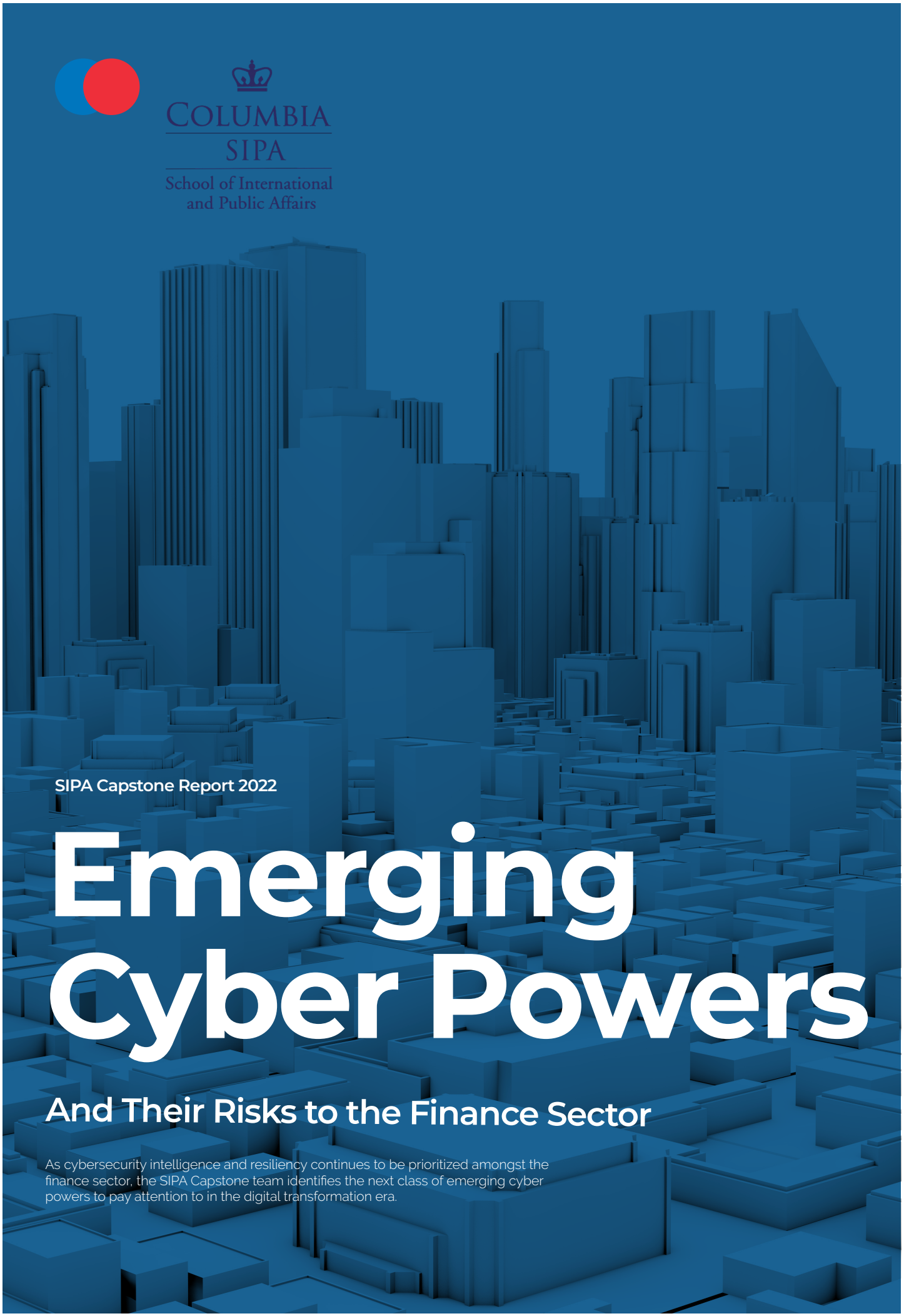


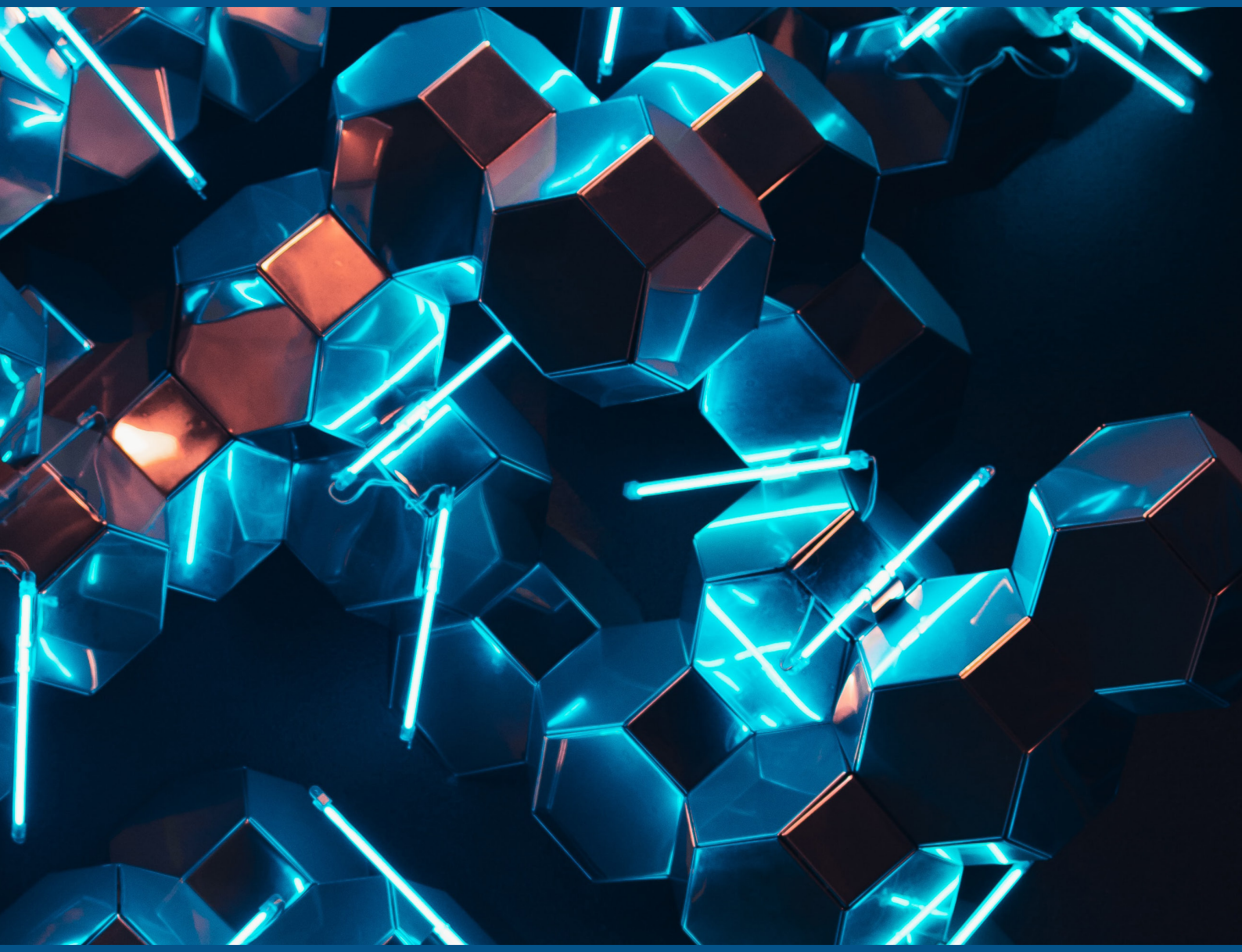
SIPA Capstone Report 2022

Emerging Cyber Powers

And Their Risks to the Finance Sector

As cybersecurity intelligence and resiliency continues to be prioritized amongst the finance sector, the SIPA Capstone team identifies the next class of emerging cyber powers to pay attention to in the digital transformation era.

Contents



SIPA Capstone Team

Stephen DiScenna
sgd2134@columbia.edu

Hyejung Hur
hh2878@columbia.edu

Seungmin (Helen) Lee
sl4238@columbia.edu

Yifan Li
yl4546@columbia.edu

Danielle Neftin
dfn2107@columbia.edu

Ryohta Yokokawa
ry2400@columbia.edu

Special Thanks

Colin Ahern
Naif Alkhathran
Michael Daniel
Luke McNamara
Sameer Patil
Ian Pelekis
Erinmichelle Perri
Neal Pollard
Greg Rattray
Adam Segal
Anina Schwarzenbach
Daniel Sorek
Waherguru Pal Sidhu
Carlyle Thayer
Ken Wolf

Published April 2022
Columbia University | School of International and Public Affairs

Report design by Danielle Neftin
Images courtesy of UnSplash image archive

Introduction

This project is sponsored by a Global Financial Institution's Cyber Threat Intelligence (CTI) team and written by Masters students at Columbia University's SIPA.

The CTI team provides global support to the Global Financial Institution's businesses and operations, providing the bank's leadership a nuanced understanding of current and emerging cyber threats.

The Global Financial Institution tasked the Capstone team to identify 2-3 emerging cyber powers, describe an understanding of their near-term strategic interests, and develop scenarios under which these countries might attack financial institutions with disruptive/destructive or espionage attacks.

The three states chosen are the Gulf States (Qatar, UAE, Saudi Arabia), India, and Vietnam. Scenarios for cyber conflict escalation and an analysis of each state's cyber capabilities is provided.

Background on Cyber Power Rankings

02

Literature review of cyber power assessments and indices

The team consulted five existing cyber rankings, Cyber Power Index 2011, the Potomac Institute's Cyber Readiness Index 2.0, ITU Global Cybersecurity Index, Belfer Center National Cyber Power Index, IISS Cyber Capabilities and EUI National Power Assessment. At a high level, each of the indices or assessments focuses on certain capabilities in determining the cyber power ranking or score of nation states.

The Cyber Power Index (CPI) 2011 was published by the Economic Intelligence Unit and Booz Allen Hamilton in 2011. The CPI 2011 measures G20 nations' digital adoption, cyber security, and the degree to which the economic and regulatory environment in G20 nations promote national cyber power.[1] The Index also identifies which states do not have cybersecurity plans or are developing them. By analyzing these measures, the Index pursued an understanding of what it takes for a state to operate in the digital era.[2] This index attempts to compare the cyber power rankings of G20 states on a scale of 0-100 with 100 being most favorable. Each country's ranking is a weighted mean of scores from four categories: Legal and Regulatory Environment, Economic and Social Context, Technology Infrastructure, Industry Application. A distinct feature of the CPI 2011 is that it considers not just military power but also emerging technology and societal shifts in states in order to measure cyber capability.[3] The CPI 2011 ranks the United Kingdom, United States, Australia, Germany and Canada as the top five cyber powers. In contrast, Brazil, Russia, India, and China (the BRICs) are labeled as states with much room for improvement, ranking 10th, 14th, 17th, and 13th respectively.[4]

The Potomac Institute for Policy Studies published the **Cyber Readiness Index 2.0** in 2015 in order "to assess the gap between a nation's current cyber security posture and the national cyber capabilities needed to achieve its economic vision."[5] This index analyzes seven indicators: national strategy, incident response, e-crime and law enforcement, information sharing, investment in R&D, diplomacy and trade, defense and crisis response.[6]

The International Telecommunications Union published the **Global Cybersecurity Index** in 2015 and updated the index in 2020. This index measured the 193 ITU Member States and Paletstine's commitment to cybersecurity by assessing six different metrics: legal measures, technical measures, organizational measures, capacity development measures, and cooperative measures. The top 10 nations were: 1. Singapore; 2. United States; 3. Malaysia; 4. Oman; 5. Estonia; 6. Mauritius; 7. Australia; 8. Georgia; 9. France; 10. Canada.[7]

In 2020, Harvard Kennedy School's Belfer Center published the **National Cyber Power Index (NCPI)** with the purpose of measuring "30 countries' cyber capabilities in the context of seven national objectives, using 32 intent indicators and 27 capability indicators."[8] NCPI defines "[t]he most comprehensive cyber power as the country that has (1) the intent to pursue multiple national objectives using cyber means and (2) the capabilities to achieve those objective(s)".[9] The Index lists the top 10 comprehensive cyber power states with the highest level of intent and capabilities: 1. United States; 2. China; 3. United Kingdom; 4. Russia; 5. Netherlands; 6. France; 7. Germany; 8. Canada; 9. Japan; 10. Australia.[10]

In 2021, the International Institute for Strategic Studies (IISS) published the **"Cyber Capabilities and National Power: A Net Assessment"** to determine the cyber power of 15 nation states.[11] The Net Assessment analyzes seven categories to rank cyber capabilities and national power: strategy and doctrine; governance, command, and control; core cyber-intelligence capability; cyber empowerment and dependence; cybersecurity and resilience; global leadership in cyberspace affairs; offensive capability.[12] Examining these seven categories, the Net Assessment ranks the 15 countries into three tiers:

1. Tier 1 of world-leading strengths in all categories: United States.

2. Tier 2 of world-leading strengths in some of the categories: Australia, Canada, China, France, Israel, Russia, United Kingdom.

