Bab IV
Kesimpulan

Berdasarkan pembahasan yang telah ditulis sebelumnya, penelitian ini menemukan lima hal utama. Pertama adalah teknologi siber semakin berperan penting dalam politik dan keamanan suatu negara. Kedua, negara-negara mulai mengembangkan kapabilitas sibernya, baik dari segi institusi maupun mekanisme resmi yang dirancang oleh pemerintahnya masing-masing. Ketiga, negara dalam pengembangan kapabilitas siber ini pun masih menemui perbedaan dan tantangannya tersendiri seperti ketersediaan infrastruktur dan keahlian dalam teknologi keamanan siber. Keempat, akibat dari tantangan yang ditemui negara di bidang siber, terbuka peluang bagi sektor swasta untuk menawarkan jasa dan keahliannya untuk digunakan oleh negara lain dalam memenuhi celah yang ada. Terakhir, dalam kasus tertentu negara dapat mengambil *extraordinary* atau *emergency measures* ketika menemui suatu ancaman sesuai dengan pre-kondisi yang negara tersebut miliki. Poin terakhir inilah yang menjadi titik pembeda kebijakan negara yang diteliti dengan negara lain.

Lima temuan tersebut membantu untuk menjawab pertanyaan penelitian, mengapa UEA menggunakan *cyber mercenaries* dalam merespons ancaman sibernya? Jawabannya adalah UEA menggunakan *cyber mercenaries* karena mereka terdesak oleh situasi darurat atau luar biasa yang menyulitkan mereka untuk menggunakan mekanisme resmi. Lebih dalamnya, jawaban pertanyaan penelitian dapat terletak dalam tiga pre-kondisi yang dimiliki oleh UEA itu sendiri yaitu; 1) mereka memiliki aturan baru yakni *UAE Federal Decree Law No. 3 of 2012* yang memungkinkan mereka untuk mengambil *extraordinary* or *emergency measures,* 2) adanya pelimpahan kuasa darurat dari pemerintah pusat kepada badan yang menangani keamanan siber, dan 3) aparat yang diberi kuasa tidak memiliki keahlian atau pengalaman dalam mengatasi ancaman siber. Melalui tiga kondisi tersebut, maka UEA dapat mengambil pendekatan yang relatif berbeda dengan negara lain yang sudah memiliki sumber daya yang memadai untuk memakai militer atau badan resmi negara.

Kendati begitu, penelitian ini masih menemui beberapa keterbatasan terkait dengan ketersediaan data. Dikarenakan sifat operasi Project Raven yang rahasia ini, maka penelitian ini tidak dapat memastikan 100% tentang arah kebijakan yang diambil oleh UEA. Penelitian ini hanya berusaha untuk terjun lebih dalam mengenai apa yang terjadi di dalam *black box* pengambilan keputusan yang dilakukan oleh NESA dan jajaran manajemen Project Raven itu sendiri. Selain itu, sifat dari studi keamanan siber ini mungkin masih berada di tahapan awal yang memungkinkan peneliti-peneliti selanjutnya dapat memiliki jawaban berbeda terkait apa yang penelitian ini hendak temukan. Oleh karena itu, penelitian ini membataskan jumlah aktor yang diteliti di beberapa negara khususnya UEA dan kawasan Teluk.

Maka daripada itu, penelitian ini masih bisa dijelajah lebih jauh dalam beberapa poin. Pertama terkait pengaruh keleluasaan perdagangan teknologi *spyware* antar aktor, baik negara maupun non-negara. Hal ini penting karena dampaknya dapat berpengaruh langsung terhadap operasi siber ofensif yang dilakukan negara-negara terhadap target sasarannya. Selain itu, penelitian ini juga bisa ditambah lagi ke sektor dampak dari manipulasi informasi terhadap akibat dari penggunaan teknologi siber sesuai dengan contoh kasus yang dipaparkan sebelumnya. Manipulasi ini mungkin dapat menjawab permasalahan polarisasi di dalam masyarakat khususnya terkait dengan gejolak politik yang ada di masing-masing negara. Terakhir, penelitian mungkin dapat diperdalam ke arah kajian strategis dari kebijakan keamanan yang diambil oleh suatu negara. Sebagaimana yang diketahui, ancaman siber semakin meningkatkan kekhawatiran negara sama seperti ancaman konvensional yang sudah dikaji sebelumnya. Khususnya, tentang strategi apa yang hendak dicapai oleh UEA dalam penggunaan operasi siber ofensifnya.

