**Universitas Katolik Parahyangan**
**Fakultas Ilmu Sosial dan Ilmu Politik**
**Program Studi Ilmu Hubungan Internasional**

*Terakreditasi A*
*SK BAN-PT NO:3095/SK/BAN-PT/Akred/S/VIII/2019*

# Analisis Penggunaan *Cyber Mercenaries* dalam Project Raven di Uni Emirat Arab (UEA)

Skripsi

Oleh
Kevin Izzan Adhitya Pratama
6091801023

Bandung
2021

**Universitas Katolik Parahyangan**

**Fakultas Ilmu Sosial dan Ilmu Politik**

**Program Studi Ilmu Hubungan Internasional**

*Terakreditasi A*

*SK BAN-PT NO:3095/SK/BAN-PT/Akred/S/VIII/2019*

# Analisis Penggunaan *Cyber Mercenaries* dalam Project Raven di Uni Emirat Arab (UEA)

Skripsi

Oleh
Kevin Izzan Adhitya Pratama
6091801023

Pembimbing
Idil Syawfi, S.IP., M.Si.

Bandung
2021

Fakultas Ilmu Sosial dan Ilmu Politik
Jurusan Hubungan Internasional
Program Studi Ilmu Hubungan Internasional

## Tanda Pengesahan Skripsi

Nama : Kevin Izzan Adhitya Pratama
Nomor Pokok : 6091801023
Judul : Analisis Penggunaan *Cyber Mercenaries* dalam Project Raven di Uni Emirat Arab

Telah diuji dalam Ujian Sidang jenjang Sarjana
Pada Rabu, 11 Januari 2022
Dan dinyatakan **LULUS**

**Tim Penguji**
**Ketua sidang merangkap anggota**
Vrameswari Omega W., S.IP., M.Si. (Han) : _____

**Sekretaris**
Idil Syawfi, S.IP., M.Si : _____

**Anggota**
Putu Agung Nara Indra, S.IP.,M.Sc. : _____

Mengesahkan,
Dekan Fakultas Ilmu Sosial dan Ilmu Politik

Dr. Pius Sugeng Prasetyo, M.Si

## Lembar Pernyataan

Saya yang bertandatangan dibawah ini :

| | |
|---|---|
| Nama | : Kevin Izzan Adhitya Pratama |
| NPM | : 6091801023 |
| Program Studi | : Ilmu Hubungan Internasional |
| Judul | : Analisis Penggunaan *Cyber Mercenaries* dalam Project Raven Uni Emirat Arab (UEA) |

Dengan ini menyatakan bahwa skripsi ini merupakan hasil karya tulis ilmiah sendiri dan bukanlah merupakan karya yang pernah diajukan untuk memperoleh gelar akademik oleh pihak lain. Adapun karya atau pendapat lain yang dikutip, ditulis sesuai dengan kaidah penulisan ilmiah yang berlaku.

Pernyataan ini saya buat dengan penuh tanggung jawab dan bersedia menerima konsekuensi apapaun sesuai aturan yang berlaku apabila dikemudian hari diketahui bahwa pernyataan ini tidak benar.

Bandung, 3 Januari 2022


Kevin Izzan Adhitya Pratama

# ABSTRAK


Nama : Kevin Izzan Adhitya Pratama
NPM : 6091801023

Judul : Analisis Penggunaan *Cyber Mercenaries* dalam Project Raven di Uni Emirat Arab (UEA)

---


Penelitian ini bertujuan untuk menunjukkan meningkatnya peranan teknologi informasi dan komunikasi (ICT) dalam konstelasi politik dan keamanan internasional. Lebih dalamnya, penelitian ini akan berfokus pada topik pengembangan keamanan siber UEA melalui Project Raven dalam kurun waktu 2009-2019. Fenomena ini dapat dianggap unik karena di dalamnya dapat diklasifikasikan sebagai penggunaan *cyber mercenaries*, yakni terlibatnya kontraktor asing dan dukungan finansial yang kuat dari aktor negara terkait. Penelitian dilakukan dengan metode analisis data kualitatif dengan pendekatan *analytic induction*. Sedangkan untuk kerangka pemikiran, penelitian ini menggunakan paham *"extraordinary emergency measures"* dari Rita Floyd yang berakar dari teori Sekuritisasi. Dalam kasus Project Raven, penelitian ini menemukan bahwa UEA terpaksa untuk menggunakan kontraktor swasta karena sifat dari keamanan siber itu sendiri. Pendekatan ini berbeda dengan negara lain seperti AS dan Iran yang menggunakan divisi militer atau badan resmi. Oleh karena itu, pertanyaan yang dapat diajukan adalah mengapa UEA menggunakan *cyber mercenaries* dalam merespons ancaman sibernya?



**Kata Kunci:** Keamanan Siber, Project Raven, UEA, Kawasan Teluk, Kapabilitas Siber Ofensif, Arab Spring, Serangan Siber Qatar 2017.