3. Tier 3 of strengths or potential strengths in some of the categories but significant weaknesses in others: India, Indonesia, Iran, Japan, Malaysia, DPRK, Vietnam. [13]

Out of the five reviewed rankings, the Potomac Institute's Cyber Readiness Index 2.0 and Cyber Power Index 2011 are the most outdated, published in 2015 and 2011 respectively. Since the cyber domain is a fast-paced and constantly evolving field, the most recent reports and analyses provide a more accurate picture of cyber power rankings. The ITU's Global Cybersecurity Index was updated fairly recently in 2020 but heavily focuses on awareness, areas of improvement in cybersecurity, and defensive measures. Furthermore, the IISS Net Assessment refers to ITU's 2018 Global Cybersecurity Index in determining cyber security and resilience capabilities of states.

Methodology

The new bespoke index

While five cyber power rankings provide some useful metrics, this project's index must be aware of both capabilities and intent. In particular, the group needed to identify countries that would have strategic interest and ability to launch destructive/disruptive cyber operations or cyber espionage against financial institutions. This report heavily draws from the Belfer NCPI and IISS Net Assessment and adds insights from interviews with financial, cyber, and regional experts as well as open source research. The group developed **14 capability indicators** for the new bespoke index.

Unlike the Belfer NCPI and IISS Net Assessment, the bespoke index does not rank or tier the states but provides justifications for why the states were identified as emerging cyber powers. With this new bespoke index, the report finds that the **Gulf States (United Arab Emirates, Saudi Arabia, Qatar), India, and Vietnam** are likely to emerge as cyber powers in the next five to ten years.

Table 1.. Comparison of Cyber Power Capabilities

	Belfer NCPI	IISS Net Assessment	Bespoke Index
Year	2020	2019-21	2022
States	30 states: US, UK, Canada, Australia, France, Israel, Japan, North Korea, China, Russian Iran, India, Indonesia, Malaysia, **Vietnam**, Netherland, Germany, Spain, Sweden, Estonia, New Zealand, ROK, Switzerland, Turkey, Ukraine, Singapore, Brazil, Egypt **Saudi Arabia,** Italy, Lithuania	15 states: US, UK, Canada, Australia, France, Israel, Japan, North Korea, China, Russian Iran, India, Indonesia, Malaysia, **Vietnam**	3 states: Gulf States (UAE, Qatar, Saudi Arabia), Vietnam, India
Method	Index-based score 0-100: 27 capability indicators, 32 intent indicators	Qualitative analysis: 7 categories of capability indicators	Qualitative analysis with likelihood scenarios: 14 capability indicators, scenarios for intent development
Output	Ranking	Three Tiers	Justification for identification as emerging cyber power

Adopted Capability Indicators

Specifically from the NCPI, the bespoke index adopts the following capability indicators: state-sponsored attacks, global top 100 technology firms, high-tech exports, skilled employees in tech industry, cyber military staffing, evidence of private sector technology, cyber military doctrine, national cyber command, high-tech exports, cybersecurity laws, skilled employees in the technology industry. NCPI analyzes 27 capability indicators on a scale of 0 to 100 and maps the indicators to national objectives. The scope of this report's research goal only includes espionage and disruptive attacks which fall under the NCPI national objectives of intelligence collection and disabling adversary infrastructure. Another national objective that this report took into consideration is the national cyber defense objective. The research goal of this report focuses on cyber attacks that affect financial institutions which make cyber defense important as well.

Table 2. Adopted NCPI Capability

National Objectives	Intelligence Collection	Disabling Adversary Infrastructure	National Cyber Defense
Capability Indicators	1. State-sponsored attacks 2. Global top 100 technology firms 3. High-tech exports 4. Skilled employees in the tech industry 5. Cyber military staffing 6. Evidence of private sector technology	1. State-sponsored attacks 2. Cyber military doctrine 3. National cyber command 4. High-tech exports 5. Cyber military staffing	1. Cyber security laws 2. Skilled employees in the technology industry 3. Global top 100 cybersecurity firms

Similarly, the IISS Net Assessment organizes capability indicators in seven categories. Despite that the IISS Net Assessment lacks transparency in its underlying assumptions to its research[14], its broader methodology that takes into account the interaction among international security, economic competition, military affairs, and cyberspace is useful.[15] As with the application of Belfer NCPI to the new bespoke index, the takeaways from the IISS Net Assessment is centered around the research scope of disruptive/destructive and espionage attacks on financial institutions. The categories that then appear useful to the report are: strategy and doctrine; governance, command, and control; core cyber-intelligence capability; offensive cyber capability; and cyber security and resilience. These five broad categories also overlap with the selected indicators and national objectives from the Belfer NCPI.

New Capability Indicators

For this report, four additional capability indicators were identified: domestic repression, underground network of cyber criminals, cybersecurity education in primary and higher education, and the purchase of commercial/off-the-shelf malware.

In the next five to ten years, authoritarian states and economic powerhouses will be the winning actors in cyberspace. Authoritarian states and economically strong states are capable of either attracting talent or making their own cyber tools. Some of the capabilities drawn from Belfer NCPI already consider economic stability and strength of states. Thus, domestic repression is a proxy for authoritarianism that leads to cyber capabilities. States with domestic repression also have an increased likelihood of an underground criminal network, black market, and Deep Web and Dark Web activity. Following this indicator, the existence of an underground network of cyber criminals is critical to analyze as it can be sponsored by a state to carry out disruptive/destructive or espionage campaigns.[16]

The "buy versus build" principle explains that a cyber power can build its own capabilities and tools or purchase them. For example, Vietnam's hacking team leaks shows that Vietnam's APT32 used both custom tools and malware developed by in-house developers and contractors as well as publicly available tools.[17] For building capabilities, the existence of a domestic technology base, companies to provide cyber training ground, and cybersecurity education are necessary. Skilled employees in the tech industry was also an indicator drawn from the Belfer NCPI, and growth of cybersecurity in primary and higher education is another factor that signals a growing human capital in cyber-related fields.[18] Thus, the development of **cybersecurity education in primary and higher education** as well as purchase of **commercial/off-the-shelf malware** are cyber capability indicators that the new bespoke index should include.

Bespoke Capability Indicators

This report's bespoke index will thus include the following 14 capability indicators organized into three categories:

1. Private sector capabilities: Global Top 100 Technology Firms; Evidence of Private Sector Technology; High Tech Exports; Cybersecurity in Primary and Higher Education; Skilled Employees in the Tech Industry

2. Government capabilities: Stance/Doctrine/Law on Cybersecurity; National Cyber Command; Intelligence Agency; Cyber Military Doctrine;Cyber Military Staffing; State Sponsored Attacks

3. Underground and malicious capabilities: Domestic Repression; Purchase of Commercial/Off-the-Shelf Malware; Underground Network of Cyber Criminals

The 14 capability indicators will be given a label of lacking, developing, or developed to determine the overall private sector, government, and underground and criminal capabilities of each state.

Cyberspace will be bigger in the next 5 years. There isn't any more ocean, air or land, but everyday there is more cyberspace.

-Michael Daniel, President & CEO, Cyber Threat Alliance

Table 3. Bespoke Index 14 Capability Indicators

#	Indicator	Measurement	Implication
1	**Global Top 100 Technology Firm**	Number of firms headquartered in the states drawn from the Reuters' Top 100 Global Tech Leaders[19] and Forbes's Top 100 Digital Companies List[20]	These firms are the innovative companies that grow the domestic industry and can have international reach.
2	**Evidence of Private Sector Technology**	Size and age of industry, level of investment, and presence of innovative technology	Presence of a domestic technology sector would drive innovation and growth of cyber capabilities. International conglomerates and governments can invest into the private tech sector. The size, age, and level of investment of the industry indicate the ability of the tech sector to assist the government in creating new cyber capabilities.
3	**High-Tech Exports**	Percentage of high-tech exports as a total of manufacturing exports.	A strong tech sector exports high-tech products which increases a state's reputation and power while allowing intelligence access to the collected data in foreign countries.
4	**Skilled Employees in the Tech Industry**	Global rankings of tech and digital skills of the workforce	A large and growing tech workforce allows private sector companies and government agencies to fill open jobs and expand teams working on cyber capabilities. The workforce can be filled by domestic as well as foreign workers with the necessary skills.
5	**Cybersecurity in Primary and Higher Education**	Assessment of the number and prominence of programs designed to promote cybersecurity in education.	Cybersecurity education is crucial as students who have access to tech education are able to become the skilled workforce that the tech industry needs to grow. Cyber education programs created by the public and private sector help build the future domestic tech workforce.
6	**Stance/Doctrine/Laws on Cybersecurity**	The existence of laws and/or stance on cybersecurity in the state	Documents that set out priorities, budgets, or national strategies can indicate the type of actor the nation is in cyberspace. The evolution and quality of the documents give an indication of how they may act in the future as well.
7	**Intelligence Agency**	The existence of an intelligence agency in the state.	Well-funded intelligence agencies with a strong performance record are likely to delve into cyberspace intelligence, pushing for greater investment and innovation in the field. Agencies already using cyber capabilities for espionage are likely to continue doing so as well.
8	**National Cyber Command**	The existence of a National Cyber Command in the state.	The analysis of the existence, age, and composition of a centralized cyber agency helps identify proper coordination of all cyber activities and efficient control of all cyber capabilities necessary in wielding military cyber means when necessary.

#	Indicator	Measurement	Implication
9	**Cyber Military Doctrine**	The existence of a Cyber Military Doctrine in the state.	This capability examines the existence, age, and content of a national doctrine. The doctrine would direct the cyber component of the military in building the capabilities deemed necessary by the government and could indicate the growth of offensive capabilities in cyberspace.
10	**Cyber Military Staffing**	The number of cyber military staffing in the state.	The number of individuals staffing cyber military units demonstrates cyber capabilities.
11	**State Sponsored Attacks**	The number, type, and severity of cyber attacks attributed to a domestic state sponsored actor.	Examination of the state sponsored cyber actions offers insight into what types of actions they are likely to take in the future.
12	**Domestic Repression**	Global rank of domestic repression by Freedom House; evidence of use of cyber attacks against domestic dissidents.	Domestic repression by authoritarian regimes are a proxy for the creation of underground networks as well as the use of the Dark Web, VPNs, surveillance technology, and more.
13	**Purchase of Commercial/ Off-the-Shelf Cyber Capabilities**	Evidence of a state purchasing off-the-shelf cyber capabilities.	Since cyber power states either build or buy cyber tools and technology, the extent to which the states buy from cyber exporting states such Israel, Russia, and China needs to be incorporated. The purchased programs, such as Pegasus, often have advanced capabilities.
14	**Underground Network of Cyber Criminals**	Existence and size of cyber criminal organizations.	Cyber criminal organizations often have highly skilled individuals who can act as proxies for nation states and carry out cyber attacks. The groups can also be sources of disruption in the nation, leading to investment in cybersecurity and growth of the industry.

Measuring Intent: Scenarios

As mentioned earlier, at a high level, a cyber power needs to demonstrate both capabilities and intent to carry out cyber operations. Out of the five cyber power rankings reviewed, only the Belfer NCPI includes intent indicators which analyze both stated and demonstrated intent. Yet because the NCPI's intent indicators were often overlapping with cyber capability indicators, drawing intent indicators from the NCPI seemed redundant and limiting. For example, national cyber strategies are referenced as both intent and capability indicators. Therefore, for the purpose of this report, intent was not necessarily measured; rather scenarios in which the states can develop intent are offered. As requested by the client, the range of scenarios will be broad and unranked.

Limitation of Cyber Power Rankings

As the report offers its unique bespoke index, it is necessary to acknowledge that the creation of a cyber power index comes with five general limitations.

First, **there is no consensus on how to evaluate cyberpower** let alone how to define it. One source notes cyber power as "the ability to use cyberspace to create advantages and influence events in all the operational environment and across the instruments of power."[21] Another describes cyber power as "the use of resources related to cyberspace to achieve specific (political) ends inside and outside of cyberspace[22]." Evaluation of an ill-defined topic is obviously difficult.

Second, there is a **lack of publicly available data.** Often, information on a state's cyber capability is classified, is unclear, or is deliberately underranked for strategic reasons.[23] In addition, cyber research's focus on the West and the resulting strong dependency on English translations create a significant information gap between the West and other states such as China or Russia. [24]

Third, there is a **lack of data surrounding proxies** in cyberspace. Researchers tend to rely on proxies to determine cyber power such as cyber military strategy or attributions of state-sponsored attacks. However, such information on proxies are limited because non-state actors--private companies or cyber terrorists--are increasingly participating in the cyber domain. [25]

Fourth, there is the **difficulty of simplifying cyber power.** Unlike conventional domains--air, sea, land--the capabilities in the cyber domain are difficult to assess quantitatively and qualitatively.[26] For example, the number and quality of machines, engineers' skills and morale, information about cyber tools and their impact, and involvement of non-state actors are all crucial but difficult to analyze.

Fifth, there is a **duality of cyber capabilities.** A cyber capability to achieve an object can sometimes be counterproductive to other objects. For example, highly connected net users can benefit a government's internet monitoring efforts, but they also increase vulnerability to cyber attacks.[27] This duality creates a challenge in determining what factors contribute to a strength or weakness in cyber power.

Furthermore, the group is also aware of **exceptions such as North Korea.** If North Korea were to be evaluated based on the bespoke index, the conclusion would be that North Korea does not have the cyber capabilities to conduct sophisticated operations because it lacks private sector capabilities. However, North Korea is widely accepted as a cyber power for its cyber operations.

*** Refer to Appendix 1 for more information regarding North Korea ***

Emerging Cyber Powers

03

Based on the new bespoke index, the report identifies three emerging cyber powers: Gulf States, India, and Vietnam. This section will provide analysis and justification of identifying these three states as emerging cyber powers.