Daftar Pustaka

Buku

Avant, Deborah D., *The Market for Force: The Consequences of Privatizing Security* (Cambridge: Cambridge University Press, 2015), hal 21-26

Bryman, Alan, *Social Research Methods*, 4th ed. (Oxford: Oxford University Press, 2015), 543-563

Buzan, Barry, Ole Wæver, dan Jaap de Wilde, *Security: A New Framework for Analysis* (London: Lynn Rienner Publishers, 1998).

Ellis, Ryan dan Vivek K. Mohan, *Rewired: Cybersecurity Governance* (Hoboken, NJ: John Wiley & Sons, Inc., 2019).

Henderson, Scott J., *The Dark Visitor: Inside the World of Chinese Hackers*, 2007.

Matthiesen, Toby. *Sectarian Gulf: Bahrain, Saudi Arabia, and the Arab Spring That Wasn't*. Stanford briefs, Stanford Univ. Press, 2013.

Maurer, Tim, *Cyber Mercenaries the State, Hackers, and Power* (Cambridge University Press, 2018).

Dokumen Negara

TRA UAE, Annual Report 2009, https://www.tdra.gov.ae/assets/oKffXSHe.pdf.aspx

TRA UAE, Annual Report 2012, https://www.tdra.gov.ae/assets/BUi9w2ng.pdf.aspx

TRA UAE, National Cyber Security Strategy (NCSS) 2019, https://u.ae/en/about-the-uae/strategies-initiatives-and-awards/federal-governments-strategies-and-plans/national-cybersecurity-strategy-2019

US Departement of Justice, “Three Former U.S. Intelligence Community and Military Personnel Agree to Pay More than $1.68 Million to Resolve Criminal Charges Arising from Their Provision of Hacking-Related Services to a Foreign Government,” The United States Department of Justice, 14 September 2021, https://www.justice.gov/opa/pr/three-former-us-intelligence-community-and-military-personnel-agree-pay-more-168-million.

Jurnal atau Artikel Akademik

Bronk, Christopher dan Eneken Tikk-Ringas, “The Cyber Attack on Saudi Aramco,” *Survival* 55, no. 2 (Maret 2013): hal. 81-96, https://doi.org/10.1080/00396338.2013.784468.

Chandra, Geetanjali Ramesh, Bhoopesh Kumar Sharma, dan Iman Ali Liaqat, “UAE‘s Strategy towards Most Cyber Resilient Nation,” *International Journal of Innovative Technology and Exploring Engineering* 8, no. 12 (October 2019): hal. 2803-2809, https://doi.org/10.35940/ijitee.l3022.1081219.

da Cruz, José de Arimatéia dan Stephanie Pedron. “Cyber Mercenaries: A New Threat to National Security,” *International Social Science Review* 96, no. 2 (Juni 2020), https://digitalcommons.northgeorgia.edu/cgi/viewcontent.cgi?article=1454&context=issr.

Echagüe, Ana, dan Jane Kinninmont. “Citizenship in the Gulf.” Essay. In *The Gulf States and Arab Uprisings*, Madrid, Spain: FRIDE, 2013.

Ellis, James. “Chinese Cyber Espionage: A Complementary Method to Aid PLA Modernization.” Tesis, (NPS, 2015), https://apps.dtic.mil/sti/pdfs/ADA632209.pdf

Floyd, Rita, “Extraordinary or Ordinary Emergency Measures: What, and Who, Defines the ‘Success’ of Securitization?,” *Cambridge Review of International Affairs* 29, no. 2 (2015): hal. 677-694, https://doi.org/10.1080/09557571.2015.1077651.

Foley, Sean. “The UAE: Political Issues and Security Dilemmas.” *Middle East Review of International Affairs* 3, no. 1 (Maret 1999). https://www.seanfoley.org/wp-content/uploads/2012/03/uae_politics_and_security_dilemas.pdf.

Forstenlechner, Ingo, Emilie Rutledge, dan Rashed Salem Alnuaimi. “The UAE, the ‘Arab Spring’ and Different Types of Dissent.” *Middle East Policy* 19, no. 4 (2012): 54–67. https://doi.org/10.1111/j.1475-4967.2012.00559.x.