## *ABSTRACT*

Name : Kevin Izzan Adhitya Pratama
Student Number : 6091801023
Title : Analysis on the Use of Cyber Mercenaries on Project Raven in the United Arab Emirates (UAE)

---

*This research aims to locate the role of information and communication technology (ICT) inside international security and politics constellation. Specifically, this research explores the development of cybersecurity in UAE through the case of Project Raven from 2009-2019 period. The phenomenon was unique because it could be classified as a use of cyber mercenaries through its distinct characteristics i.e., the involvement of foreign contractors and financial backing. The research would be conducted via qualitative data analysis and analytic induction method. Moreover, this research utilizes Rita Floyd's revision on Securitization Theory called "extraordinary emergency measures" theoretical framework. Under this framework, state actor can take policies that are exceptional or outside their legal framework. In the case of Project Raven, due to the nature of cybersecurity realm, UAE are forced to outsource their operations to private contractors. This is different to other countries approach, which is to develop military and governmental institutions to tackle incoming cyber threats such as US and Iran. Thus, this paper aims to delve deeper on to this topic on why states use cyber mercenaries?*



***Keywords:*** *Cybersecurity, Project Raven, UAE, Gulf region, Offensive Cyber Capabilities, Arab Spring, Qatar Cyber Attack 2017.*

## Kata Pengantar

Puji dan syukur saya panjatkan kepada Allah SWT, atas berkat dan rahmatnya saya bisa menyelesaikan skripsi yang berjudul Analisis Penggunaan *Cyber Mercenaries* dalam *Project Raven* di Uni Emirat Arab. Skripsi ini utamanya diajukan untuk memenuhi ujian sidang jenjang sarjana Program Studi Ilmu Hubungan Internasional Fakultas Ilmu Sosial dan Ilmu Politik Universitas Katolik Parahyangan. Selain itu, skripsi ini ingin memaparkan tentang isu keamanan siber dalam konstelasi politik dan keamanan internasional di Uni Emirat Arab (UEA) dan kawasan Teluk Timur Tengah. Harapannya, skripsi ini dapat menyumbang pemahaman terbaru tentang peranan teknologi siber dalam studi hubungan internasional. Tidak hanya itu, penulis juga berharap atas masukan dari pembaca untuk dapat menyempurnakan penelitian berikutnya. Khususnya terkait dengan studi Project Raven atau keamanan siber secara keseluruhan.

Akhir kata, penulis mengucapkan terima kasih kepada seluruh pihak yang terlibat dalam penulisan skripsi ini.

Bandung, 22 Desember 2021

Kevin Izzan Adhitya Pratama

## Ucapan Terima Kasih

Terima kasih pertama saya ucapkan kepada Allah SWT, karena tanpa kehadiran-Nya tidak akan mungkin saya mampu untuk menuntaskan skripsi ini dengan tepat waktu. Tidak lupa juga saya ucapkan terima kasih tak terhingga kepada kedua orang tua yakni Kartika Herawati dan Irwan Budhi Setiawan atas kasih sayang dan bimbingannya telah membuat saya mampu berada di akhir studi sarjana. Kepada adik saya Azrian Rifqi Radhitya juga saya ucapkan terima kasih atas dorongannya untuk selalu mengingatkan untuk menyelesaikan skripsi sebelum tenggat waktu berakhir. Keluarga besar yang tidak ada hentinya mendoakan kelancaran skripsi pun tak lupa untuk saya berikan apresiasi dan terima kasih. Kepada pembimbing Mas Idil Syawfi juga saya ucapkan terima kasih sebesar-besarnya atas didikan dan bimbingannya.

Ucapan selanjutnya saya dedikasikan kepada seluruh jajaran teman kuliah selama empat tahun terakhir mulai dari Prosper Nosa saya membuat catatan perkuliahan, tanpa dia saya tidak akan mampu menyintas di semester-semester awal. Kepada barisan ambisius Sandy Ilmi, Rizki Kurniawan, dkk saya haturkan terima kasih atas semangatnya yang membuat saya ikut ambis juga di paruh awal kuliah. Sedangkan kepada jajaran Coop Space yang bau rokoknya hampir membuat saya semaput juga saya haturkan terima kasih atas kehadirannya yang selalu setia menemani saya ketika pulang ke rumah tidak dapat menjadi pilihan. Kepada teman-teman yang saya tidak menyangka akan menjadi pendamping di akhir-akhir kuliah seperti Mas Ben Manik, Audre Augurius, Archangela Rachel Dharmaputri, Juan Wangsadiputra, Rassya Mahesa Axagoras, Ruby Adrian, Hanssel Kamajaya, semuanya saya haturkan terima kasih bumi dan langit. Tanpa mereka

semua, sulit bagi saya untuk dapat menjalani penghujung kuliah dengan aman, damai, tentram, dan sentosa.

Terakhir saya dedikasikan untuk organisasi penampung saya yang selalu beban yakni Warta Himahi (WH) dan beberapa acara lainnya. Terima kasih pertama saya ucapkan untuk WH, khususnya ibu kordiv tercinta Alya Diva serta jajaran staf Thalista, Zahra, Nata, dan Chrisa. Doa terbaik kuucapkan untuk kalian semua. Sedangkan untuk TAHI 2018, GINTRE 2019, BMUN 2019, AIESEC in Bandung, Gang Bengkel, Lab Coffee, Kurokoffee, dan Aerox ku, serta semua tempat, momen, waktu, dan suasana yang saya tidak dapat ucapkan satu per satu, saya ucapkan terima kasih untuk empat tahun terakhir. Kalian semua sangat bermakna bagi petualangan hidup saya. Panjang umur terus hal-hal yang baik. Aamiin yaa rabbal alamin.