Gulf States: United Arab Emirates, Qatar, and Saudi Arabia

Background

The Gulf region has accelerated its development of cyber capabilities, particularly in the last five years. The three primary Gulf countries observed, Saudi Arabia, United Arab Emirates (UAE), and Qatar, have all shown expansion of cyber capabilities in both defensive and offensive arenas.

The Gulf states are emerging cyber powers not just because of the observed advancements in their cyber capabilities, but also because of the growing interdependencies which contribute to cyber security risks and disruptions. The three Gulf states are engaged in a regional power struggle to promote ideological principles and ro assert geopolitical influence, and they see the cyber domain as a potential weapon as well as a source of vulnerability.

The signing of the 2020 Abraham Accords initiated a new era of cyber cooperations between the Gulf states and Israel and simultaneously contributed to the recent turbulence in the region. Even though Saudi Arabia and Qatar did not sign the agreement, Saudi Arabia and the UAE are aligned on their cybersecurity partnerships with Israel. Israel, a known cyber power, is responsible for capturing 40% of all global private cyber investments[28] and for creating powerful cyber surveillance technologies like Pegasus, which has been purchased by both Saudi Arabia and the UAE.[29] Moreover, Saudi Arabia and the UAE share a common regional adversary with Israel--Iran. However, Qatar still retains close cooperations with Iran..

The region's recent improvements in cyber capabilities only contribute to the added turbulence in the Gulf. The region's desire to digitize their societies, adopt cloud networking technologies, incorporate cryptocurrencies to attract foreign investment, and shift away from energy dependence through economic diversification efforts creates new risks and opportunities. Since 2012, the Gulf has already experienced its share of cyber attacks. Below is an overview of examples of previous cyber attacks, which also serve as the bases for the plausible future disruptive cyber scenarios further described in this section:

Gulf States: United Arab Emirates, Qatar, and Saudi Arabia

> Some Arab Gulf states, particularly Saudi Arabia have heavily invested in cyber capability-building that includes digital transformation and e-governance aiming to overcome cyber security concerns but also to create a safe cyber infrastructure for private sector and potential foreign direct investments.

-Naif Alkhathran, Regional Researcher for Middle Eastern Security Policy

Table 4. Cyberattacks in the Gulf

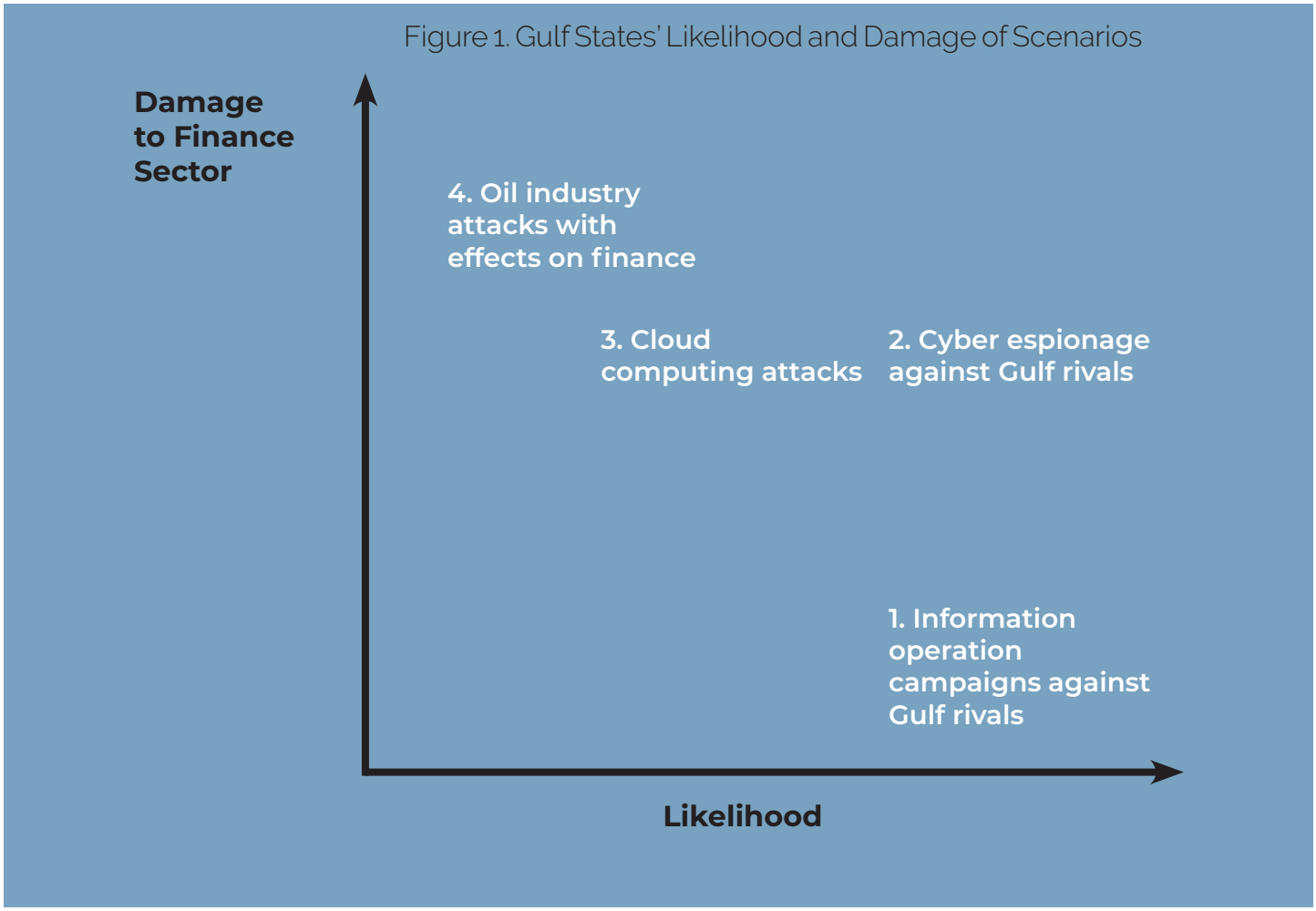
Year	Attacker	Target	What Happened
2012	Iran	Saudi Aramco	Iran was attributed for spreading the 'Shamoon' virus in 2012 to hack Aramco; 35,000 computers were partially wiped out or destroyed.[30]
2016	UAE's Project Raven	Emir of Qatar, a Nobel Peace laureate human-rights activist in Yemen	Project Raven, a UAE funded hacking group, obtained remote-access to smartphones and other computer devices via a "zero-click" exploit.[31]
2017	NSA	Middle Eastern Banks, including Dubai based SWIFT management company "EastNets"	In 2017, hacking group Shadow Brokers revealed NSA data infiltration/espionage motivated hacks into Middle Eastern banking systems, including those in UAE and Qatar.[32]
2017	UAE's Project Raven	Journalists and dissidents with connections to Qatar and/or Muslim Brotherhood	Using the hacking tool, "Karma", Project Raven hacked into the smartphones of journalists who had connections to Qatar and the Muslim Brotherhood.[33]
2017	Saudi Arabia	Qatar	Disinformation campaigns--spreading misinformation about a coup in Qatar[34] and direct hacks of Qatar's news site QNA[35]--spurred a diplomatic crisis.[36]
2017	Saudi Arabia	Jammal Khashoggi	Saudi Arabia allegedly used Pegasus spyware to surveil dissidents and journalists, like Khashoggi.[37]
2021	Unknown Cyber Criminals	Saudi Aramco	1,000 gigabytes of data were extorted, resulting in a $50M ransom by the extortionists.[38]

Interviews with regional, cyber, and financial sector experts have delivered conflicting views regarding whether the Gulf states will use their increased cyber capabilities to engage in conflict with each other.[39] Whereas the Gulf's successful cyber capability developments cannot be denied, there are still disagreements regarding motivations behind one Gulf power committing a disruptive cyber attack against a neighboring Gulf power.

Intent Scenario and Likelihood

Based on expert interviews, an analysis of the 14 capability indicators for each Gulf state, and open source research, the team identified the following plausible scenarios for cyber attacks affecting financial institutions.

Figure 1. Gulf States' Likelihood and Damage of Scenarios



1. Information Campaigns against rivals in the Gulf

Saudi Arabia, UAE, and Qatar compete against each other in terms of speed towards economic diversification away from gas and oil, digital transformation of urban hubs, and fight over the role of being the regional leader of the Gulf. As part of their efforts to counter their rivals, the states have launched campaigns and used cyber to silence dissidents who were not aligned with larger strategic security goals.

For example, in 2017, Qatar reportedly launched multiple online information campaigns designed to mobilize support for the Muslim Brotherhood amongst Saudi audiences. The Muslim Brotherhood is a political movement which is currently designated as a terrorist organization in Saudi Arabia, but is financially supported by Qatar. In the 2017 "GlobalLeaks"[40] campaign, Qatar reportedly released confidential communications between the UAE and American pro-Israel think tanks regarding preventing Iran's nuclear developments, just after Saudi Arabia and the UAE condemned Qatar for supporting terrorist organizations.

The relative success of previous hacking, doxxing, and disinformation campaigns suggests they might be used again by regional actors. Financial institutions could be directly targeted or find proprietary information released to the public through attacks on others such as law firms, journalists, and government regulatory agencies.

2. Cyber espionage against rivals in the Gulf

Cases of cyber espionage have become rampant in the Gulf, with increases largely due to the utilization of off-the-shelf tracking software like Pegasus and DarkMatter, and the institutionalization of "cyber armies" in all three Gulf states.

In Saudi Arabia, the crown prince Mohammed bin Salman Al Saud hired Saud al-Qahtani, a hacker best known as the "lord of the flies", to institutionalize the kingdom's first information operations army. The soldiers, coined as "the flies", assisted al-Qahtani with hacking and spying on the dissident journalist Jammal Khashoggi through the use of Pegasus, a controversial Israeli spyware. UAE also used Pegasus to hack civil rights activists[41] while developing its own domestic cybersecurity firm, DarkMatter, to lead targeted cyber espionage under a program called Project Raven.[42] There are limited reports that suggest that Qatar uses these spyware softwares, or conducts similar espionage activities at the same scale as Saudi Arabia and UAE.[43]

As tensions between Saudi Arabia, UAE, and Qatar rise, the rivals may turn to cyber espionage campaigns in order to gain an advantage in the information war or a potential physical conflict. Financial information would be a prime target for cyber attackers as they seek to learn their rivals' proprietary information in order to gain offensive advantages. For example, attackers could be motivated to extract financial data in order to use the information for competitive advantage, trace payments to terrorist groups like the Muslim Brotherhood, or to find financial evidence that could point to a future destructive attack.

3. Cloud computing attacks including on enterprise and consumer cloud

The three Gulf states have their own "Vision 2030" programs underway to digitize their respective major cities. The Vision 2030 projects' goals are to: 1) upgrade digital infrastructures in order to diversify the economies and welcome foreign investment, and; 2) improve cyber capabilities in order to remain competitive and as well as to protect the new digital infrastructures.

Some regional and cyber experts are skeptical that further economic digitization projects like the Vision 2030 plans will lead to any scenarios of disruptive cyber attacks to the finance sector.[44] Because the ultimate desire is to invite foreign investment into the region, it is not in the Gulf's interest to show any form of instability, whether in one's own state, or in a neighboring Gulf state. However, CrowdStrike's 2022 Global Threat Report cites an increase in overall adversarial attacks shifting to the cloud computing space.[45]

Other security experts who agree with this scenario state that strategic advantage always trumps any facade of regional economic cooperation.[46] With growing tensions regarding ideological differences and competition to secure the role of regional leadership, it remains plausible that the new digitized systems and cloud infrastructures remain a target for a disruptive attack, which could easily have a negative impact on financial systems.

4. Continued attacks on the oil industry with direct effects on financial sector

Saudi Aramco has been subject to three large disruptive cyber attacks since 2012. The latest was a July 2021 cyber attack on the oil company, in which hackers demanded $50 million to return stolen data.[47] Even though it has been reported that the region's finance sector has not been directly affected by these targeted attacks, it is plausible that these hacks to the oil sector will become more persistent and have an impact on the banking sector.