Gibbs, Tanya “Seeking Economic Cyber Security: A Middle Eastern Example,” *Journal of Money Laundering Control* 23, no. 2 (April 2020): hal. 493-507, https://doi.org/10.1108/jmlc-09-2019-0076

Hemsley, Kevin dan Ronald Fisher, “A History of Cyber Incidents and Threats Involving Industrial Control Systems,” *Critical Infrastructure Protection XII*, 2018, hal. 215-242, https://doi.org/10.1007/978-3-030-04537-1_12.

Leeson, Peter T., dan Ennio E Piano, “The Golden Age of Mercenaries,” *European Review of Economic History* 25, no. 3 (2020): hal. 429-446, https://doi.org/10.1093/ereh/heaa020.

Lindsay, Jon R.. “Stuxnet and the Limits of Cyber Warfare,” *Security Studies* 22, no. 3 (2013): hal. 365-404, DOI: https://doi.org/10.1080/09636412.2013.816122.

Lynch, Marc, “Digital Activism and Authoritarian Adaptation in the Middle East,” *Digital Activism and Authoritarian Adaptation in the Middle East - POMEPS Studies* 43 (2021): hal. 4-7, https://pomeps.org/digital-activism-and-authoritarian-adaptation-in-the-middle-east.

Mahoney, Charles W. “Corporate Hackers: Outsourcing US Cyber Capabilities,” *Strategic Studies Quarterly* 15, no. 1 (1 April 2021): hal. 61-89, https://www.jstor.org/stable/26984768.

Mawgoud, Ahmed A. et al., “Cyber Security Risks in MENA Region: Threats, Challenges and Countermeasures,” *Advances in Intelligent Systems and Computing*, Februari 2019, hal. 912-921, https://doi.org/10.1007/978-3-030-31129-2_83.

McMurdo, Jesse, “Cybersecurity Firms Cyber Mercenaries?,” *SSRN Electronic Journal*, 12 Desember 2014, https://doi.org/10.2139/ssrn.2556412.

Pauwels, Eleonore dan Sarah W. Deton, “Hybrid Emerging Threats and Information Warfare: The Story of the Cyber-AI Deception Machine,” *21st Century Prometheus*, 2020, hal. 107-124, https://doi.org/10.1007/978-3-030-28285-1_6.

Petterson, Jason P. dan Matthew N. Smith, “Developing a Reliable Methodology for Assessing the Computer Network Operations Threat of Iran,” Master Tesis, (NPS, September 2005), https://fas.org/irp/eprint/cno-iran.pdf

Pöpper, Christina, Michail Maniatakos, dan Roberto Di Pietro, “Cyber Security Research in the Arab Region,” *Communications of the ACM* 64, no. 4 (2021): hal. 96-101, https://doi.org/10.1145/3447741.

Ragab, Eman, “Beyond Money and Diplomacy: Regional Policies of Saudi Arabia and UAE after the Arab Spring,” *Foreign Relations of the GCC Countries*, Juli 2018, hal. 37-53, https://doi.org/10.4324/9780203701287-4.

Rose, Lena Andrea, “Bridging the Realms Between Cyber and Physical: Approaching Cyberspace with an Interdisciplinary Lens.” (Fordham Research Commons, 2020), 25, https://research.library.fordham.edu/international_senior/80/.

Rugh, William A., “The Foreign Policy of the United Arab Emirates,” *Middle East Journal* 50, no. 1 (1996): hal. 55-70, https://www.jstor.org/stable/4328896.

Salisbury, Peter. “Risk Perception and Appetite in UAE Foreign and National Security Policy.” *Middle East and North Africa Programme*, Juli 2020. https://www.chathamhouse.org/sites/default/files/2020-07-01-risk-in-uae-salisbury.pdf.

Shires, James, “Hack-and-Leak Operations: Intrusion and Influence in the Gulf,” *Journal of Cyber Policy* 4, no. 2 (2019): hal. 235-256, DOI: https://doi.org/10.1080/23738871.2019.1636108

Shires, James, “The Cyber Operation Against Qatar News Agency,” *Gulf Studies*, October 2020, hal. 101-113, https://doi.org/10.1007/978-981-15-8735-1_6.

Smith, Troy E., “The Specter of Cyber in the Service of the Islamic State,” *American Intelligence Journal* 34, no. 1 (2017): hal. 54-58, https://www.jstor.org/stable/26497117.