**Daftar Isi**

## Daftar Gambar

## Daftar Singkatan

CSJ : Cutting Sword of Justice

DDOS : *Distributed Denial-Of-Sevice*

GCI : *Global Cybersecurity Index*

GDS : Gharargah-E Defa-E Saiberi

ICT : *Information And Communication Technology*

IM : Ikhwanul Muslimin

ITAR : *International Traffic in Arms Regulation*

ITU : International Telecommunications Union

MbZ : Mohammed bin Zayed al Nahyan

NCSS : *National Cyber Security Strategy*

NESA : National Electronic Security Agency

NRI : *Network Readiness Index*

NSA : National Security Agency

PCSFs : *Private Cyber Security Forces*

PMCs : *Private Military Contractors*

PSF : Peninsula Shield Force

QNA : Qatar News Agency

RAKBANK : National Bank of Ras Al Khaimah

SIA : Signal Intelligence Agency

SSHGs : *State-Sponsored Hacker Groups*

SWF : *Sovereign Wealth Fund*

TDRA : Telecommunications and Digital Government Regulatory Authority

TRA : Telecommunication Regulatory Authority

UAE : *United Arab Emirates*

UEA : Uni Emirat Arab

# Bab I

# Pendahuluan

## 1.1. Latar Belakang Masalah

Uni Emirat Arab (UEA) merupakan negara yang mengalami transformasi cukup besar. Berawal dari negara kecil penghasil minyak, kini UEA merupakan negara dengan mayoritas penduduknya memiliki wawasan dan penggunaan teknologi informasi dan komunikasi (ICT) tinggi, di mana penetrasi internet telah mencapai 100% pada tahun 2020.[1] Selain itu, Pemerintah UEA juga giat dalam melakukan digitalisasi layanan pemerintahan di berbagai sektor seperti program *smart cities, UAE e-Government*, serta pembuatan strategi dan regulasi terkait pengembangan teknologi siber nasional. Dampaknya, UEA menjadi negara di kawasan Teluk Timur Tengah dengan perkembangan ICT yang sangat pesat.[2]

Kendati begitu, seiring dengan berkembangnya teknologi ICT di masyarakat terjadi juga peningkatan ancaman siber. Terdapat banyak kekurangan jumlah tenaga siber di instansi pemerintah serta perusahaan asal UEA. Sehingga hal ini membuat UEA menjadi salah satu target utama serangan siber di kawasan Teluk Timur Tengah, terutama yang terkait dengan infrastruktur digital di sektor finansial dan industri minyak bumi.[3]

---

[1] Christina Pöpper, Michail Maniatakos, dan Roberto Di Pietro, "Cyber Security Research in the Arab Region," *Communications of the ACM* 64, no. 4 (2021): pp. 96-101, https://doi.org/10.1145/3447741.
[2] Geetanjali Ramesh Chandra, 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.
[3] *Ibid.*

Salah satu insiden utama yang menimpa UEA terjadi dalam rentang tahun 2012-2014 di mana 19 laman resmi pemerintah serta jaringan *National Bank of Ras Al-Khaimah* (RAKBANK) diretas.[4] Menurut data *Telecommuncations Regulatory Authority* (TRA) UEA, rata-rata kerugian yang dialami oleh negara ini akibat dari serangan siber mencapai 5,9 juta dolar AS pada tahun 2019.[5]

Secara politik, UEA juga menghadapi rival kawasan Iran yang sama-sama sedang meningkatkan keamanan sibernya. Iran sendiri juga memiliki ancaman siber dengan insiden utama terjadi pada tahun 2010 ketika *malware* Stuxnet menyerang reaktor nuklir Natanz memperlambat perkembangan program nuklir Iran selama beberapa tahun.[6] Kerugian Iran mendorong mereka untuk membangun unit pertahanan siber militer yakni Gharargah-e Defa-e Saiberi (GDS) pada November 2010. Komando ini bekerja sebagai sub-divisi militer Iran. Kedigdayaan Iran ini juga berdampak pada meningkatnya serangan siber kawasan ditandai dengan adanya virus Shamoon yang menyerang data serta produksi perusahaan energi Aramco (Arab Saudi) dan Ras Gas (Qatar) pada tahun 2012.[7] Akibat dari adanya serangan tersebut, UEA meningkatkan pertahanan sibernya dengan mendirikan National Electronic Security Agency (NESA) tahun 2014 dan membuat *National Cyber Security Strategy* (NCSS) tahun 2019. Langkah yang diambil

[4] Tanya Gibbs, "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
[5] Alkesh Sharma, "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.
[6] Jon R. Lindsay, "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.
[7] Pöpper, Maniatakos, dan Di Pietro, "Cyber Security Research in the Arab Region."

ini menunjukkan bahwa keamanan siber merupakan isu yang penting untuk diperhatikan oleh UEA.