Cyber attacks outside the financial sector can have indirect effects on the banking industry. For example, a destructive attack on the oil sector can have short term effects on the financial markets. Or, Iran can continue to support its proxy war in Yemen and continue to launch attacks on Saudi and UAE oil fields, which will lead to market instabilities. There are past examples of economic volatilities in Saudi Arabia caused by physical warfare in Yemen. Starting in 2015, the Houthis were financed by Iran to conduct drone strikes on Saudi and UAE oil tanks.[48]

In 2019, the Houthis managed to destroy core Saudi oil facilities, taking them offline for a few days, which largely affected the world's oil supply and caused oil prices to spike by 10-15%.[49]

Capability Indicators

Overview Of Gulf States

PRIVATE SECTOR 	**Global Top 100 Technology Firms** *Developing*	**Evidence of Private Sector Tech** *Developing*	**High Tech Exports** *Lacking*	**Education** *Developing*	**Skilled Employees in the Tech Industry** *Developed*	
GOVERNMENT 	**Cybersecurity Law/Doctrine** *Developed*	**Intelligence Agency** *Developing*	**Cyber Military Doctrine** *Lacking*	**Cyber Military Staffing** *Lacking*	**State Sponsored Actors** *Developing*	**National Cyber Command** *Lacking*
UNDERGROUND AND MALICIOUS 	**Domestic Repression** *Developed*	**Purchase of Malware** *Developed*	**Underground Network of Cyber Criminals** *Lacking*			

*** Refer to Appendices 2,3,4 for more detailed analyses on Gulf States capabilities ***

QATAR

Private Sector Capabilities:

Qatar has no top 100 technology firms based in the nation and only 7.1% of their manufactured exports are considered high-tech.[50] However, the state has one of the highest internet penetrations in the world and shows evidence of strong private sector technology growth. The ICT sector is currently estimated to be $4.4 billion and should double within the next 4 years with the assistance of massive government funding and promotion.[51] Qatar ranks 6th in the world for quality of math and science education.[52] Partnerships in higher education with the private sector seeks to promote greater technical competency in the workforce which has led to graduates having the 8th best digital skills in the world. Qatar ranks 9th among all nations in retaining skilled employees, suggesting that the state has the necessary draws to maintain a strong tech industry.[53]

Government Capabilities:

Qatar's government lacks several important capabilities from the index. It has no cyber military doctrine, no national cyber command, and no known cyber military staff. The Qatar State Security, the national intelligence agency, performs internal security investigations, gathers intelligence, and has primary responsibility for sedition and espionage cases, but Qatar lacks a dedicated cyber intelligence agency. The state established the Cybercrime Prevention Law in 2014 to govern cyber crimes and the Personal Data Privacy Protection Law in 2016 to define individual right to the protection of personal data. Qatar also established a National Cyber Security Strategy in 2014.[54] In terms of state-sponsored activities, the state hired U.S.-based hackers to carry out cyber espionage operations against several critics of the regime.[55]

Underground and Malicious Capabilities:

Qatar has an immense police and internal security apparatus and has purchased off-the-shelf capabilities to increase their repression capabilities in cyberspace. The state has also approached U.S. defense contractors for help in building offensive capabilities.[56] There is no significant underground cyber group or individual in Qatar, but the whole region does host several underground servers that sell malware and malicious services.

> **The Gulf states seem like natural places [for emerging cyber conflict]. The realignment with Israel and its relationships with the Gulf states seems like a definite thing.**
> *-Colin Ahern, Deputy Chief Information Security Officer for the City of New York*

UNITED ARAB EMIRATES (UAE)

Private Sector Capabilities:

The UAE has one top 100 technology firm based in the nation: Etisalat, a telecommunications company with $14 billion in sales.[57] The ICT sector is estimated to reach $23 billion in 2024.[58] Several government campaigns promote diversification away from oil and into technology to push this growth. Currently, only 5% of UAE's manufactured exports are classified as high-tech.[59] The state is 13th in the world for quality of math and science education and has announced several partnerships with private firms and global universities in order to help grow the skilled domestic workforce. The digital skills of its workforce ranks 14th in the world, and the UAE ranks 2nd among all nations in retaining skilled workers.[60]

Government Capabilities:

The UAE's government lacks several important capabilities from the index. It has no cyber military doctrine, no national cyber command, and no known cyber military staff. The Signals Intelligence Agency seeks to protect the nation's cybersecurity and is considered the equivalent of the U.S. National Security Agency. Its precursor was known to endorse Project Raven.[61] The state established Combating Cybercrimes legislation in 2012 and updated it in 2018 and the National Cybersecurity Strategy of 2019 was introduced to guide the nation's cyber response. The UAE has sponsored cyberattacks on Qatari government news and social media sites and has hacked phones of journalists and media execs.[62]

Underground and Malicious Capabilities:

The UAE also has a well developed domestic repression apparatus, and the state has purchased off-the-shelf capabilities to increase their repression capabilities in cyberspace. The state has purchased Pegasus from NSO. The state also hired former U.S. government intelligence personnel working for Dark Matter to build an advanced capability to compromise challenging technical targets and boost the government's cyber abilities, thus boosting the UAE's cyber abilities significantly and quickly to achieve previously hard-to-obtain goals in cyberspace.[63] While no major underground cyber groups or individuals are based in the UAE, the Middle East hosts several servers that sell malware and malicious services.

SAUDI ARABIA

Private Sector Capabilities:

Saudi Arabia has one top 100 technology firm based in the nation: Saudi Telecom, a telecommunications company with $16 billion in sales.[64] The state's ICT market is considered relatively untapped at the moment, but recent government campaigns are seeking to jump start domestic ICT growth. In April 2022, it was announced that Kaspersky Lab, the Russian multinational cybersecurity firm, would open its regional headquarters in Saudi Arabia.[65] Despite these recent private sector advancements, the current lack of a formal tech sector is evident as only 0.61% of manufactured exports are considered high-tech.[66] The state also lags behind on their education standards, ranking 63rd in the world for their math and science education programs. However, Saudi Arabia does have 15 top ranked universities and is seeking to update its STEM curriculum through several government initiatives. Saudi Arabia has a distinct lack of a skilled workforce and will be short over half a million highly skilled workers by 2030.[67]

Government Capabilities:

Saudi Arabia's government lacks several important capabilities from the index. It has no cyber military doctrine, no national cyber command, and no known cyber military staff. The General Intelligence Presidency is the primary intelligence agency but does not have a significant cyber component. The state only has the Anti-Cyber Crime Law of 2007 to address unauthorized online behavior, and it recently approved a National Cybersecurity Strategy in 2020 to address the need for forming a cyber competent nation.[68]

Underground and Malicious Capabilities:

According to Freedom House, Saudi Arabia is the least free of the Gulf States, with extensive domestic repression.[69] The state has expanded its arsenal in cyberspace through purchasing capabilities from foreign entities such as NSO. Their focus has primarily been on surveillance activities.[70] Saudi Arabia plays host to Dev-point, an underground forum that sells malware.[71]

India

Indian policy makers are taking interest on cyber issues and the pursuit of digital policies is the key dimension of India's growing diplomatic profile.

-Sameer Patil, Senior Fellow on Observer Research Foundation

India

Background

India has had long-standing disputes over territories with Pakistan and China, India's top adversaries and both nuclear powers. Pakistan has threatened Indian territories, leading to skirmishes at the border in which a majority of residents are Islamic supporters of the Pakistani government. Tensions have especially intensified in Kashmir. China's rise and increasing ability to project military power also pose a threat. China and India share thousands of miles of contested border in the Himalayan mountain region, and the navies of the two countries increasingly face each other in the Indian Ocean.[72]

The China-India border is a hot spot especially worth monitoring. Chinese and Indian troops have been in a standoff in the Ladakh region, and, in June 2020, at least 20 Indian soldiers were killed in a clash with Chinese forces--using sticks and clubs--in the Galwan Valley for the first time in 45 years.[73] Several rounds of talks have failed to resolve the boundary disputes, and the two states are strengthening their presence in the region by building infrastructure. In the Indian Ocean, China has dispatched naval ships and constructed bases and ports in Pakistan, strategic points for the Chinese "the Belt and Road Initiative (BRI)".[74] This trend has significantly threatened India's maritime security and sea lanes.

The two adversaries also clash in the cyber domain. India has faced numerous cyber attacks from Chinese state-sponsored groups, and the targets have included the networks of military units, the energy sector, and financial institutions.

India is one of the top three targets of cyberattacks with Japan and Australia in Asia.[75] The most targeted sectors are in banking and finance, though government agencies have also experienced widespread cyberespionage campaigns.

Some of the major reported cyberattacks against India include the following listed in Table 5 below:

Table 5. Cyberattacks against India

Year	Attacker	Target	What Happened
2019 - 2022	APT36 (Operation SideCopy)	Indian defense units and armed forces individuals [76]	A Pakistani cyber group conducted phishing attacks against Indian defense networks to steal confidential information.The attack used fake COVID-19 health advisories.
2011 - 2021	Undetected Hackers	The airline data service provider of the Air India [77]	By hacking into the passenger service system, 4.5 million passengers' personal data was leaked.
2021	Undetected Hackers	Customer data of Domino's India Pizza. [78]	Hackers stole credit card records, names, phone numbers, and email addresses.
2021	Pakistan-related Hackers	Indian police [79]	Personal information of 500,000 Indian police officers was put up for sale on a database sharing forum after hacks by what is assumed to be a Pakistan-related group.

Over the last few years, cybersecurity firms have begun tracking state-sponsored Indian cyber threat actors. Recent incidents include:

Table 6. Indian cyberattacks or related incidents

Year	Attacker	Target	What Happened
2020	Two cyber groups (one is ModifiedElephant)	Indian activist charged with terrorism [80]	A program for cyber espionage was found from a jailed human rights activist's laptop, which indicated the possibility of connections between the Indian government and cyber groups targeting foreign adversaries and domestic critics. (No clear evidence found)
2020	Unknown hackers from India	Organizations and individuals in China, Pakistan, Nepal[81]	Chinese news outlet, Global Times, reported that cyberattacks from groups in India targeted China, Pakistan and Nepal.
2017	N/A	N/A	Indian government's purchase of "Pegasus," which allows the government to inject malware in others' cyber networks.[82]

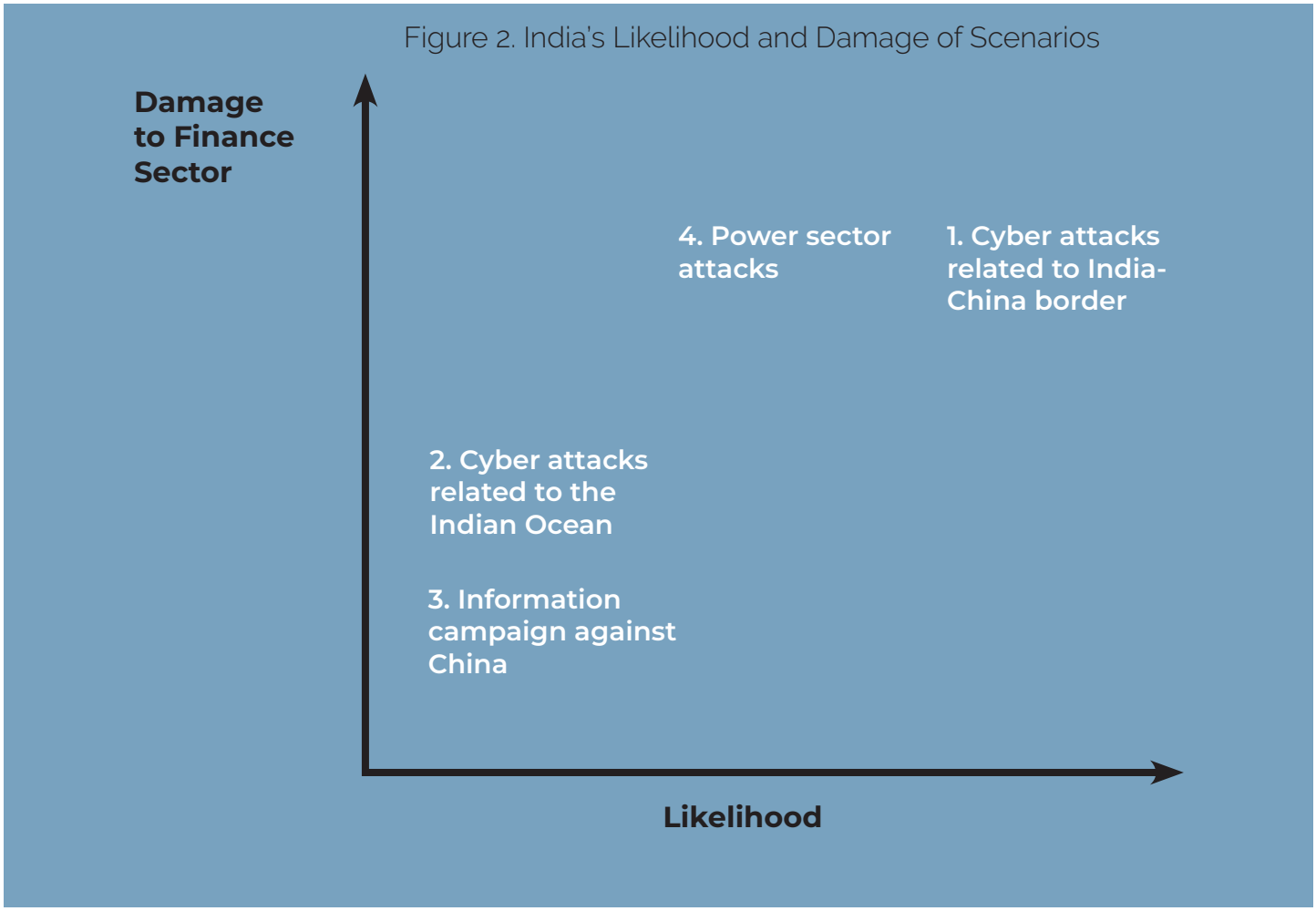
If you look at India's economy, a large part of the export is coming from the software industry.

-Waheguru Pal Sidhu, Clinical Professor of New York University

Intent Scenario and Likelihood

There are four possible scenarios, considering the recent border disputes. A cyberattack between China and India regarding border disputes is the most likely scenario in the near term that can cause considerable damage to the finance sector.

Figure 2. India's Likelihood and Damage of Scenarios



Both the Indian Ocean and the Tibetan issues are not likely to happen in the near future. Although the Indian Ocean conflict could cause a medium level of damage, India still controls the ocean and chokepoints, and the Chinese navy is focusing on the South and East China Sea; therefore, a large-scale Indian Ocean event could only happen in the long term. For the Tibetan issue, the Dalai Lama still has a considerable amount of time to arrange his reincarceration and the real damage to the Chinese and Indian people is still unknown, especially since the Tibetan issue has been deescalating in recent years.