Whyte, Christopher, “Cyber Conflict or Democracy ‘Hacked’? How Cyber Operations Enhance Information Warfare,” *Journal of Cybersecurity* 6, no. 1 (Januari 2020), https://doi.org/10.1093/cybsec/tyaa013.

Sumber Web

Aboul-Enein, Sameh, “Cybersecurity Challenges in the Middle East,” Geneva Centre for Security Policy (GCSP), 19 April 2017, https://www.gcsp.ch/publications/cybersecurity-challenges-middle-east.

Ayman, Adly “Qatar Presents Proof of UAE Role in QNA Website Hacking,” Gulf Times, 20 Juli 2017, https://www.gulf-times.com/story/557315/Qatar-presents-proof-of-UAE-role-in-QNA-website-ha.

Bell, Jennifer, “UAE Companies 'Wide Open' to Cyber Attacks Due to Lack of Staff Training,” The National (The National, 16 Juni 2021), https://www.thenationalnews.com/business/technology/uae-companies-wide-open-to-cyber-attacks-due-to-lack-of-staff-training-1.220114.

Bensaid, Adam. “The UAE’s Covert Web of Spies, Hackers and Mercenary Death Squads.” TRT World, 5 Februari 2019. https://www.trtworld.com/magazine/the-uae-s-covert-web-of-spies-hackers-and-mercenary-death-squads-23805.

Bing, Christopher dan Joel Schectman, “Special Report: Inside the UAE's Secret Hacking Team of U.S. Mercenaries,” Reuters (Thomson Reuters, 30 Januari 2019), https://www.reuters.com/article/us-usa-spying-raven-specialreport-idUSKCN1PO19O.

Davidson, Christopher M. “The Making of a Police State.” Foreign Policy, April 14, 2011. https://foreignpolicy.com/2011/04/14/the-making-of-a-police-state-2/.

DeYoung, Karen dan Ellen Nakashima, “UAE Orchestrated Hacking of Qatari Government Sites, Sparking Regional Upheaval, According to U.S. Intelligence Officials,” The Washington Post (WP Company, 16 Juli 2017), https://www.washingtonpost.com/world/national-security/uae-hacked-qatari-government-sites-sparking-regional-upheaval-according-to-us-intelligence-officials/2017/07/16/00c46e54-698f-11e7-8eb5-cbccc2e7bfbf_story.html?utm_term=.6952ff7c3e5b.

“Ex-U.S. Intel Operatives Admit Hacking American Networks for UAE.” euronews, 15 September 2021. https://www.euronews.com/next/2021/09/14/us-usa-cyber-raven.

Fang, Lee, “Why Did the Firm That Sold Spyware to the UAE Win a Special Export License from State Department?,” The Intercept, 7 Juli 2015, https://theintercept.com/2015/07/07/baltimore-firm-supplying-united-arab-emirates-surveillance-software-won-special-export-license-state-department/.

Finkle, Jim, “Exclusive: Insiders Suspected in Saudi Cyber Attack,” Reuters (Thomson Reuters, 7 September 2012), https://www.reuters.com/article/net-us-saudi-aramco-hack-idUSBRE8860CR20120907.

Gambrell, Jon, “UAE Cyber Firm Darkmatter Slowly Steps out of the Shadows,” Phys.org, 1 Februari 2018, https://phys.org/news/2018-02-uae-cyber-firm-darkmatter-slowly.html.

Hasbini, Mohamad Amin, “The Rise of Cybercrime in Dubai and UAE,” Securelist English Global. Kaspersky, 23 Juni 2014, https://securelist.com/the-rise-of-cybercrime-in-dubai-and-uae/63682/.

“Hybrid Warfare Poses a Serious Threat to National Security, Say Defence Experts.” Crown Prince Court, 6 Juni 2018. https://www.cpc.gov.ae/en-us/thecrownprince/Majlis/Pages/PressRelease_Details.aspx?press_Id=73.

“INEGMA: UAE Leaders Have Worked on Building National Defense 1st Add,” WAM, 14 Desember 2014, https://www.wam.ae/en/details/1395273791751.

Jones, Seth G., “War by Proxy: Iran's Growing Footprint in the Middle East,” Center for Strategic and International Studies (CSIS), 20 Oktober 2021, https://www.csis.org/war-by-proxy.

