

SAME CLOAK, MORE DAGGER: DECODING HOW THE PEOPLE'S REPUBLIC OF CHINA USES CYBERATTACKS



CONTENTS

EXECUTIVE SUMMARY	2
KEY ASSESSMENTS	3
HOW THE PRC COMPETES USING CYBERATTACKS	4
FACTORS INCREASING THE LIKELIHOOD OF TARGETING BY PRC CYBERATTACK OPERATIONS	5
PRIMARY PRC CYBERATTACK TACTICS	6
RECOMMENDATIONS FOR THREAT ANALYSTS AND CISOS	4–7
ANALYTIC FRAMEWORK	9
CORE INTERESTS	9
Security	9
Sovereignty	9
Development	9
AGENCIES AND ACTORS	10
People's Liberation Army (PLA)	10
Ministry of State Security (MSS)	10
Ministry of Public Security (MPS)	11
Cyberspace Administration of China (CAC)	11
Central Propaganda Department (CPD) and the United Front Work Department (UFWD)	11
STRATEGY AND GOALS	12
CASE STUDIES	13
THREATS TO DOMESTIC INTERESTS	13
Key Findings	13
Theme #1: Foreign Information Threats	13
Disrupting Online Petitions to the PRC (April 2011)	13
Disrupting Anti-Censorship Efforts (March 2015)	14
Confronting Persistent Corruption Allegations (2017–2018)	16

Theme #2: The Hong Kong Democracy Movement	17
Disrupting a Referendum on Hong Kong’s Elections (June 2014)	18
Suppressing Hong Kong’s Democracy Movement (September to October 2014)	20
Disrupting Hong Kong’s Pro-Democracy Protests (2019–2020)	21
THREATS TO FOREIGN INTERESTS	23
Key Findings	23
Theme #3: Competing South China Sea Claims	24
Retaliating Against Vietnam’s Assertion of Drilling Rights (2011)	24
Asserting the PRC’s Drilling Rights (2014)	25
Disputing South China Sea Arbitration Favoring the Philippines (July 2016)	27
Disrupting Vietnam’s Aviation Sector (July 2016)	28
Theme #4: Indo-Pacific Competition	29
Preparing for the U.S. Pivot to Asia (2011–2013)	30
Attempting to Intimidate Resistant Politicians in Taiwan (May 2020)	31
Disputing the Border with India (2020–2022)	32
CONCLUSION	35
APPENDIX A: THREAT ACTORS AND ACTIVITY CLUSTERS	36
HURRICANE PANDA	36
1937CN TEAM/GOBLIN PANDA	39
CHENGDU-BASED INDIVIDUALS	41
TONTO TEAM	44
TICK	45
REDECHO	45
APT1	46
ENDNOTES	47

This report is based solely on open source research and analysis and was completed for research purposes. The opinions within do not represent the official opinions of Booz Allen Hamilton, its officers, directors, or shareholders.

AGGREGATION OF OPEN SOURCES

Previously published reports and analysis of individual PRC-aligned operations were critical to developing this report’s findings. These sources are fully cited inline, giving specific credit to their authors. Each of these accounts provided different crucial components of the threat that this report assesses.

CONTEXT

“ Regarding public opinion online, if the right voice does not occupy this space, the wrong voice will spread. In this battlefield without gunpowder smoke, whether we can stand up and win is directly related to national political security, social harmony, and stability.”

– Xi Jinping, President of the People’s Republic of China (PRC), General Secretary of the Chinese Communist Party, and Chairman of the Central Military Commission (2020)¹

“ China presents a prolific and effective cyber-espionage threat, possesses substantial cyber-attack capabilities, and presents a growing influence threat. China’s cyber pursuits and proliferation of related technologies increase the threats of cyber attacks against the US homeland, suppression of US web content that Beijing views as threatening to its internal ideological control, and the expansion of technology-driven authoritarianism around the world.”