Power sector attacks between China and India are increasing in recent years, and Chinese hackers are reportedly targeting India's power grid recently. The power sector plays an important role in the financial world, and a potential attack on the power sector could cause a considerable amount of damage to India's financial sector.

1. Cyber Attacks related to China-India Border

Border disputes between China and India are not likely to be resolved anytime soon even though the two countries have held several talks. The risk of escalation of tensions remains significant. In the near term, both parties show considerable restraint: in the military border conflicts, both forces restrain from using any hot weapons. These cases show that both states do not want an escalation, which could create the motivation for a DDoS or malware attacks. In terms of the spillover effect, the financial sector could be caught in the crossfire and some websites might be taken down.

2. Cyber Attacks related to Indian Ocean

The Indian Ocean includes China's vital energy routes from the Persian Gulf and Africa. India has considerable advantages in the maritime dimension that it could employ to restrict China's Indian Ocean trade. The significance of the Indian Ocean has driven the Indian Navy to adopt a strategy of building its naval capabilities near the Indian Ocean chokepoints, particularly around the Malacca Strait, to create an implicit threat of interdiction of China's sea lines of communication. Previously, the Navy had threatened blockades against Pakistan.

After the India-China border clashes, the Indian Navy deployed additional ships, although precise locations are unclear. While India would have a difficult time imposing a blockade on Chinese shipping, it could consider interdicting Chinese tankers as they pass near India's Andaman and Nicobar Islands or delaying Chinese shipping traffic.

Cyber attacks during maritime disputes are highly critical. Potential cyber attacks on maritime infrastructure include phishing, malware, social engineering, brute force, denial of service, and ransomware.[83] Another risk factor is the absence of IT people on ships. Attacks targeting maritime information systems are on the rise. The Indian Ocean is important in maritime trade, and a lot of commerce is going on in the Indian Ocean. The cyber conflict related to the Indian Ocean could cause the websites of financial services to be taken down and influence financial transactions.

3. Cyber Attacks related to Indian Ocean

Tibetan Issues

The 14th Dalai Lama and China may clash over the next reincarnation of the Dalai Lama. The spiritual leader has mused that he may reincarnate outside of the Tibet region, but Beijing has enshrined the right to choose his successor into Chinese law. The Dalai Lama, who recently turned 86, has insisted that discussions of his death are premature because according to his visions, he will live to 113. Nevertheless, a power struggle for his successors ensues. Tibetan issues have remained a sensitive factor in India's relationship with China, and India controls the Dalai Lama's movements. As relations with China have deteriorated to historic lows over the past year due to border aggression, there has been increased pressure on the Indian government to strengthen its Tibet policy in order to counter China.

India could carry out an espionage campaign on China for information regarding the Dalai Lama. Either leaking the information about political discussion of the issue or distributing information from the 14th Dalai Lama could cause disturbances in Chinese society. Such information leaks could harm Chinese reputation which may influence the foreign investment towards China, thus affecting the financial sector.

Coronavirus Related

The 14th Dalai Lama and China may clash over the next reincarnation of the Dalai Lama. The spiritual leader has mused that he may reincarnate outside of the Tibet region, but Beijing has enshrined the right to choose his successor into Chinese law. The Dalai Lama, who recently turned 86, has insisted that discussions of his death are premature because according to his visions, he will live to 113. Nevertheless, a power struggle for his successors ensues. Tibetan issues have remained a sensitive factor in India's relationship with China, and India controls the Dalai Lama's movements. As relations with China have deteriorated to historic lows over the past year due to border aggression, there has been increased pressure on the Indian government to strengthen its Tibet policy in order to counter China.

India could carry out an espionage campaign on China for information regarding the Dalai Lama. Either leaking the information about political discussion of the issue or distributing information from the 14th Dalai Lama could cause disturbances in Chinese society. Such information leaks could harm Chinese reputation which may influence the foreign investment towards China, thus affecting the financial sector.

4. Power Sector Attacks

India and China are highly vulnerable for their reliance on coal for electricity. Cyber attacks on the power sector could potentially cause a blackout. A Chinese state-sponsored group, Red Echo, gained a foothold in nearly a dozen critical nodes across the Indian power generation and transmission infrastructure.[84] Potential Chinese DDoS attacks targeting India's power sector could create considerable damage to India's financial world. If India's power sector was disrupted, all financial transactions and activities would malfunction. Then, the Indian financial and stock market would be disrupted.

A surge of malware directed at India's power sector, from petroleum refineries to nuclear power plants, have been reported.[85] According to a U.S.-based private cybersecurity company's report, India's power sector has been targeted by hackers in a long-term operation by a Chinese state-sponsored group.[86]

So far, there is no public attribution of power sector DDoS and Malware attacks from India, but it could be a source of conflict in future cyber attacks. The financial sector is interrelated with the power sector in India. Not only do daily transactions need the power sector's support, but the entire city could be shut down without electricity.

Capability Indicators

Overview of India

India's build-up of cyber capability is delayed in all sectors, and cyber skills remain underdeveloped. However, India has huge cyber potential given the number of computer users and its economic growth. In the last decade, India has launched a number of cyber policies including the National Cyber Security Policy and established a military cyber command, Defense Cyber Agency (DCA). India has the potential to become a cyber power that can counter not only Pakistan but also China in the near future.

PRIVATE SECTOR	**Global Top 100 Technology Firms** *Developed*	**Evidence of Private Sector Tech** *Developing*	**High Tech Exports** *Developing*	**Education** *Developing*	**Skilled Employees in the Tech Industry** *Developing*	
GOVERNMENT	**Cybersecurity Law/Doctrine** *Developing*	**Intelligence Agency** *Developing*	**Cyber Military Doctrine** *Developing*	**Cyber Military Staffing** *Developing*	**State Sponsored Actors** *Lacking*	**National Cyber Command** *Developing*
UNDERGROUND AND MALICIOUS	**Domestic Repression** *Developing*	**Purchase of Malware** *Developing*	**Underground Network of Cyber Criminals** *Developing*			

*** Refer to Appendix 5 for more detailed analysis on India's capabilities **

Private Sector Capabilities:

India's private sector has great potential backed by the population and robust economic growth, yet it has a large, underskilled, young population. In particular, the digital literacy and skill of the citizens are poor, and education levels have not kept pace with the sharp increase in the number of computer users.

Five Indian technology firms are ranked in global top 100 technology firms lists.[87] Though this number surpasses those of China and Pakistan, it is less than other developed Asian nations such as Japan and Taiwan. India's private sector technology shows salient development in recent years.[88] The ICT market had an estimated value of $200 billion in 2019 and is expected to grow at 5-6% per year between 2021 and 2025. India also showcases strong high tech exports.[89]
The average value of high tech exports as a percentage of total manufactured exports for India from 2009 to 2020 was 8.69%. In comparison, the average of 129 countries in 2020 was 10.9%. Also, according to the World Rank,[90] India's percent of manufactured exports from 2009 to 2020 ranked at 45th out of 129 countries.

However, India's cybersecurity education is lagging. The Data Security Council of India (DSCI), the National Critical Information Infrastructure (NCIIPC), and a cyber partnership with the UK attempted to enhance Indian cybersecurity education but the DSCI and NCIIPC are in nascent phases and the partnership is still under discussion.[91] India also has few skilled tech employees. According to the Global Skills Index (GSI) 2021 report,[92] India's employees' skills are ranked 66th out of 102 countries in information technology and in data science. Moreover, the ITU's 2018 Global Cybersecurity Index (GCI)[93] ranked Indian cybersecurity education 47th out of 175 countries. Thus, India has poorly trained workers and underdeveloped cybersecurity education.

Government Capabilities:

The Indian government and military turned their attention to national cyber security policy in 2010. Many intelligence agencies also have attempted to cover cyber domains in their missions. Yet, the different organizations fail to coordinate in the cyber domain.

India set up the National Cyber Security Policy[94] and the Information Technology Act to enhance its cyber capability. It also established the Defense Cyber Agency (DCA) and is planning a new command of Defense Cyber Command (DCC). The Integrated Defense Staff Ministry of Defense published the Joint Doctrine Indian Armed Forces in 2017 as the first Indian military doctrine that emphasizes the integration of capabilities across the armed forces and cyber power. Simultaneously, the military has strengthened its cyber warfare training for military personnels in DCA and the Department of Military Affairs (DMA). The Indian government has also organized a Computer Emergency Response Team (CERT-In) and National Cyber Coordination Center (NCCC) to enhance the cybersecurity and cooperated with the Research and Analysis Wing (RAW) for cyberintelligence.

India has revealed little about public investment in offensive cyber capabilities. Some reports suggest that state-backed groups, such as ModifiedElephant, attack domestic critics, foreign defense firms, military units, and Chinese and Pakistani state-owned enterprises.

Underground and Criminal Capabilities:

With the second-largest internet population in the world, India is a large target for cyber criminals. On the other hand, some hacker groups that target China and Pakistan and are based in Delhi--such as "baby elephant" and "white elephant".[95] In 2021, Freedom House reported that India scored a 70 out of 100 for civil liberties and rights, receiving the title of "partly free".[96] However, the Indian government is strengthening online censorship. In 2020 the Indian government asked Twitter to remove nearly 10,000 tweets that criticized the government.[97] The Indian government also acquired the spyware "Pegasus'' from Israel in 2017. [98]

Vietnam

Even though cyber is seen as an asymmetric weapon, it is not in Vietnam's interest to provoke China because that will lead to 100 years of pressure and retaliation.

-Carlyle Thayer, Emeritus Professor of the University of New South Wales Canberra

Vietnam

Background

Since the 1970s, Vietnam and China have asserted claims over the South China Sea, a major shipping route for global commerce that has fish and oil and gas reserves.[99] Tensions between the two have increased over the last two decades as China increased its military activities in the South China Sea with fighter jets, cruise missiles, a radar system, and military exercises.[100]

The arrest of the Vietnamese maritime militia by the Chinese coast guards may serve as a trigger to escalate into military conflict. China previously argued that the activities of the Vietnamese maritime militia around the disputed reefs and islets pose a threat to China's maritime law enforcement and national security. As a retaliatory measure against such an arrest, Vietnam, who has filed only diplomatic protests against China's claims of sovereignty over the South China Sea, may decide to carry out cyberattacks against China. Considering its inferior military power, economic dependence on China, and historical communist ties to Beijing, the Vietnamese leaders may view cyberattacks as a useful tool to push back against China's claims of sovereignty over the South China Sea, without risking further escalation.

There have been numerous state-sponsored cyberattacks between the two. Chinese state-sponsored cyber espionage operations target the government and private sector across Southeast Asia. Malaysia, Indonesia, and Vietnam are the top three targeted countries according to Insikt Group. More than 100 Chinese state-sponsored intrusions targeting Vietnam were carried out for nine months in 2021.[101]

Table 7. Chinese cyberattacks against Vietnam and Southeast Asian

Year	Attacker	Target	What Happened
2016	China 1937CN team	Airports in Vietnam	Flight information screens were compromised, check-in counters were shut down, and the personal data of 411,000 passengers were leaked. [106]
2021	TAG-16	National Assembly, the central office of the Communist Party, and government organizations in Southeast Asia	Using custom malware such as FunnyDream and Chinoxy, TAG-16 conducted cyber espionage campaigns. [102]
2021	Naikon	Military organizations in Australia, Indonesia, the Philippines, Vietnam, Thailand, Myanmar, and Brunei	Stealth campaigns for espionage and data exfiltration against forieng militaries were executed.[104]
2021	Cycldek	Government and military entities in Vietnam	Cycldek used malware to take full control over compromised devices and exfiltrated data. [105]
2021	Gallium, Naikon APT, TG-3390	Five major telecom companies in Southeast Asia	A cyber espionage campaign collected sensitive information and compromised high profile business assets. [103]

Recently, Vietnam carried out intrusions against China to collect information on COVID-19. In addition, it has conducted several cyber espionage operations which aim to gain economic advantage over regional competitors.