Marczak, Bill dan John Scott-Railton, “The Million Dollar Dissident: NSO Group's Iphone Zero-Days Used against a UAE Human Rights Defender,” The Citizen Lab, 23 Juni 2020, https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/.

McLaughlin, Jenna, “Deep Pockets, Deep Cover,” Foreign Policy, 21 Desember 2017, https://foreignpolicy.com/2017/12/21/deep-pockets-deep-cover-the-uae-is-paying-ex-cia-officers-to-build-a-spy-empire-in-the-gulf/.

Odell, Joe. “How the UAE's pro-Democracy Movement Fell into a Death Spiral.” Middle East Eye, 2 April 2018. https://www.middleeasteye.net/opinion/how-uaes-pro-democracy-movement-fell-death-spiral.

“Qatar Crisis: UAE Denies Hacking News Agency,” BBC News (BBC, 17 Juli 2017), https://www.bbc.com/news/world-middle-east-40630602.

Reuters Dubai, “UAE Woman Executed over Killing of American Teacher in Abu Dhabi,” The Guardian (Guardian News and Media, 13 Juli 2015), https://www.theguardian.com/world/2015/jul/13/uae-woman-executed-over-killing-of-american-teacher-in-abu-dhabi.

Sami Zaatari, “UAE's Strategy to Counter Cyber Terrorism Can Be a Model for Others,” Government – Gulf News (Gulf News, 31 Oktober 2018), https://gulfnews.com/uae/government/uaes-strategy-to-counter-cyber-terrorism-can-be-a-model-for-others-1.2028229.

Salisbury, Peter, “The Untold, inside Story of the First Hack to Nearly Start a War,” Quartz (Quartz, 20 Oktober 2017), https://qz.com/1107023/the-inside-story-of-the-hack-that-nearly-started-another-middle-east-war/.

Sarvy Geranpayeh dan Sami Zaatari, “5% Of Global Cyber Attacks Targeted UAE Last Year,” Crime – Gulf News (Gulf News, 31 Oktober 2018), https://gulfnews.com/uae/crime/5-of-global-cyber-attacks-targeted-uae-last-year-1.2027770.

Sharma, Alkesh, “UAE's Federal Entities Witness 11% Jump in Cyber Attack Attempts in March,” The National (The National, 4 Juli 2021), https://www.thenationalnews.com/business/technology/uae-s-federal-entities-witness-11-jump-in-cyber-attack-attempts-in-march-1.1003042.

“Six Arrested over $45 Million Cyber Heist on Middle East Banks,” Al Arabiya English (Reuters, 20 Mei 2020), https://english.alarabiya.net/business/banking-and-finance/2013/11/19/Six-arrested-over-45-million-cyber-heist-on-Middle-East-banks.\

Staff Report, “UAE, Kuwait Most Vulnerable for Cyberattacks in the Gulf,” Technology – Gulf News (Gulf News, 7 November 2018), https://gulfnews.com/technology/uae-kuwait-most-vulnerable-for-cyberattacks-in-the-gulf-1.2241327.

Staff Report. “UAE Upgrades Cyber Security across 35 Federal Bodies.” Government – Gulf News. Gulf News, 28 Oktober 2018. https://gulfnews.com/uae/government/uae-upgrades-cyber-security-across-35-federal-bodies-1.2072921.

“UAE National Electronic Security Authority Introduces New Strategies, Policies and Standards,” WAM, 5 April 2021, http://wam.ae/en/details/1395267081900.

“US Charges American Mercenary Hackers over Their Work in UAE.” The Guardian. Guardian News and Media, 14 September 2021. https://www.theguardian.com/us-news/2021/sep/14/hacking-spying-charges-united-arab-emirates-us-intelligence.

WAM Team, “مجلس الأمن السيبراني يعقد اجتماعه الأول ‘عن بعد’,” WAM, 28 Januari 2021, http://wam.ae/ar/details/1395302905117.

Ziv, Amitai. “Mysterious UAE Cyber Firm Luring Ex-Israeli Intel Officers with Astronomical Salaries.” Haaretz.com. Haaretz, 16 Oktober 2019. https://www.haaretz.com/israel-news/.premium-mysterious-uae-cyber-firm-luring-ex-israeli-intel-officers-with-astronomical-salaries-1.7991274.