiplin dan Metodologi*. Yogyakarta: Pusat Antar Universitas-Studi Sosial Universitas Gadjah Mada, LP3E. 1990

McKenzie, Timothy M. "Is Cyber Deterrence Possible". *Air Force Research Institute Papers* (2017)

Middleton, Bruce. "A History of Cyber Security Attacks: 1980 to Present". (USA: CRC Press. 2017)

Nicola, Stefan. "China Working to Halt Commercial Cyberwar in Deal with Germany", *BLOOMBERG* (2015) <https://www.bloomberg.com/news/articles/2015-10-29/china-working-to-halt-commercial-cyberwar-in-deal-with-germany> (diakses, 29 April 2019)

Patterson Manson III, George. "Cyberwar : The United States and China Prepare for the Next Generation of Conflict". *Comparative Strategy*. Vol.30. No.2. DOI:10.1080/01495933.2011.561730

Pidathala, Vinay, dkk. "Threat Research: Operation Beebus". *FireEye*. <https://www.fireeye.com/blog/threat-research/2013/02/operation-beebus.html>. (diakses 9 Maret 2019)

Price, David H. "The New Surveillance Normal: NSA and Corporate Surveillance in the Age of Global Capitalism". *Monthly Review*. 2014. [https://www.researchgate.net/publication/274283920\\_The\\_New\\_Surveillance\\_Normal\\_NSA\\_and\\_Corporate\\_Surveillance\\_in\\_the\\_Age\\_of\\_Global\\_Capitalism](https://www.researchgate.net/publication/274283920_The_New_Surveillance_Normal_NSA_and_Corporate_Surveillance_in_the_Age_of_Global_Capitalism) (diakses 12 Maret 2019)

Presidential Document. “Executive Order 13694: Blocking the Property of Certain Person Engaging in Significant Malicious Cyber-Enabled Activities”. *Federal Register*. Vol. 80. No. 63 (2015)

RAND Cooperation. <https://www.rand.org/topics/cyber-warfare.html>. (diakses 11 Maret 2011)

Renard, Thomas. “US-China Cybersecurity Agreement : A Good Case of Cyber Diplomacy”. *Europe for Citizens Programme of the European Union*. 2015

Rubenstein, Dana.”Nation State Cyber Espionage and Its Impact”. Washington University in St.Louis. <https://www.google.com/search?q=cse+wustle+edu&oq=cse+wustle+edu &sourceid=chrome&ie=UTF-8>. (diakses 10 Maret 2019)

Rollins, John W. “U.S – China Cyber Agreement”. CRS Insight. <https://fas.org/sgp/crs/row/IN10376.pdf> (diakses 30 Maret 2019)

Ryan, Camille dan Jamie M. Lewis. “Computer and Internet Use in the United States : 2015”. *American Community Survey Reports*. 2017. diakses di <https://www.census.gov/content/dam/Census/library/publications/2017/acs/acs-37.pdf>, 18 Desember 2018

Saalman, Lora .“Rethinking China-Russia-U.S. Deterrence in Cyberspace”.*ThinkChina.dk Policy Brief*. No.4 (2017)

Sanger David E. dan Nicole Perloth.”NSA Breached Chinese Servers Seen as Security Threat”.New York Times, <https://www.nytimes.com/2014/03/23/world/asia/nsa-breached-chinese-servers-seen-as-spy-peril.html>. (diakses 12 maret 2019)

Schou, Corey D. dan Kenneth J. Trimmer. “Information Assurance and Security”. *Journal of Organizational and End User Computing on Information Security* (2005).[https://www.researchgate.net/publication/220349069\\_Information\\_Assurance\\_and\\_Security](https://www.researchgate.net/publication/220349069_Information_Assurance_and_Security)

Siddiqi Murtaza A., dan Naveed Ghani. “Critical Analysis on Advanced Persistent Threats”. *International Journal of Computer Applications*. Vol.141. No.13 (2016)

Smeets, Max. dan Herbert S. Lin. “Offensive Cyber Capabilities: To What End” NATO CCDCOE (2018)

Spiegel.”NSA Spied on Chinese Government and Networking Firm”. 2014.  
<http://www.spiegel.de/international/world/nsa-spied-on-chinese-government-and-networking-firm-huawei-a-960199.html>. (diakses 12 Maret 2019)