– Annual Threat Assessment of the U.S. Intelligence Community, Office of the Director of National Intelligence (2021)²

“ The PRC presents a sophisticated, persistent cyber espionage and attack threat to military and critical infrastructure systems. The PRC seeks to create disruptive and destructive effects—from denial-of-service attacks to physical disruptions of critical infrastructure—to shape decision-making and disrupt military operations at the initial stages and throughout a conflict. The PRC believes these capabilities are even more effective against militarily superior adversaries that depend on information technologies. As a result, the PRC is advancing its cyberattack capabilities and has the ability to launch cyberattacks—such as disruption of a natural gas pipeline for days to weeks—in the United States.”

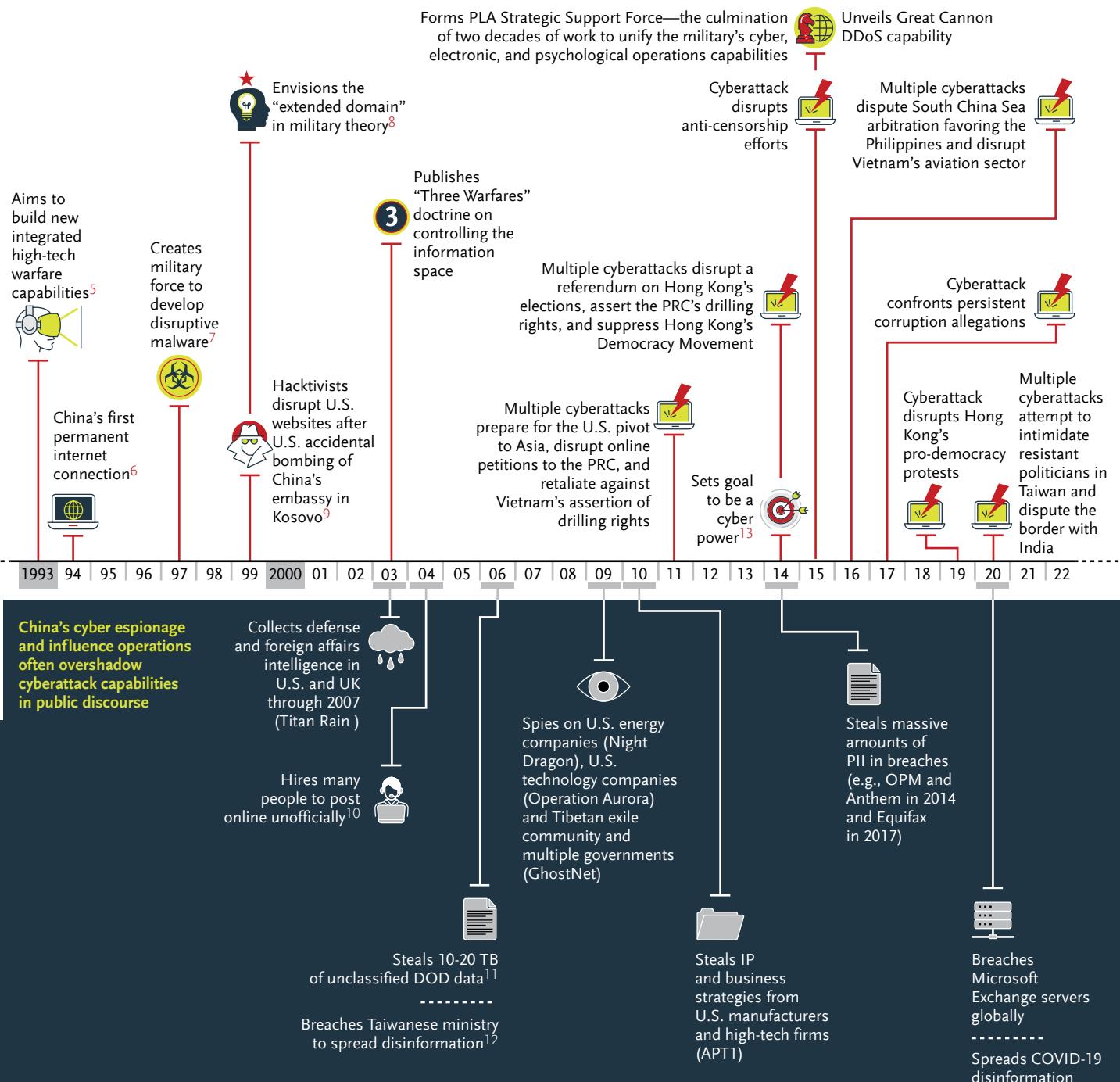
– Military and Security Developments Involving the People’s Republic China: 2021, Office of the Secretary of Defense (2021)³