Table 8. Vietnamese cyberattacks against China and other economic competitors

Year	Attacker	Target	What Happened
2020	APT32	China's Ministry of Emergency Management and the Wuhan municipal government	APT32 intruded on Chinese government devices to collect intelligence on the Covid-19 crisis. [107]
2017	APT32	Foreign corporations in Asia, Germany, and the United States	Industrial espionage against foreign corporations were executed. [108]
2016	APT32	Global corporation based in Asia	APT32 conducted a year-long cyberattack that targeted intellectual property, confidential business information, and the details of specific projects. [109]

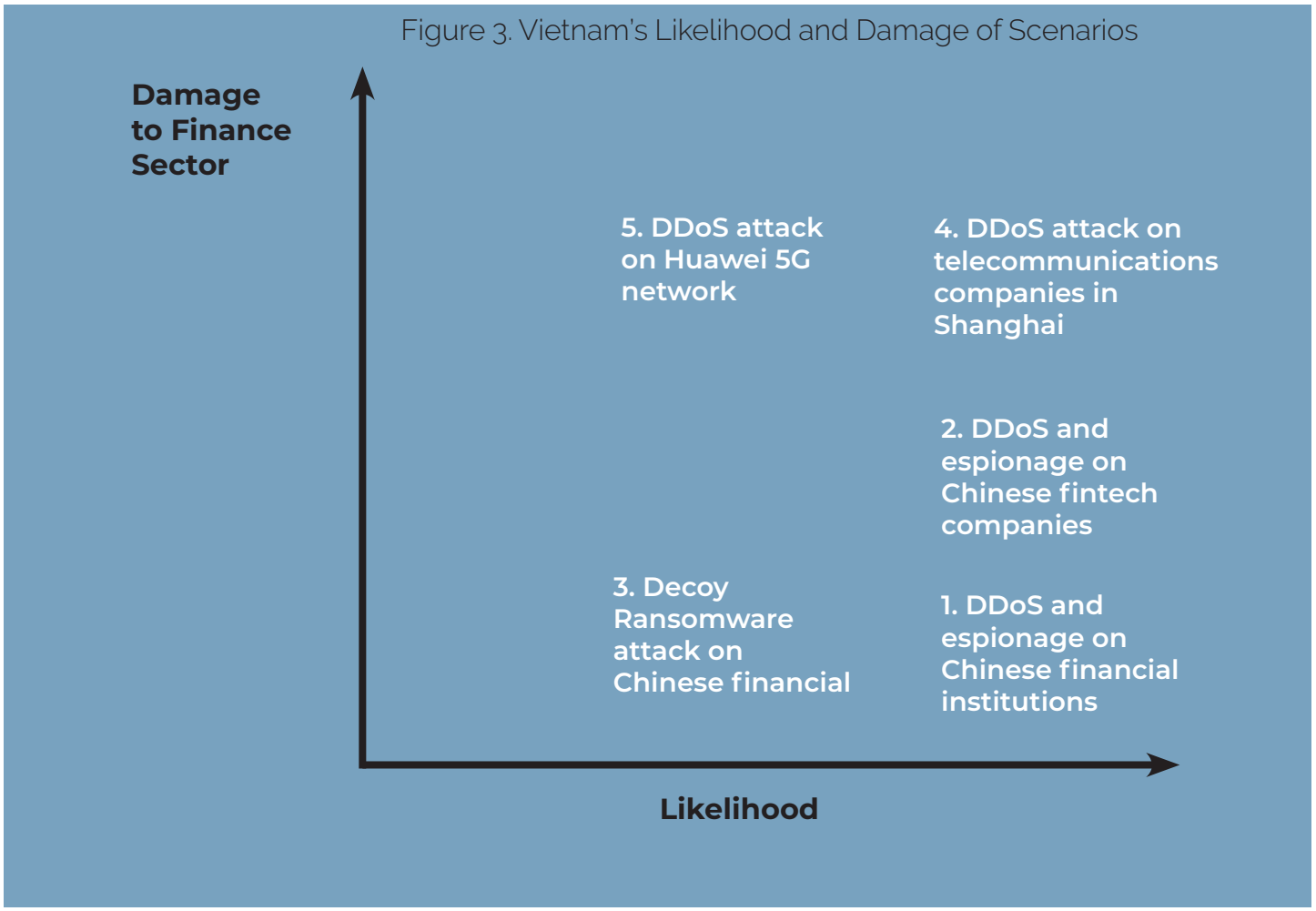
Vietnam is building up the capability to defend itself. Cyber warfare would be there because Vietnam knows they are vulnerable.

-Carlyle Thayer, Emeritus Professor of the University of New South Wales Canberra

Intent Scenario and Likelihood

There are five potential scenarios given Vietnam's economic ties to China and its desire to avoid escalating cyber conflicts into a kinetic conflict. [110] Scenario 4 (DDoS on telecommunications companies in Shanghai), Scenario 2 (DDoS and espionage on Chinese fintech companies), and Scenario 1 (DDoS and espionage on Chinese financial institutions) are the most likely to occur within the next 5-10 years. DDoS and espionage attacks on financial institutions are already being conducted. Scenario 4 (DDoS on critical network infrastructure) would cause the most serious damage.

Figure 3. Vietnam's Likelihood and Damage of Scenarios



1. DDoS and espionage on Chinese defense enterprises and financial institutions

APT32, a Vietnamese state-sponsored hacking group, may attack Chinese state-owned defense enterprises--Aviation Industry Corporation of China (AVIC) or China State Shipbuilding Corporation (CSSC)--and state-owned financial institutes that fund the development of defense technologies. The attack would be a warning to China for its increased military activities in the South China Sea. The attackers may steal state-of-the-art technologies, ongoing project documents, and personal information from defense companies. They may also steal and encrypt documents related to loans to defense companies from financial institutions to disrupt the defense projects. In addition, the attackers may change ID information of leadership personnel to prevent them from accessing the system, and steal transaction history. All such attacks would spill over to the financial sector as financial websites may be changed and access to the financial systems may be disrupted.

2. DDoS and espionage on Chinese fintech companies

A Vietnamese state-sponsored hacking group may limit users' access to their accounts on Fintech platforms like Alipay and Tenpay and steal their financial information. By attacking Fintech companies, mobile transactions and financial services would be paralyzed. According to one estimate, 79.3% of smartphone users in China scan and swipe at the point of sale in 2021.[111] Disruptive/destructive attacks on fintech companies not only pose economic damage caused by the suspension of transactions, but also raise security issues in China's fintech companies, reducing corporate credibility and having a long-term negative impact.

3. Decoy ransomware attack on Chinese financial institutions

A ransomware may block financial institutions' access to a network. The ransomware may spread through phishing emails that contain malicious attachments or infected software apps and encrypt data across the operating system. It will pretend to require Chinese financial institutions to decrypt and restore data. However, unlike usual ransomware attacks, the ransomware attack conducted by the state-sponsored hacking group will not be designed to make money. It will aim to cause damage to Chinese financial institutions.

4. DDoS attack on telecommunication companies in Shanghai

In order to retaliate cyberattacks by Chinese cyber forces, a Vietnamese state-sponsored hacking group may carry out DDoS attacks on the websites and networks of telecommunications companies in Shanghai where allegedly the 61398 unit, one of the PLA's cyber units, is located. With DDoS attacks on telecommunications companies such as China Mobile, China Telecom, and China Unicom, financial institutions in Shanghai that use service from those telecommunications companies suffer delayed access to their websites and delayed

5. DDoS attack on Huawei 5G network

A Vietnamese state-sponsored hacking group may carry out DDoS attacks using the vulnerabilities of Huawei equipment. Vietnam is the only Southeast Asian state which does not use Huawei equipment for security concerns. Its largest wireless carrier Viettel has developed 5G equipment and competes with Huawei for 5G equipment exports. The hackers may attack Huawei equipment to expose its vulnerabilities so that Viettel can gain advantage in the 5G equipment competition. Financial institutions both in and out of China which use Huawei equipment may be compromised by this attack.

Capability Indicators

Overview of Vietnam

Vietnam's private sector and government capabilities are still developing, but the underground/criminal capabilities are developed. Vietnam is increasing its investment in all three types of capabilities and is modely some of its cyber activity after China with increasing activity of APT groups and underground actors.[112] Vietnam is the second most targeted ASEAN nation state [113] and is emerging as a hotspot for blocked suspicious web activity.[114]

PRIVATE SECTOR	**Global Top 100 Technology Firms**	**Evidence of Private Sector Tech**	**High Tech Exports**	**Education**	**Skilled Employees in the Tech Industry**	
	Lacking	*Developing*	*Developing*	*Developed*	*Developing*	
GOVERNMENT	**Cybersecurity Law/Doctrine**	**Intelligence Agency**	**Cyber Military Doctrine**	**Cyber Military Staffing**	**State Sponsored Actors**	**National Cyber Command**
	Developing	*Developed*	*Lacking*	*Developing*	*Developed*	*Developing*
UNDERGROUND AND MALICIOUS	**Domestic Repression**	**Purchase of Malware**	**Underground Network of Cyber Criminals**			
	Developed	*Developing*	*Developed*			

*** Refer to Appendix 6 for more detailed analysis on Vietnam's capabilities **

Private Sector Capabilities:

Vietnam has limited private sector capabilities though it is increasing investment and the sector can be expected to grow over the next 5-10 years.

Vietnam has no firms that rank in global top[115] 100 technology firms lists[116] and is a communist state with mostly state-owned enterprises (SOEs). It imports much of its hardware, software, and services.[117] However, many international companies see potential in Vietnam, and foreign investment is increasing in Vietnam[118]. Vietnam is also the only Southeast Asian nation state that is developing its own 5G technology: Viettel is working in cooperation with Sweden's Ericsson. Vietnam's high technology export has been growing at a steady rate from $3013.19 million in 2008 to $101,534.39 million in 2020.[119]

Vietnam is investing in domestic cybersecurity education. National information security programs for primary and secondary education were first passed in 2015. In January 2021, a new requirement for 10th to 12th grade to have a fundamental understanding of cybersecurity, cyberspace, and related laws were also created.[121] There are college, postgraduate, and doctoral level programs for cybersecurity as well,[122] and further development through partnerships with foreign universities are being pursued. [123]

In the private sector, global technology giants are also assisting in cybersecurity education development. Samsung and LG launched their own programs--which includes education on technology--to educate Vietnamese workers to work at their companies. [124] The state is experiencing a labor shortage as the World Bank reported in October 2021 that the digital sector growth is hampered by shortage of skilled workers. [125]

Government Capabilities:

The Vietnamese government has strong capabilities, especially when looking at its state-sponsored actor APT32. It began introducing cyber laws in the 2010s and established a national cyber command in 2018. The Law on Cyber-Information Security (LCIS), the first-ever comprehensive Vietnamese cybersecurity law, was passed in 2015.[126] Vietnam's national cyber command's cyber offensive unit, Force 47, reportedly has 10,000 members.[127] However, its only goal and doctrine are to manipulate online discourse and silence dissent to strengthen the Communist Party.[128]

Vietnam's General Department of Defense Intelligence focuses on executing intel activities at the strategic level, advises the Minister of National Defense and General Chief of Staff on intel operations, and instructs and guides military intelligence and reconnaissance networks.[129]

Its strongest government cyber capability is its state-sponsored cyber attacks on foreign multinational organizations based in Vietnam--especially automotive companies and media outlets--are increasing.[130] Most prominently, APT32--also known as OCEANLOTUS--is associated with the Vietnamese government and has supported the government's strategic interests by attacking anti-government media outlets, foreign competitors of Vietnam's domestic automobile manufacturer,[131] It has also been accused of cyber espionage as well as mass digital surveillance and attacks against ASEAN, other states in Asia, media outlets, human rights groups, and civil society.[132]

Underground and Malicious Capabilities:

The underground and criminal capabilities are well developed as domestic repression and internet censorship pushed many Vietnamese internet users to the Deep Web and Dark Web, creating an underground network of cyber criminals. In the 2021 Freedom House report, Vietnam scored a 19 out of 100, demonstrating strong domestic repression and the lack of freedom.[133] Internet censorship laws are evident and increasingly used to silence anti-state discourse. [134]

There is some evidence that Vietnamese hackers are purchasing malware as reported by Google and McAfree in 2010 and a Vietnam-based Associated Press reporter in 2013. Malware for spying and DoS attacks appear to have been bought.[135]

Vietnam is reportedly one of the top five cybercrime hotspots in the world. Vietnamese hackers have stolen up to 200 million personal records from the West in 2014. The government has also been recruiting domestic hackers to spy on media outlets and anti-state activists. [136] The Insights Report revealed that Dark Web users are now looking for more information on cryptocurrency and cybercrime opportunities.[137]

Conclusion

04

Through analysis of existing cyber power indices, the Capstone team developed a bespoke cyber power index with 14 capability indicators that can be used to determine the potential for a state to emerge as a cyber power in the next 5-10 years. The custom index established three emerging cyber powers: the Gulf States (Qatar, UAE, Saudi Arabia), India, and Vietnam. All three states are shown to have developed or to be developing key sectors of their private, government, and malicious sectors that would lead them to become relevant players in the global cyber arena.

From these selections, the team hypothesized several potential scenarios under which these countries would develop the intent to carry out disruptive, destructive, or espionage attacks that would directly or indirectly damage financial institutions. Finally, the bespoke index provides a methodology for the Global Financial Institution to identify future emerging cyber powers beyond the 5-10 year timeline and the three identified states.

I do truly believe that the internet in 5 years will be more fragmented and balkanized. Authoritarian regimes will wall off more. What does that mean for threats?

Harder for threats to spread and cascade. The free flow of data and commerce will be constricted. The Internet will be less efficient and open.

Crime as a service will escalate to conflict as a service.