## 1.2. Identifikasi Masalah

### 1.2.1. Deskripsi Masalah

Dalam menghadapi ancaman di atas UEA meningkatkan kapabilitas siber ofensifnya dengan merekrut ahli siber bekas eks-intel National Security Agency (NSA) AS ke dalam proyek rahasia yang bernama Raven. Bekas ahli siber NSA yang bekerja di Raven ini terafiliasi dengan kontraktor keamanan siber bernama Cyberpoint asal AS. Proyek ini dapat dikategorikan sebagai *cyber mercenaries* karena ciri khasnya sesuai yakni, tenaga kerja yang tidak berafiliasi dengan negara yang dibayar tinggi sebesar 200.000-400.00 dolar AS oleh pemerintah UEA sebagai pelaksana proyek melalui dana *sovereign wealth fund* (SWF) nya yakni Mubadala ICT.[8] Tenaga siber asing ini ditugaskan untuk mengembangkan keahlian staf Emirat dalam operasi siber defensif dan ofensif. Utamanya mereka dapat melakukan peretasan serta pengintaian siber menggunakan alat intrusi yang bernama Karma dan Pegasus.[9] Alat yang diperoleh dari perusahaan NSO Group ini mampu memenetrasi gawai sasaran dan mengendalikannya

[8] Christopher Bing 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.
[9] Eleonore Pauwels 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.

baik untuk mendapatkan informasi pengguna atau untuk menyimpan informasi palsu sesuai keinginan klien.[10]

Langkah UEA ini menarik karena berbeda dibandingkan negara lain di kawasan Timur Tengah. Ketika negara Teluk lain berfokus pada pengembangan keamanan siber nasional secara resmi, UEA justru memilih menggunakan tenaga alih daya atau dapat dikatakan sebagai *cyber mercenaries* dalam pengembangan kapabilitas sibernya. Selain itu, *cyber mercenaries* UEA ini diarahkan kepada kapabilitas ofensif alih-alih diarahkan kepada kapabilitas defensif. Hal ini menunjukkan bahwa terdapat pasar menarik bagi tenaga keamanan siber swasta yang dapat mengurangi monopoli kekuatan negara.

Project Raven dibentuk karena memiliki urgensi untuk mengatasi ancaman siber yang sebelumnya terjadi pada UEA. Hal ini mencakup beberapa insiden siber terhadap pergerakan oposisi UAE-5 secara daring tahun 2011, serangan data terhadap RAKBANK 2012, hingga insiden jaringan siber ISIS yang menyebabkan terbunuhnya WNA di Abu Dhabi 2014. Insiden yang secara khusus mulai menyasar status-quo pemerintahan adalah ancaman yang dianggap eksistensial bagi elite politik yang mengambil keputusan di UEA. Hal ini ditandai sejak adanya insiden UAE-5, pemerintah mulai mengembangkan badan intelijen siber NESA dan menggelontorkan dana untuk pengembangan infrastruktur dan SDM keamanan siber.[11]

[10] Bill Marczak and 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/.
[11] 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

Namun, keterlibatan Raven yang paling kentara terlihat dalam serangan siber terhadap kanal media Qatar News Agency (QNA) pada Mei 2017 di mana operasi mereka semakin ofensif. Laporan paling awal ditemukan pada Juli 2017 bahwa UEA mempersiapkan rencana operasi terhadap QNA.[12] Serangan siber ini bertujuan untuk menyebarkan disinformasi terkait posisi Emir Qatar yang mendukung Iran dan Ikhwanul Muslimin. Disinformasi ini menciptakan permusuhan antara blok GCC pimpinan UEA dan Arab Saudi dengan Qatar yang berakhir dengan blokade selama dua tahun. Project Raven UEA dikatakan terlibat karena alamat IP pelaku terdeteksi oleh otoritas Qatar setelah investigasi pada April 2018.[13] Dampaknya peranan *cyber mercenaries* UEA tersebut menjadi isu lintas batas negara yang hendak diangkat oleh penelitian ini.

### 1.2.2. Pembatasan Masalah

Penelitian ini dibatasi dalam kurun waktu 2009-2019. Periode ini diambil dari mula dibentuknya Project Raven hingga terjadinya serangan kantor berita QNA pada Mei 2017 dan dampak terhadap jalannya krisis diplomatik yang terjadi setelahnya. Selain itu, aktor yang dibahas dibatasi dalam negara UEA berserta program atau badan turunannya yang terkait langsung dengan tata kelola pertahanan siber dan aktor non-negara yakni *cyber mercenaries* Project Raven. Hal ini dijabarkan dengan membahas faktor-faktor

[12] Karen DeYoung 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.

[13] James Shires, "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

penyebab UEA mendirikan proyek tersebut terkait ancaman siber dan kepentingan terkait di dalamnya.

### 1.2.3. Perumusan Masalah

Berdasarkan topik dan permasalahan yang telah ditulis di atas, maka rumusan pertanyaan penelitian yang akan digunakan adalah**, mengapa UEA menggunakan *cyber mercenaries* dalam menghadapi ancaman siber mereka?**

## 1.3. Tujuan Dan Kegunaan Penelitian

### 1.3.1. Tujuan Penelitian

Terdapat beberapa tujuan yang hendak dicapai penelitian ini, pertama adalah menjawab pertanyaan penelitian dengan memberikan faktor pendorong dan pendukung dari penggunaan teknologi siber sebagai upaya untuk meningkatkan kapabilitas keamanan siber. Hal ini mencakup pengembangan kapabilitas siber secara ofensif maupun defensif. Khususnya hal ini terkait dengan konsep *cyber mercenaries* serta hubungannya dengan negara. Kedua adalah untuk membantu memahami pengembangan instrumen keamanan UEA dan dampaknya terhadap negara di sub-kawasan Teluk Timur Tengah, khususnya terkait dengan Kuartet Arab.