“ ... for the Chinese [government], like the Russians, like the Americans, cyber is an instrument of power, and we have to imagine to what purposes they would apply that—which immediately points back to the geopolitics of the situation, less so the technology. And so, you have to focus on what the end purposes are, and what they will do with this tool and a range of other tools to essentially achieve those purposes.”

–Chris Inglis, U.S. National Cyber Director (2022)⁴

CHINA'S PATH TO OFFENSIVE CYBER POWER

China's cyberattack capabilities and intentions have evolved over several decades, but 2014–15 seems to have been a major turning point.



EXECUTIVE SUMMARY

Cyberattacks^a by the People's Republic of China (PRC)^b pose a growing threat to U.S. national security. The PRC has a proven pattern of infiltrating the critical infrastructure of its national competitors—including the U.S.—and has demonstrated the ability to conduct disruptive and destructive attacks against key sectors. These attacks have become an integral part of Beijing's playbook to deter and compel its opponents, especially the U.S., while minimizing escalation. While many documented examples of these offensive operations are already public, the lack of cohesive analysis tying these operations to the broader PRC strategy hinders U.S. preparedness for this threat.

This report shows a pattern of PRC cyberattacks over the past decade designed to influence countries, organizations, and people that threaten the PRC's stated core interests. For example, PRC actors likely:

- ★ Knocked the U.S.-based developer platform GitHub offline for enabling targeted subversion of PRC censorship
- ★ Disrupted semiconductor manufacturing in Taiwan after it re-elected a resistant president seeking closer U.S. ties
- ★ Infiltrated American natural gas pipeline operators in response to the U.S. strategic reorientation to the Indo-Pacific

Now, U.S. critical infrastructure organizations and countless companies with global interests face increased risk from PRC cyberattacks. Beijing's intensifying pressure on Taiwan, in particular, greatly raises the likelihood of cyberattacks disrupting critical supply chains.

Organizations that could be impacted by future PRC cyberattacks must make defensive preparations now. To help these organizations prepare, this report offers insights and actionable advice for the following stakeholders:

- ★ **Threat analysts:** This report presents a framework for anticipating and interpreting PRC cyberattacks, relevant adversaries, and their tactics.
- ★ **Chief information security officers (CISOs):** This report identifies factors that increase an organization's risk from PRC cyberattacks and advises on strategies to prepare for this specific threat.

Finally, this report underpins these findings with more than a dozen case studies from the past decade, arming defenders with evidence to sharpen their insights. By understanding the conditions that ignite PRC cyber offensives, organizations can better anticipate when, where, and how those attacks may occur—ensuring they are ready to defend against them.



^a In this report, the term **cyberattack** refers to actions taken via computers that disrupt, deny, degrade, or destroy data, systems, or networks. The term cyberattack does not encompass cyberespionage, the gathering of data via a computer from a target system or network.

^b Consistent with U.S. policy since the 1970s, this report uses the terms "**People's Republic of China**" (PRC) and "**China**" interchangeably to refer to the same entity. Any mention in this report of "China's" actions, intentions, capabilities, and responsibility for cyberattacks refers only to the government of China; it does not refer collectively to people of Chinese heritage, ethnicity, citizenship, or nationality within the PRC or elsewhere.