-Neal Pollard, Former CISO, UBS

End Notes

04

1 "New Index Ranks Ability of G20 Nations to Withstand Cyber Attacks, Harness Digital Environment". The 1st paragraph.
2 "New Index Ranks Ability of G20 Nations to Withstand Cyber Attacks, Harness Digital Environment". The 4th paragraph.
3 "New Index Ranks Ability of G20 Nations to Withstand Cyber Attacks, Harness Digital Environment". The 4th paragraph.
4 "New Index Ranks Ability of G20 Nations to Withstand Cyber Attacks, Harness Digital Environment". The 5-6th paragraph.
5 Hathaway, Melissa, ?Chris Demchak, Jason Kerben, Jennifer McArdle, Francesca Spidalieri, "Cyber Readiness Index 2.0," Potomac Institute for Policy Studies, November 2015, 3-4.
6 Hathaway et. al, "Cyber Readiness Index 2.0," 4.
7 "ITU Publications." ITU, https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E/. Accessed 7 April 2022.
8 Voo, Julia, Irfan Hemani, Simon Jones, Winnona DeSombre, Dan Cassidy and Anina Schwarzenbach, "National Cyber Power Index 2020," Harvard Kennedy School Belfer Center, September 2020, 1.
9 Voo et. al, "National Cyber Power Index 2020," 2.
10 Voo et. al, "National Cyber Power Index 2020," 11.
11 "Cyber Capabilities and National Power: A Net Assessment," 6.
12 "Cyber Capabilities and National Power: A Net Assessment," 3.
13 "Cyber Capabilities and National Power: A Net Assessment," 9-12.
14 Iasiello, Emilio. "Don't Rely on Tiered Rankings to Measure Cyber Power." OODA Loop, 13 July 2021, https://www.oodaloop.com/archive/2021/07/13/dont-rely-on-tiered-rankings-to-measure-cyber-power/. Accessed 7 April 2022.
15 "Cyber Capabilities and National Power: A Net Assessment."
16 Interview with Erinmichelle Perri, CISO of NYT
17 Inverview with Luke McNamara
18 Interview with Michael Daniel, President and CEO of Cyber Threat Alliance
19 "Thomson Reuters Top 100 Global Tech Leaders." Thomson Reuters, https://www.thomsonreuters.com/en/products-services/technology/top-100.html. Accessed 7 April 2022.
20"Top 100 Digital Companies List." Forbes, https://www.forbes.com/top-digital-companies/list/. Accessed 7 April 2022.
21 Franklin Kramer, Stuart H. Starr, & Larry Wentz. (2009). Cyberpower and National Security: Vol. 1st ed. Potomac Books.
22 Myriam Dunn Cavelty. (2018). Europe's cyber-power. European Politics and Society: Vol. 9, Issue 3. https://doi.org/10.1080/23745118.2018.1430718
23 Voo, Julia, Irfan Hemani, Simon Jones, Winnona DeSombre, Dan Cassidy and Anina Schwarzenbach, "National Cyber Power Index 2020," Harvard Kennedy School Belfer Center, September 2020, 16.
24 Voo et. al, "National Cyber Power Index 2020," 17.
25 Voo et. al, "National Cyber Power Index 2020," 17.
26 Voo et. al, "National Cyber Power Index 2020," 18.
27 Voo et. al, "National Cyber Power Index 2020," 19.
28 Klein, Abigail. "How Israel became the world's cyber powerhouse." ISRAEL21c, 29 November 2021, https://www.israel21c.org/how-israel-became-the-worlds-cyber-powerhouse/
29 Times of Israel. "Report: Israel pushed NSO spyware to Gulf states to help track dissidents." Times of Israel, August 2020, https://www.timesofisrael.com/report-israel-pushed-nso-spyware-to-gulf-states-to-help-track-dissidents/.
30 Pagliery, Jose. "The inside story of the biggest hack in history." CNN Business, 5 August 2015, https://money.cnn.com/2015/08/05/technology/aramco-hack/
31 Cox, Joseph. "US Company Sold Zero-Click Hacking Tool to UAE Spy Operation." VICE, 14 September 2021, https://www.vice.com/en/article/3aq9a5/us-company-sold-zero-click-exploit-project-raven-uae
32 Perlroth, Nicole. "Hacking Group Claims N.S.A. Infiltrated Mideast Banking System (Published 2017)." The New York Times, 15 April 2017, https://www.nytimes.com/2017/04/15/us/shadow-brokers-nsa-hack-middle-east.html
33 Bing, Christopher, and Joel Schectman. "Exclusive: Ex-NSA cyberspies reveal how they helped hack foes of UAE." Reuters, 30 January 2019, https://www.reuters.com/investigates/special-report/usa-spying-raven/
34 Jones, Owen. "Anatomy of a disinformation campaign: The coup that never was." Al Jazeera, 19 May 2020, https://www.aljazeera.com/features/2020/5/19/anatomy-of-a-disinformation-campaign-the-coup-that-never-was.
35 Pinnell, Owen. "The online war between Qatar and Saudi Arabia." BBC, 3 June 2018, https://www.bbc.com/news/blogs-trending-44294826.
36 "Qatar state news agency's hacking linked to Riyadh." Al Jazeera, 4 June 2018, https://www.aljazeera.com/news/2018/6/4/qatar-state-news-agencys-hacking-linked-to-riyadh.
37 Kirchgaessner, Stephanie. "Saudis behind NSO spyware attack on Jamal Khashoggi's family, leak suggests." The Guardian, 19 July 2021, https://www.theguardian.com/world/2021/jul/18/nso-spyware-used-to-target-family-of-jamal-khashoggi-leaked-data-shows-saudis-pegasus.
38 "Hackers reportedly demand $50m from Saudi Aramco over data leak." BBC, 22 July 2021, https://www.bbc.com/news/business-57924355. Accessed 7 April 2022.
39 Gulf scenarios and analysis cite conversations with cyber, technology, and regional experts including, Colin Ahern, Deputy CISO to New York City; Greg Rattray, former CISO to J.P Morgan and current Partner at Next Peak, a cybersecurity risk management firm; and Naif Alkhathran, a Saudi-born regional researcher of the Gulf states.

40 Jones, Marc. "Analysis | Hacking, bots and information wars in the Qatar spat." The Washington Post, 7 June 2017,https://www.washingtonpost.com/news/monkey-cage/wp/2017/06/07/hacking-bots-and-information-wars-in-the-qatar-spat/. Accessed 27 March 2022.
41 Mazzetti, Mark. "The Battle for the World's Most Powerful Cyberweapon." The New York Times, 31 January 2022, https://www.nytimes.com/2022/01/28/magazine/nso-group-israel-spyware.html. Accessed 29 March 2022.
42 Bing, Christopher, and Joel Schectman. "Exclusive: Ex-NSA cyberspies reveal how they helped hack foes of UAE." Reuters, 30 January 2019, https://www.reuters.com/investigates/special-report/usa-spying-raven/. Accessed 29 March 2022.
43 "Qatar: Mandatory Covid-19 tracking app raises serious privacy & security concerns, say NGOs." Business & Human Rights Resource Centre, https://www.business-humanrights.org/en/latest-news/qatar-mandatory-covid-19-tracking-app-raises-serious-privacy-security-concerns-say-ngos/. Accessed 29 March 2022.
44 Interviews with Dr. Greg Rattray and Naif Alkhathran.
45 CrowdStrike. CrowdStrike 2022 Global Threat Report. 2022
46 Interview with Colin Ahern
47 "Hackers reportedly demand $50m from Saudi Aramco over data leak." BBC, 22 July 2021, https://www.bbc.com/news/business-57924355. Accessed 7 April 2022.
48 Hubbard, Ben. "Yemeni Rebel Attack Sets Saudi Oil Facility Ablaze." The New York Times, 25 March 2022, https://www.nytimes.com/2022/03/25/world/middleeast/yemen-attack-saudi-arabia.html.
49 Neuman, Scott, et al. "Attack On Saudi Oil Facilities Makes Oil Prices Spike." NPR, 16 September 2019, https://www.npr.org/2019/09/16/761118726/oil-prices-jump-following-drone-attack-on-saudi-oil-facility.
50 "High-technology exports (current US$) - Qatar." The World Bank, The World Bank, https://data.worldbank.org/indicator/TX.VAL.TECH.CD?locations=QA&most_recent_value_desc=true. Accessed 14 April 2022.
51 "Qatar National Vision 2030." Government Communications Office, https://www.gco.gov.qa/en/about-qatar/national-vision2030/. Accessed 14 April 2022.
52 "Ranking in the Gulf Cooperation Council region for quality of math and science of education in 2018, by country." Statista, Statista, https://www.statista.com/statistics/943548/gcc-quality-of-math-and-science-of-education-ranking-by-country/. Accessed 14 April 2022.
53 "Country capacity to retain talent - Ranking of the 20 countries with the lowest emigration of skilled professionals in 2017-2018." Statista, Statista, https://www-statista-com.ezproxy.cul.columbia.edu/statistics/264654/ranking-of-the-20-countries-with-the- lowest-emigration-of-skilled-professionals/. Accessed 14 April 2022.
54 Qatar. United Nations Institute for Disarmament Research, March 2021. Accessed 14 April 2022.
55 Amlot, Matthew, "Qatar hired ex-CIA, US military officials to hack Republican activist Broidy: Reports, Al Arabiya News, 1 July 2020, https://english.alarabiya.net/News/gulf/2020/07/01/Qatar-hired-former-CIA-US-military-officials-to-hack-Republican-activist-Reports. Accessed 18 April 2022.
56 Valentino-DeVries, Jennifer, and Danny Yadron. "Cataloging the World's Cyberforces - WSJ." Wall Street Journal, 11 October 2015, https://www.wsj.com/articles/cataloging-the-worlds-cyberforces-1444610710. Accessed 14 April 2022.
57 Forbes, https://www.forbes.com/top-digital-companies/list/#tab:rank. Accessed 7 April 2022.
58 "ICT spending in UAE will reach US$23bn by 2024, says GlobalData." GlobalData, GlobalData Plc, 12 March 2020, https://www.globaldata.com/ict-spending-in-uae-will-reach-us23bn-by-2024-says-globaldata/. Accessed 14 April 2022.
59 "High-technology exports (current US$) - United Arab Emirates | Data." World Bank Data, https://data.worldbank.org/indicator/TX.VAL.TECH.CD?locations=AE. Accessed 14 April 2022.
60 Ranking in the Gulf Cooperation Council region for the digital skills of the current workforce in 2019, by country." Statista, Statista, https://www.statista.com/statistics/1227354/gcc-ranking-by-country-for-digital-skills-of-workforce/. Accessed 14 April 2022.
61 McLaughlin, Jenna. "Deep Pockets, Deep Cover." Foreign Policy, Foreign Policy, 21 December 2017, https://web.archive.org/web/20190614155213mp_/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/. Accessed 14 April 2022.
62 Reuters Staff, "UAE arranged for hacking of Qatar government sites, sparking diplomatic row: Washington Post," Reuters, 16 July 2017, https://www.reuters.com/article/us-usa-qatar-report/uae-arranged-for-hacking-of-qatar-government-sites-sparking-diplomatic-row-washington-post-idUSKBN1A200H. Accessed 18 April 2022.
63 "https://www.dhs.gov/sites/default/files/publications/ia/ia_geopolitical-impact-cyber-threats-nation-state- actors.pdf." Commodification of Cyber Capabilities: A Grand Cyber Arms Bazaar, 2019, https://www.dhs.gov/sites/default/files/publications/ia/ia_geopolitical-impact-cyber-threats-nation-state-actors.pdf. Accessed 14 April 2022.
64 "Top 100 Digital Companies List." Forbes, https://www.forbes.com/top-digital-companies/list/#tab:rank. Accessed 7 April 2022.
65 "Russian cyber security firm Kaspersky opens new office in Saudi Arabia." Arab News, 20 April 2022, https://www.arabnews.com/node/2067031/business-economy
66 "High-technology exports (current US$) - Saudi Arabia | Data." World Bank Data, https://data.worldbank.org/indicator/TX.VAL.TECH.CD?locations=SA. Accessed 14 April 2022.
67 "The Talent Shift." Korn Ferry, https://www.kornferry.com/content/dam/kornferry/docs/pdfs/KF-Talent-Shift-Country-Report-Saudi-Arabia-Digital.pdf. Accessed 14 April 2022.
68 "Saudi Arabia | UNIDIR." Cyber Policy Portal, https://cyberpolicyportal.org/en/states/saudiarabia. Accessed 14 April 2022.
69 "Saudi Arabia: Freedom in the World 2021 Country Report." Freedom House, https://freedomhouse.org/country/saudi-arabia/freedom-world/2021. Accessed 14 April 2022.
70 Sebenius, Alyza. "Saudi Arabia Outsources Cyber Arsenal, Buys Spyware, Experts Say." Claims Journal, 28 January 2020, https://www.claimsjournal.com/news/international/2020/01/28/295217.htm. Accessed 14 April 2022.
71 "Digital Souks: A Glimpse into the Middle Eastern and North African Underground." Trend Micro, Trend Micro, https://documents.trendmicro.com/assets/white_papers/wp-middle-eastern-north-african-underground.pdf. Accessed 14 April 2022.
72 BBC. India-China dispute: The border row explained in 400 words. 25 January 2021.
https://www.bbc.com/news/world-asia-53062484
73 Aljazeera. China admits it lost four soldiers in the 2020 India border clash. 19 February 2021.
74 Russel, Daniel and Berger, Blake. Weaponizing the Belt and Road Initiative. Asia Society Policy Institute.
https://asiasociety.org/sites/default/files/2020-09/Weaponizing%20the%20Belt%20and%20Road%20Initiative_0.pdf
75 "Cyber attacks: India among top 3 most-affected nations in Asia." The Statesman, 24 February 2022, https://www.thestatesman.com/technology/cyber-attacks-india-among-top-3-affected-nations-asia-1503048173.html. Accessed 12 April 2022.
76 Mantri,, Kalpesh, et al. Operation SideCopy. Quick Heal Technologies Limited, India, 2020.
77 Ghosh, Soumik. "The biggest data breaches in India." CSO Online, https://www.csoonline.com/article/3541148/the-biggest-data-breaches-in-india.html. Accessed 12 April 2022.
78 Ghosh, Soumik. "The biggest data breaches in India." CSO Online, https://www.csoonline.com/article/3541148/the-biggest-data-breaches-in-india.html. Accessed 12 April 2022.
79 Ghosh, Soumik. "The biggest data breaches in India." CSO Online, https://www.csoonline.com/article/3541148/the-biggest-data-breaches-in-india.html. Accessed 12 April 2022.
80 Shih, Gerry. "Indian activist charged with terrorism was targeted by hackers linked to prominent cyber espionage attacks, new report finds." The Washington Post, 10 February 2022, https://www.washingtonpost.com/world/2022/02/10/bhima-koregaon-india-sentinelone/. Accessed 12 April 2022.