### 1.3.2. Kegunaan Penelitian

Pertama, penelitian ini bertujuan untuk memenuhi tugas akhir Program Studi Ilmu Hubungan Internasional. Kedua, penelitian ini diharapkan dapat membantu kalangan akademisi dalam riset keamanan siber nasional. Lebih dalamnya, penelitian ini diarahkan

kepada kajian keamanan siber dalam hubungan internasional serta hubungannya dengan konsep keamanan non-tradisional. Selain itu, penelitian ini diharapkan dapat menambah riset terkait pengembangan keamanan siber nasional suatu negara.

### 1.4. Tinjauan Pustaka

Pada umumnya, konsep *cyber mercenaries* dianggap sebagai alternatif dari monopoli kekuatan militer ofensif milik negara. *Mercenaries* sendiri merupakan konsep yang telah lama digunakan oleh dalam ranah hubungan internasional. Niccoló Machiavelli dari zaman Renaisans menganggapnya sebagai tentara asing yang digaji oleh negara untuk melindungi mereka dengan membunuh musuhnya.[14] Dalam kata lain, *mercenaries* berupa aktor non-negara dianggap akademisi sebagai proksi atau perpanjangan tangan dari *beneficiary actor* yang umumnya berupa aktor negara. Menurut Deborah Avant, dengan adanya aktor proksi menguntungkan negara karena mereka tidak perlu untuk mengorbankan sumber daya negara secara massal. Hal ini juga membuat adanya pasar bagi *mercenaries* itu sendiri. Dalam kata lain, *mercenaries* konvensional juga disebut sebagai *private military contractors* (PMCs).[15]

Sedangkan untuk konsep *cyber mercenaries*, ia merujuk pada konsep yang sama namun bergerak pada ruang siber yakni ahli siber yang dibayar klien (dapat berupa negara atau non-negara) untuk melakukan tindakan atas nama dirinya. Namun operasinya sendiri

[14] Peter T Leeson 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.
[15] Deborah D. Avant, *The Market for Force: The Consequences of Privatizing Security* (Cambridge: Cambridge University Press, 2015), hal 21-26.

berbeda dari *mercenaries* tradisional di mana ia lebih beragam, ada yang mengaitkannya dengan perang siber, spionase siber, perang informasi, hingga perang hibrid (gabungan antara perang dalam ruang siber dan ruang konvensional). Jelasnya, tindakan yang dilakukan oleh kelompok individu yang mengancam keamanan siber dapat dikategorikan dalam payung besar operasi siber.[16]

Berdasarkan penelitian yang sudah ada, terdapat dua pendapat utama mengenai alasan negara menggunakan *cyber mercenaries*. Lena Andrea Rose misalnya, meneliti soal Project Raven dan menyimpulkannya sebagai alat penyebar disinformasi dan spionase bagi negara untuk melawan oposisi mereka. Ia menyorot juga faktor kekuatan finansial sebagai pendorong negara untuk melakukan *outsourcing* tenaga keamanan mereka.[17] Namun kunci utama mengapa negara memilih menggunakan *cyber mercenaries* untuk adalah cocoknya ciri khas operasi siber yang anonim serta kecilnya biaya yang dikeluarkan. Dalam konteks Project Raven serta serangan terhadap QNA, Rose melihat UEA berusaha untuk menjaga status-quo di kawasan merupakan alasan utama mengapa mereka menggunakan *cyber mercenaries*.

Sedangkan José de Arimatéia da Cruz dan Stephanie Pedron justru menyorot kurangnya regulasi internasional yang membatasi gerak negara dalam menggunakan

---

[16] Christopher Whyte, "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.

[17] *"In this second case study, I will look at the use of Project Raven in the UAE's hack of the Qatari News Agency. This case study primarily demonstrates how cyber tools are used to spread disinformation and conduct espionage on state adversaries. The UAE hack on Qatar signaled a broader transformation in cyber espionage. It is a clear sign that cyberattacks and disinformation campaigns are no longer the exclusive domain of sophisticated powers."* dikutip dari Lena Andrea Rose, "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/.

*cyber mercenaries* menjadi penyebab kemunculan mereka dalam konteks keamanan internasional.[18] Jesse Jacob McMurdo juga setuju dengan absennya hukum internasional yang membahas tentang penggunaan teknologi siber dan *cyber mercenaries* (istilah yang digunakan McMurdo adalah *private cyber security forces* (PCSFs) atau *state-sponsored hacker groups* (SSHGs)) membuatnya tidak harmoni menimbulkan celah hukum yang dimanfaatkan negara.[19] Perbedaan dari kedua istilah ini menurut McMurdo terletak di besaran peranan yang dimiliki aktor. *Private* artinya sektor bisnis yang memiliki wewenang dan aksi yang lebih besar, sedangkan *State-sponsored* artinya negara yang lebih berwenang dalam penentuan arah operasi siber.