An oil terminal and tank farm. The U.S. government has publicly attributed natural-gas pipeline operator intrusions to unspecified "Chinese state-sponsored actors."

CASE STUDIES: HOW THE PRC HAS USED CYBERATTACKS TO ADVANCE CORE INTERESTS

CHINA'S
DOMESTIC
INTERESTS



FOREIGN
INFORMATION
THREATS

- ★ Disrupting Online Petitions to the PRC (April 2011)
- ★ Disrupting Anti-Censorship Efforts (March 2015)
- ★ Confronting Persistent Corruption Allegations (2017–2018)



HONG KONG
DEMOCRACY
MOVEMENT

- ★ Disrupting a Referendum on Hong Kong's Elections (June 2014)
- ★ Suppressing Hong Kong's Democracy Movement (September to October 2014)
- ★ Disrupting Hong Kong's Pro-Democracy Protests (2019–2020)

CHINA'S
FOREIGN
INTERESTS



COMPETING
SOUTH CHINA
SEA CLAIMS

- ★ Retaliating Against Vietnam's Assertion of Drilling Rights (2011)
- ★ Asserting the PRC's Drilling Rights (2014)
- ★ Disputing South China Sea Arbitration Favoring the Philippines (July 2016)
- ★ Disrupting Vietnam's Aviation Sector (July 2016)



INDO-PACIFIC
COMPETITION

- ★ Preparing for the U.S. Pivot to Asia (2011–2013)
- ★ Attempting to Intimidate Resistant Politicians in Taiwan (May 2020)
- ★ Disputing the Border with India (2020–2022)

KEY ASSESSMENTS

- ★ Several different elements of China's security apparatus—including the military, state^c security, and internet censorship organizations—likely possess distinct cyberattack capabilities. These capabilities are deployed by operators along a spectrum of acknowledged state affiliation and control, from formal units and militias to contractors, recruited criminals, and voluntary civilian patriotic actors.
- ★ PRC state-aligned threat actors have conducted attacks such as denial-of-service, data destruction, and defacement, as well as hold-at-risk operations targeting industrial control systems (ICS). Targets over the last decade have been within China and abroad—including in the United States and its close partners.
- ★ China's cyberattacks are intended to secure its “core interests,” three officially referenced but not formally defined matters of vital interest to China related to its political system, territory, and economy. Ultimately, advancing these interests serves to sustain the legitimacy and continuity of the Chinese Communist Party (CCP).

^c In this report, the term “state” is used in the political science sense of the totality of permanent power structures representing and governing people in a territory (i.e., used in the sense of “state secrets” or “head of state”), not in the sense of subnational political and territorial units unless being explicitly discussed in the context of the United States.

- ★ The PRC conducts digital espionage worldwide, but its known attack operations have been more focused. These have involved direct threats to the CCP's domestic legitimacy and primacy or geopolitical competition in the Indo-Pacific region. The U.S. is an Indo-Pacific power with many states and territories, large military bases, and substantial trade and investment in the region.¹⁴
- ★ The PRC's cyberattacks frequently mirror its non-cyber policy responses to the same problems, such as harassing counterclaimants to South China Sea territories with substate actors like fishermen and hacktivists.
- ★ China will likely mature its cyberattack capabilities in response to increasing regional and global competition.



HOW THE PRC COMPETES USING CYBERATTACKS

Power dynamics greatly influence the PRC's policy, according to its leadership. This chart summarizes how PRC threat actors have responded to different competitor categories with cyberattacks. Threat analysts can use this chart to identify the circumstances that lead to various kinds of PRC cyberattacks.