81 "Cyberattacks from groups in India targeted China, Pak & Nepal, claims Chinese media." The Economic Times, 5 November 2021, https://economictimes.indiatimes.com/news/defence/cyberattacks-from-groups-in-india-targeted-china-pak-nepal-claims-chinese-media/articleshow/87536155.cms. Accessed 12 April 2022.
82 "India bought Pegasus spyware as part of $2bn arms deal: NYT." Al Jazeera, 29 January 2022, https://www.aljazeera.com/news/2022/1/29/india-bought-israeli-pegasus-spyware-as-part-of-weapon-deal-nyt. Accessed 12 April 2022.
83 Elgan, Mike. Maritime Cybersecurity: A Rising Tide Lifts all Boats.
https://securityintelligence.com/articles/maritime-cybersecurity-rising-tide/
84 Sanger, David and Schmal, Emily. China Appears to Warn India: Push Too Hard and the Lights Could Go Out.
https://www.nytimes.com/2021/02/28/us/politics/china-india-hacking-electricity.html
85 Sanger, David and Schmall, Emily. China Appears to Warn India: Push Too Hard and the Lights Could Go Out.
https://www.nytimes.com/2021/02/28/us/politics/china-india-hacking-electricity.html
86 Rising, David. Chinese Hackers Reportedly Target India's Power Grid.
https://techxplore.com/news/2022-04-chinese-hackers-reportedly-india-power.html
87 "Thomson Reuters Top 100 Global Tech Leaders." Thomson Reuters, https://www.thomsonreuters.com/en/products-services/technology/top-100.html. Accessed 10 April 2022, or "Top 100 Digital Companies List." Forbes, https://www.forbes.com/top-digital-companies/list/#tab:rank. Accessed 10 April 2022.
88 "India - Information and Communication Technology." International Trade Administration, 22 October 2021, https://www.trade.gov/country-commercial-guides/india-information-and-communication-technology. Accessed 10 April 2022.
89 "India High tech exports, percent of manufactured exports - data, chart | TheGlobalEconomy.com." The Global Economy, https://www.theglobaleconomy.com/India/High_tech_exports_percent_of_manufactured_exports/. Accessed 10 April 2022.
90 "High tech exports, percent of manufactured exports by country, around the world | TheGlobalEconomy.com." The Global Economy, https://www.theglobaleconomy.com/rankings/High_tech_exports_percent_of_manufactured_exports/. Accessed 10 April 2022.
91 "India, UK discuss steps in implementing Enhanced Cyber Security Partnership | Business." Devdiscourse, 12 April 2022, https://www.devdiscourse.com/article/business/2000701-india-uk-discuss-steps-in-implementing-enhanced-cyber-security-partnership. Accessed 14 April 2022.
92 Coursera. The Global Skills Report. COURSERA, 2021.
93 ITUPublications. Global Cybersecurity Index (GCI). ITUPublications, 2018.
94"National Cyber Security Policy — Vikaspedia." Vikaspedia, https://vikaspedia.in/e-governance/national-e-governance-plan/national-cyber-security-policy. Accessed 10 April 2022.
95 "Hackers from Delhi reportedly launching cyberattacks against China, Pakistan." The New Indian Express, 20 November 2021, https://www.newindianexpress.com/nation/2021/nov/20/hackers-from-delhi-reportedly-launching-cyberattacks-against-china-pakistan-2386047.html. Accessed 10 April 2022.
96 "India: Freedom in the World 2021 Country Report." Freedom House, https://freedomhouse.org/country/india/freedom-world/2021. Accessed 10 April 2022.
97 Soni, Paroma, and Jon Allsop. "Online censorship is growing in Modi's India." Columbia Journalism Review, 14 December 2021, https://www.cjr.org/investigation/modi-censorship-india-twitter.php. Accessed 10 April 2022.
98 Duggal, Pavan. "Pegasus Controversy: Where Does India Stand On Cyber Laws." Outlook India, 22 July 2021, https://www.outlookindia.com/website/story/opinion-pegasus-controversy-where-does-india-stand-on-cyber-laws/389018. Accessed 10 April 2022.
99 Federal News Network. "Recent developments surrounding South China Sea." April 26, 2020, https://federalnewsnetwork.com/government-news/2020/04/recent-developments-surrounding-the-south-china-sea-30/. Accessed 7 April 2022.
100 Council on Foreign Relations. "Territorial Disputes in the South China Sea." April 5, 2022, https://www.cfr.org/global-conflict-tracker/conflict/territorial-disputes-south-china-sea. Accessed 7 April 2022.
101 Insikt Group. "Chinese State-Sponsored Cyber Espionage Activity Supports Expansion of Regional Power and Influence in Southeast Asia." December 8, 2021, https://go.recordedfuture.com/hubfs/reports/cta-2021-1208.pdf. Accessed 7 April 2022.

102 Rising, David. "Report: Chinese hackers targeted Southeast Asian nations." AP News, 8 December 2021, https://apnews.com/article/technology-business-indonesia-beijing-asia-bca3e5785c03cb4d7a1e3052f545a922. Accessed 23 April 2022.
103 Lakshmanan, Ravie. "Chinese Hackers Target Major Southeast Asian Telecom Companies." The Hacker News, 3 August 2021, https://thehackernews.com/2021/08/chinese-hackers-target-major-southeast.html. Accessed 23 April 2022.
104 Arghire, Ionut. "Chinese Cyberspies Target Military Organizations in Asia With New Malware." SecurityWeek, 29 April 2021, https://www.securityweek.com/chinese-cyberspies-target-military-organizations-asia-new-malware. Accessed 23 April 2022.
105 Arghire, Ionut. "China-Linked 'Cycldek' Hackers Target Vietnamese Government, Military." SecurityWeek, 5 April 2021, https://www.securityweek.com/china-linked-cycldek-hackers-target-vietnamese-government-military. Accessed 23 April 2022.
106 Osborne, Charlie. "Chinese hackers take down Vietnam airport systems." ZDNet, 1 August 2016, https://www.zdnet.com/article/chinese-hackers-take-down-vietnam-airport-systems/. Accessed 23 April 2022.
107 Thayer, Carl, and Catherine Putz. "Did Vietnamese Hackers Target the Chinese Government to Get Information on COVID-19?" The Diplomat, 4 May 2020, https://thediplomat.com/2020/05/did-vietnamese-hackers-target-the-chinese-government-to-get-information-on-covid-19/. Accessed 23 April 2022.
108 Carr, Nick. "Cyber Espionage is Alive and Well: APT32 and the Threat to Global Corporations." Mandiant, 14 May 2017, https://www.mandiant.com/resources/cyber-espionage-apt32. Accessed 23 April 2022.
109 Newman, Lily Hay. "How the APT32 Hacking Group Operates." WIRED, 24 May 2017, https://www.wired.com/2017/05/close-look-notorious-apt32-hacking-group-action/. Accessed 23 April 2022.
110 Carlyle Thayer, Emeritus Professor of the University of New South Wales Canberra, said in an interview (February 22, 2022) "Vietnam has a very defense-oriented strategy. Given the asymmetric differences in defense capabilities and political and economic ties as socialist countries, Vietnam takes a defensive and prudent posture. Even though cyber is seen as an asymmetric weapon, it is not in Vietnam's interest to provoke China because that will lead to 100 years of pressure and retaliation."
111 Engen, John. "Why China's mobile payments revolution matters for US bankers." American Banker, https://www.americanbanker.com/news/why-chinas-mobile-payments-revolution-matters-for-us-bankers. Accessed 7 April 2022.
112Dorfman, Zach, and Breanne Deppisch. "Cyber Threat Assessment: Rise of the Rest." The Aspen Institute, https://www.aspeninstitute.org/programs/threat-assessment-2019/. Accessed 7 April 2022.
113Snowden, Edward. "Cybersecurity in Southeast Asia." Asia Centre, https://centreasia.eu/wp-content/uploads/2018/12/NotePre%CC%81sentation-AngRaska-Cybersecurity_180518.pdf. Accessed 7 April 2022.
114"Cybersecurity Policy in ASEAN Countries." ResearchGate, https://www.researchgate.net/profile/Jirapon-Sunkpho-2/publication/324106226_Cybersecurity_Policy_in_ASEAN_Countries/links/5abdc2ea45851584fa6fca37/Cybersecurity-Policy-in-ASEAN-Countries.pdf. Accessed 7 April 2022.
115 "Thomson Reuters Top 100 Global Tech Leaders." Thomson Reuters, https://www.thomsonreuters.com/en/products-services/technology/top-100.html. Accessed 7 April 2022.

116 "Top 100 Digital Companies List." Forbes, https://www.forbes.com/top-digital-companies/list/. Accessed 7 April 2022.
117"Vietnam - Information and Communication Technologies." International Trade Administration, 15 September 2021, https://www.trade.gov/country-commercial-guides/vietnam-information-and-communication-technologies. Accessed 7 April 2022.
118"The paradoxes of private sector development in Vietnam." East Asia Forum, 4 June 2020, https://www.eastasiaforum.org/2020/06/04/the-paradoxes-of-private-sector-development-in-vietnam/. Accessed 7 April 2022.
119 "Vietnam High tech exports - data, chart | TheGlobalEconomy.com." The Global Economy, https://www.theglobaleconomy.com/Vietnam/High_tech_exports/. Accessed 7 April 2022.
120 ITU Vietnam National Cybersecurity Education Capacity Assessment, p. 12
121 "Cybersecurity to be included in high school curriculum | Society | Vietnam+ (VietnamPlus)." Vietnam Plus, 20 January 2021, https://en.vietnamplus.vn/cybersecurity-to-be-included-in-high-school-curriculum/195015.vnp. Accessed 7 April 2022.
122 ITU Vietnam National Cybersecurity Education Capacity Assessment, p. 4-10.
123 "Finnish cyber security education goes to Vietnam." Good News from Finland, https://www.goodnewsfinland.com/finnish-cyber-security-education-goes-vietnam/. Accessed 7 April 2022.
124Tibken, Shara. "Schooling Vietnam: How tech companies are training the next wave of workers." CNET, A RED VENTURES COMPANY, 22 July 2015, https://www.cnet.com/tech/tech-industry/schooling-vietnam-how-tech-companies-are-training-the-next-wave-of-workers/. Accessed 7 April 2022.
125 Morisset, Jacques. "Digital transformation in Vietnam: Skills must transform too." World Bank Blogs, 8 October 2021, https://blogs.worldbank.org/eastasiapacific/digital-transformation-vietnam-skills-must-transform-too. Accessed 7 April 2022.
126 Jirapon Sunkpho, Sarawut Ramjan, Chaiwat Ottamakorn, "Cybersecurity Policy in ASEAN Countries," Information Institute Conferences, Las Vegas, Nevada, March 26-28, 2018.
127 "Vietnam Rises as Cyberthreat." Dark Reading, 5 June 2019, https://www.darkreading.com/attacks-breaches/vietnam-rises-as-cyberthreat. Accessed 7 April 2022.
128 "How The Vietnamese State Uses Cyber Troops to Shape Online Discourse." ISEAS-Yusof Ishak Institute, 3 March 2021, https://www.iseas.edu.sg/wp-content/uploads/2021/02/ISEAS_Perspective_2021_22.pdf. Accessed 7 April 2022.
129"General Department and Agencies." Ministry of National Defence, http://mod.gov.vn/wps/portal/!ut/p/b1/vZNfj6IwFMU_kaEVYfSxUJXSAZR_Ql-IggIFARXB4dMvO9lsNpud8WXj7dNNfu055zZXYEIgsGrf5em-zetqX_7smRytkGnPFYgA2GgrQHQRGS6BAMxmIxD-CVjWJzCVqUTkKYHSs_s7ITDDu4RD1GOkVPVeBW8bdU3sFN3PqEpzoqjO_YZ7bosMju9vDGe7SGK7EemxBEstVipwpXJgncTO4Y. Accessed 7 April 2022.
130 "Vietnam Rises as Cyberthreat." Dark Reading, 5 June 2019, https://www.darkreading.com/attacks-breaches/vietnam-rises-as-cyberthreat. Accessed 7 April 2022.
131 "APT32, SeaLotus, OceanLotus, APT-C-00, Group G0050 | MITRE ATT&CK®." MITRE ATT&CK®, https://attack.mitre.org/groups/G0050/. Accessed 7 April 2022.
132 Ocean Lotus | CFR Interactives, https://www.cfr.org/cyber-operations/ocean-lotus. Accessed 7 April 2022.
133 "Vietnam: Freedom in the World 2021 Country Report." Freedom House, https://freedomhouse.org/country/vietnam/freedom-world/2021. Accessed 7 April 2022.
134 "Vietnam Rises as Cyberthreat." Dark Reading, 5 June 2019, https://www.darkreading.com/attacks-breaches/vietnam-rises-as-cyberthreat. Accessed 7 April 2022.
135"Cataloging the World's Cyberforces - WSJ." Wall Street Journal, 11 October 2015, https://www.wsj.com/articles/cataloging-the-worlds-cyberforces-1444610710. Accessed 7 April 2022.
136Rayman, Noah. "Here Are the World's Five Cybercrime Hotspots | Time." TIME, 7 August 2014, https://time.com/3087768/the-worlds-5-cybercrime-hotspots/. Accessed 7 April 2022.
137"Threat Brief: The Rising Vietnamese Cybercriminal Landscape." IntSights, https://intsights.com/resources/threat-brief-the-rising-vietnamese-cybercriminal-landscape. Accessed 7 April 2022.