Stevens, T. “A cyberwar of ideas?: Deterrence and norms in cyberspace”. *Contemporary Security Policy*. Vol. 33. No.1. (2012): 151.  
doi:10.1080/13523260.2012.659597

Symantec. “Internet Security Threat Report”. Vol.21,2017.diakses di  
<https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf>, (22 November 2018)

The White House. “Critical Foundations: Protecting America’s Infrastructure”(1997) <https://fas.org/sgp/library/pccip.pdf>, diakses 7 April 2019

The White House. “Presidential Decision Directive/NSC-63”(1998) <https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-012.pdf> (diakses 7 April 2019)

The White House, “National Plan for Information Systems Protection Version 1.0”, 2000, <https://fas.org/irp/offdocs/pdd/CIP-plan.pdf>, diakses (7 April 2019)

The White House.”The National Strategy to Secure Cyberspace”.2003.  
<https://www.energy.gov/sites/prod/files/National%20Strategy%20to%20Secure%20Cyberspace.pdf>. (diakses 1 April 2019)



The White House. “Presidential Policy Directive/PPD-21: Critical Infrastructure Security and Resilience,” U.S. General Services Administration. [http://www.gsa.gov/portal/mediaId/176571/fileName/ATTCH\\_2\\_-\\_PPD-21.action](http://www.gsa.gov/portal/mediaId/176571/fileName/ATTCH_2_-_PPD-21.action) (diakses 19 April 2019)

The White House Office of the Press Secretary. “The U.S-China Strategic and Economic Dialogue”. 2009. <https://obamawhitehouse.archives.gov/realitycheck/the-press-office/remarks-president-uschina-strategic-and-economic-dialogue>. (diakses 27 Maret 2019)

The White House Office of the Press Secretary. “U.S-China Joint Statement”. 2011. <https://obamawhitehouse.archives.gov/the-pressoffice/2011/01/19/us-china-joint-statement>. (diakses 27 Maret 2019)

The White House. “The National Strategy to Secure Cyberspace”. Washington. 2003. diakses di <https://georgewbush-whitehouse.archives.gov/pcipb/> (diakses 18 Desember 2018)

The White House. “Cyberspace Policy Review : Assuring a Trusted and Resilient Information and Communication Infrastructure”. 2010 diakses di [http://www.whitehouse.gov/assets/documents/Cyberspace\\_Policy\\_Review\\_final.pdf](http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf)

Thornburgh, Nathan.”Inside the Chinese Hack Attack”.TIME. <http://content.time.com/time/nation/article/0,8599,1098371,00.html> (diakses 6 Maret 2019)

Trisal, Sidarth.”Remembering Operation Titan Rain”.Cyware. <https://cyware.com/news/remembering-operation-titan-rain-c54ad3e4>, (diakses 6 Maret 2019)

U.S Department of Defense.”Department of Defense Strategy for Operating in Cyberspace” (2011)

Usman, Husaini dan Purnomo Setiady Akbar.*Metodologi Penelitian Sosial*. Jakarta: PT Bumi Aksara. 2011

Vaidya, V. "2001-2003: Survey and Analysis of Major Cyberattacks". Georgetown University. <https://arxiv.org/pdf/1507.06673.pdf>. (diakses 10 Maret 2019)

Valeriano, Brandon dan Ryan C Maness. The Dynamics of Cyber Conflict between Rival Antagonist. *Journal of Peace Research*. Vol.51. No.3. 2011

Warren Harold, Scott, Martin C. Libicki, Astrid Stuth Cevallos. "Getting Yes With China in Cyberspace". ( Santa Monica, CA: RAND Corporation. 2016)

Wong, Edward. "Hacking U.S. Secrets, China Pushes for Drones". The New York Times. 2013. <https://www.nytimes.com/2013/09/21/world/asia/hacking-us-secrets-china-pushes-for-drones.html>, (diakses 9 Maret 2019)

Xu, Ting. "China and The United States : Hacking Away at Cyber Warfare". *Asia Pacific Bulletin*. No. 135. 2011

Yeniman Yildirim, Erbu . "The Importance of Risk Management in Information Security". IIER International Conference. ISBN: 978-93-86083-34-0 (2016)