Namun ia menambahkan argumen bahwa sifat ruang siber yang jauh berbeda dari konflik konvensional sebagai pendorong *cyber mercenaries* untuk berkembang. Menurut McMurdo, penghalang masuk dalam perang siber kecil yang kecil membuat negara menggunakan *cyber mercenaries.* Negara hanya membutuhkan, akses internet, serta sumber daya manusia yang memadai. Metodenya pun tidak memakan korban jiwa sehingga biayanya dianggap relatif kecil. Terakhir, McMurdo juga menjelaskan bahwa pertahanan siber terbaik adalah pertahanan ofensif, karena itulah operasi siber yang muncul cenderung bersifat ofensif.

Di luar tiga faktor tersebut, variasi dari penggunaan operasi siber ofensif oleh negara dan proksinya juga berbeda-beda. Perspektif AS misalnya memandang bahwa

[18] José de Arimatéia da Cruz 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.
[19] Jesse McMurdo, "Cybersecurity Firms Cyber Mercenaries?," *SSRN Electronic Journal*, 12 Desember 2014, https://doi.org/10.2139/ssrn.2556412.

operasi siber mencakup segala usaha pertahanan dan sampai batas tertentu mencakup kapabilitas siber ofensif.[20] AS melakukan hal ini dengan menggandeng kontraktor korporasi militer seperti Raytheon dan Northrop Grumman yang memberikan mereka alat dan tenaga ahli di mana mereka menggelontorkan dana yang mencapai 2,6 miliar dolar AS pada 2017.[21] Sedangkan Tiongkok memiliki pendekatan lain atas di mana mereka berangkat dari dukungan pasif dengan membiarkan SSHGs leluasa melakukan operasi siber terhadap negara lain menjadi milisi siber, selama itu berjalan sesuai kepentingannya.[22] Salah kasusnya menimpa ruang siber Indonesia ketika Green Army dan Red Hacker Alliance asal Tiongkok melakukan serangan *Distributed Denial-of-Sevice* (DDoS) dan *Web Defacements* sebagai respons atas diskriminasi ras Tionghoa pada Kerusuhan Mei 1998.[23] Kelompok peretas ini lalu menjadi inspirasi bagi modernisasi PLA dari segi teknologi siber era Hu Jintao. Sedangkan variasi terakhir datang dari Iran, di mana mereka mengetahui adanya aksi kelompok peretas seperti ITSec Team dan Mersad Company yang merugikan industri perbankan di AS pada 2016 yang meliputi CitiGroup, JPMorgan Classic, dan HSBC.[24] Namun, Iran tidak melakukan apa-apa yang membatasi pergerakan kelompok peretas bahkan cenderung membuat kondisi di mana peretasan dapat berkembang seperti pelatihan dan kompetisi alat retas dalam negeri.[25] Tiga variasi ini menunjukkan bahwa tiap negara memiliki pendekatannya

[20] Charles W. Mahoney, "Corporate Hackers: Outsourcing US Cyber Capabilities," *Strategic Studies Quarterly* 15, no. 1 (1 April 2021): hal. 61-89, https://www.jstor.org/stable/26984768.
[21] *Ibid*, hal. 64-67.
[22] James Ellis. "Chinese Cyber Espionage: A Complementary Method to Aid PLA Modernization." Tesis, (NPS, 2015), hal. 50-59, https://apps.dtic.mil/sti/pdfs/ADA632209.pdf
[23] Scott J. Henderson, *The Dark Visitor: Inside the World of Chinese Hackers*, 2007.
[24] Kevin Hemsley 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.
[25] Jason P. Petterson 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

masing-masing terhadap aksi aktor non-negara dan korelasinya terhadap agenda negara dalam ruang siber.

Maka daripada itu, penelitian ini lebih berusaha untuk masuk ke dalam bagaimana proses hubungan antara aktor negara dan non-negara terkait pengembangan kapabilitas siber ofensif. Hal ini juga diperdalam untuk mengetahui varian hubungan apakah yang dimiliki oleh UEA dan Project Raven. Penelitian ini dapat dicapai dengan menggunakan model kerangka pemikiran serta metode kerja dari *cyber mercenaries* ditambah dengan identifikasi faktor independen apa yang dapat mempengaruhi negara untuk menggunakan *cyber mercenaries.*

### 1.5. Kerangka Pemikiran

Penggunaan *cyber mercenaries* oleh negara dapat dikategorikan sebagai bagian dari *extraordinary emergency measures*, yakni kebijakan negara yang terjadi di luar mekanisme resmi atau yang telah ada sebelumnya. Lebih dalamnya, *extraordinary emergency measures* merupakan revisi atas Teori Sekuritisasi dalam Mazhab Kopenhagen, di mana ia mencoba untuk menjawab dua permasalahan terikat dalam proses sekuritisasi. Pertama ia membahas asumsi apakah tingkat keberhasilan sekuritisasi dapat diukur dari seberapa ekstremnya atau luar biasanya tindakan yang diambil negara. Sedangkan yang kedua adalah faktor siapakah yang dapat membuat sekuritisasi dianggap berhasil. Menurut Rita Floyd, ketika negara dalam menghadapi suatu ancaman bersifat darurat terhadap keamanan nasional, mereka dapat mengambil tindakan di luar kebiasaan

mereka.[26] Tindakan ini pun bervariasi tergantung dengan sistem pemerintahan yang berlaku seperti demokrasi atau non-demokrasi.

Pertama, Floyd menggunakan asumsi negara sebagai demokrasi liberal, tindakan luar biasa dapat terjadi dalam tiga situasi yakni 1) apabila hukum atau regulasi baru disahkan, 2) diizinkannya pemerintah untuk menggunakan kuasa darurat (hal ini mengacu pada kondisi di mana upaya yang diambil bertujuan untuk menindak situasi krisis atau ketidakamanan, yang mana semua tindakan diperbolehkan, termasuk di beberapa negara yang harus melalui lembaga yudisial, semua sesuai dengan konteks ancaman yang dihadapi), atau 3) kondisi di mana aparat negara belum pernah menghadapi isu yang baru atau belum pernah ada sebelumnya.[27] Asumsi ini dapat dijadikan sebagai rujukan pertama yang dapat digunakan untuk menganalisis apakah tindakan darurat yang diambil merupakan tindakan wajar atau di luar kebiasaan. Kendati begitu, kini permasalahannya adalah apa yang terjadi apabila negara yang diteliti belum tentu bersifat demokrasi liberal?

Menurut Floyd, mengenai asumsi yang dapat digunakan oleh aktor negara autokrasi (non-demokrasi) hingga aktor non-negara, tindakan yang diambil akan kembali pada pemahaman apa yang masuk akal di kalangan awan terkait ancaman yang hendak diatasi. Hal ini tentu membuat pemikiran diputar kembali bahwasanya ancaman atau objek yang akan disekuritisasi adalah konstruksi sosial aktor yang membuat proses

[26] Rita Floyd, "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.
[27] *Ibid*, hal. 679.

sekuritisasi itu sendiri. Hal ini dijadikan argumen oleh Felix Ciută dan Barry Buzan yakni "*...securitization is radically construtivist in nature,...(thus) security issues are made by acts of securitization*.[28] Sehingga sulit bagi akademisi Mazhab Kopenhagen untuk mendefinisikan apakah semakin luar biasanya tindakan darurat dapat dikategorikan sebagai sekuritsasi yang sukses. Oleh karena itu, menjawab permasalahan pertama Floyd menawarkan tiga faktor analisis yang dapat mengategorikan proses sekuritisasi yang sukses yakni, 1) Identifikasi ancaman menjustifikasikan respons sekuritisasi, yang diikuti oleh; 2) perubahan sikap atau aksi oleh agen terkait (yakni aktor yang menyekuritisasikan atau pihak yang diinstruksikan demikian); serta 3) aksi yang diambil dijustifikasikan oleh pelaku sekuritisasi dengan merujuk pada jenis ancaman yang mereka temukan atau dideklarasikan dalam gerakan sekuritisasi.[29]

Selanjutnya, Floyd membahas tentang beberapa aspek bagi aktor dan relasi antar unit di dalamnya mengatur apakah ini bentuk *extraordinary emergency measures* atau tidak. Aspek pertama adalah adanya tindakan dan perilaku, bukan sekedar bahasa keamanan. Artinya dalam konteks negara, selama mereka yakin dengan tindakan yang diambil itu dapat mengentaskan ancaman di depan mereka, hal ini dapat dikategorikan sebagai keberhasilan sekuritisasi. Kedua adalah *agency* atau lembaga yang memiliki kuasa untuk mengeksekusi tindakan sekuritisasi tersebut. Penting bagi keberhasilan sekuritisasi apabila 'siapa' yang menindak relevan dengan ancaman yang ada. Ketiga

[28] Barry Buzan, Ole Wæver, and Jaap de Wilde, *Security: A New Framework for Analysis* (London: Lynn Rienner Publishers, 1998).
[29] Floyd, "Extraordinary or Ordinary Emergency Measures: What, and Who, Defines the 'Success' of Securitization," hal. 682.

adalah justifikasi dari tindakan yang diambil, yakni tujuan apa yang mau aktor sekuritisasi bawa di dalam *extraordinary emergency measures* tersebut berpengaruh terhadap keberhasilannya itu sendiri.[30]

Terakhir, Floyd memberikan skenario yang dapat terjadi pada *audience* dan proses sekuritisasi yang dilakukan negara. Dari enam skenario yang dipaparkan, terdapat satu skenario yang cocok ciri khas isu keamanan siber. Skenario tersebut adalah apabila negara sebagai pelaku sekuritisasi mengeluarkan *speech act* berupa janji peningkatan keamanan siber bertujuan untuk mengurangi ancaman yang ada di masyarakat, Terdapat dua kemungkinan yakni disetujui, ditolak, atau tidak dapat direspons. Ketiganya akan mendorong aktor untuk melakukan tindakan di luar kebiasaan mereka. Terutama apabila mereka ditolak, tidak direspons, hingga tak mampu memberikan tindakan konkret yang dapat mengentaskan ancaman. Kendati begitu, tujuan Floyd membuat ragam skenario ini adalah menunjukkan bahwa tidak akan akhir konklusif yang artinya negara bebas melakukan tindakan luar biasa selama mereka yakin hal ini sesuai dengan tujuan awal sekuritisasi.[31]

Isu keamanan siber memang merupakan hal yang baru, bahkan di beberapa negara tidak pernah ada yang menghadapinya. Khususnya di negara dengan tingkat interkoneksi jaringan internet tinggi.[32] Sehingga ketika ancaman siber datang negara dapat melakukan sekuritisasi dan mengambil *extraordinary emergency measures* yang belum pernah

[30] *Ibid*, hal. 683-686.
[31] *Ibid*, hal. 686-690.
[32] Ryan Ellis and Vivek K. Mohan, *Rewired: Cybersecurity Governance* (Hoboken, NJ: John Wiley & Sons, Inc., 2019).

diambil seperti membayar tenaga dan keahlian orang asing untuk membantu mereka, terutama apabila tiga skenario di atas terpenuhi. Oleh karena itu, penelitian ini berusaha menjawab pertanyaan penelitian dengan membedah apakah ini merupakan bagian dari *extraordinary emergency measures* negara dalam proses sekuritisasi. Terakhir, penelitian ini juga mencoba untuk mengategorikan kasus *cyber mercenaries* ke dalam jenis skenario Floyd yang sesuai.

### 1.6. Metode Penelitian dan Teknik Pengumpulan Data

Pertama, penelitian ini utamanya menggunakan logika kualitatif di mana fokusnya terletak tulisan dibandingkan dengan angka. Penelitian dengan logika kualitatif yang dilakukan ini lebih berfokus pada realitas sosial serta makna budaya. Tidak hanya itu fokus penelitian ini terletak pada proses interaksi antar aktor dengan peristiwa-peristiwa yang terjadi di dalamnya. Teori yang digunakan pun dianalisis secara terpisah dengan pengumpulan data yang dilakukan. Terakhir penempatan peneliti dalam penelitian logika kualitatif ini menempatkan diri dalam sudut pandang aktor yang hendak diteliti.[33]

Kedua, teknik pengumpulan data yang digunakan adalah studi dokumen. Dokumen yang dimaksud di sini adalah data yang dapat diperoleh secara fisik maupun digital. Kriteria bagi dokumen untuk dapat digunakan dalam penelitian ini adalah otentik, kredibel, representatif, dan bermakna atau relevan dengan topik penelitian. Dokumen yang digunakan dalam penelitian ini mencakup, 1) dokumen resmi negara seperti *press release*, laporan tahunan kementerian atau instansi negara, hingga undang-undang resmi

[33] Alan Bryman, *Social Research Methods*, 4th ed. (Oxford: Oxford University Press, 2015)

negara yang dirilis secara publik, 2) data dari media massa terkait dengan subjek penelitian seperti berita atau *in-depth report*, dan 3) dokumen virtual yang dapat diperoleh dari internet seperti buku, artikel atau jurnal akademik, data statistik. Dokumen yang telah dikumpulkan ini lalu diinterpretasikan dengan pendekatan *content analysis* di mana data dengan tema terkait dicari dan dikelompokkan lalu dicocokan dengan kebutuhan penelitian.[34]

Ketiga, analisis data kualitatif ini lalu dibantu dengan strategi *analytic induction*, di mana penulis mencoba mencari penjelasan universal menggunakan teori yang sudah untuk menemukan jawaban atas pertanyaan penelitian. Langkah yang diambil selanjutnya adalah hipotesis awal dari pertanyaan penelitian diuji dengan data yang telah dikumpulkan. Hal ini dilakukan hingga data dari studi kasus menunjukkan adanya kesamaan atau tidaknya dengan hipotesis yang diajukan di awal. Setelah mendapatkan data tersebut, maka hipotesis akan diformulasikan lagi menjadi hipotesis akhir yang akan menjadi titik akhir pengujian.[35]

## 1.7. SISTEMATIKA PENULISAN

Sistematika penulisan diawali oleh **Bab I**, membahas tentang rancangan penelitian. Bab ini memaparkan latar belakang masalah dan identifikasi masalah, yakni membahas tentang bagaimana posisi UEA dan *Project Raven* dapat terbentuk dan isu apa yang terjadi di dalam kawasan yang memunculkan pertanyaan penelitian. Selanjutnya

[34] *Ibid*, hal. 542-563.
[35] *Ibid*, hal. 566-567.

dibahas pula mengenai perdebatan serta tinjauan pustaka yang sudah terlebih dahulu membahas tentang topik masalah yang diangkat. Hal tersebut lalu diperdalam lagi melalui kerangka pemikiran yang digunakan di dalam penelitian ini. Bab ini lalu ditutup dengan alur sistematika penulisan seperti pembagian bab berserta isi konten yang akan ditulis.

**Bab II** membahas tentang pra-kondisi keamanan siber di UEA yang mendasari adanya Project Raven. Hal ini termasuk ancaman siber UEA serta kekurangan pertahanan siber mereka. Pembahasan disambung dengan program-program resmi UEA terkait pengembangan kapabilitas siber nasional. Laporan *whistleblower* serta dokumen resmi terkait adanya penggunaan *cyber mercenaries* dalam Project Raven juga dipaparkan sebagai argumen utama yang berupaya untuk menjawab pertanyaan penelitian. Bab ini ditutup dengan implikasi singkat aktivitas konkret dari *cyber mercenaries* UEA. **Bab III** membahas teknis *cyber mercenaries* serta analisis klasifikasi *extraordinary* atau *ordinary measures* yang dapat ditemukan dalam Project Raven serta kondisi apa yang membuat negara tertarik untuk menggunakannya. Lebih tepatnya, hipotesis akan dibedah menggunakan teori yang sudah ditulis sebelumnya. Penelitian lalu ditutup dengan **Bab IV** yang berisikan tulisan kesimpulan serta daftar pustaka.