COMPETITORS		MAJOR AREAS OF COMPETITION	EVIDENCED CYBER THREATS (# CASE STUDY)
NON-STATE ENTITIES (e.g., technology companies, news outlets, activists)	★ Foreign entities	★ Perceptions of PRC internal affairs, its political system, and the CCP ★ CCP legitimacy and continuity	★ Distributed Denial of Service (DDoS) attacks against offending and enabling entities (#1, #2, #3) ★ National-level blocking and censorship of offending and enabling entities (#2) ★ Coordinated inauthentic social media messaging (#3)
	★ Domestic entities	★ PRC electoral, judicial, and political reform ★ Hong Kong's autonomy	★ DDoS attacks against offending and enabling entities (#4, #5, #6) ★ Weaponized data leaks to embroil competitors in legal, professional, or public controversy (#4) ★ Coordinated inauthentic social media messaging (#6)
STATE-LEVEL ENTITIES	★ PRC has a clear power advantage (e.g., Vietnam, the Philippines)	★ Territorial claims	★ DDoS attacks (#7, #9, #10) ★ Defacements of websites and digital signage (#7, #8, #9, #10) ★ Data leaks (#10)
	★ PRC lacks a clear power advantage (e.g., U.S., India, Taiwan)	★ Territorial claims ★ Regional hegemony ★ “Taiwan independence”	★ Positioning in critical sectors, including in industrial control systems (#11, #13) ★ Data destruction, especially against critical and politically significant sectors (#12)

Recommendations for Threat Analysts to Increase Vigilance

- ★ **Political Monitoring:** Monitor for political developments that may trigger response or retaliation by PRC-aligned groups. Official policy documents, speeches by senior leaders, statements by ministries and agencies, and publications by authoritative media outlets like *People's Daily*, *Xinhua*, and *China Daily* often convey Beijing's intentions, motivations, and positions concerning these developments. Overlay activity spikes in threat activity—captured in internal monitoring and external reporting—with geopolitical activity to investigate possible causes.
- ★ **Indicators and Warnings:** When facing a challenge, the PRC typically uses multiple forms of power concurrently, since a single policy (e.g., cyberattacks) is unlikely to have a



decisive impact. To identify possible indicators and warnings, monitor for the PRC's hostile application of national pressure on a competitor through non-cyber means, such as nearby military exercises, coast guard harassment of maritime resource surveys, and banning imports from a country.

- ★ **Threat Actor Profiling:** Assess suspected PRC actors' missions, which often reflect geographic or functional responsibilities. Major confounding factors in this analysis are the use of common contractors and operational resources (e.g., tooling, infrastructure) across PRC threat groups. This insight can prioritize proactive hunt and defensive measures tailored to relevant groups' tactics, techniques, and procedures (TTP).

FACTORS INCREASING THE LIKELIHOOD OF TARGETING BY PRC CYBERATTACK OPERATIONS

This chart identifies factors that increase an organization's likelihood of becoming the target or being impacted by a PRC cyberattack, based on the case studies in this report. CISOs and other risk management professionals can use this chart to inform risk assessments and threat profiles for their organizations, partners, vendors, and other third parties.



ORGANIZATIONAL ATTRIBUTE	MODERATELY INCREASES RISK	GREATLY INCREASES RISK
LOCATION 	<ul style="list-style-type: none"> ★ PRC has a clear power advantage (e.g., Vietnam, the Philippines) 	<ul style="list-style-type: none"> ★ PRC lacks a clear power advantage (e.g., U.S., India, Taiwan)
SECTOR 	<ul style="list-style-type: none"> ★ Critical sectors (e.g., transportation, logistics, energy, power) ★ Academia ★ News and Media 	<ul style="list-style-type: none"> ★ Politically significant sectors (e.g., semiconductors) ★ Political entities (e.g., democracy promotion, anticorruption groups)
ACTIONS 	<ul style="list-style-type: none"> ★ Enables online censorship subversion ★ Publishes anti-PRC messages or messages conflicting with core PRC political positions 	<ul style="list-style-type: none"> ★ Attempts to specifically subvert PRC online censorship ★ Targets a Chinese audience with an anti-PRC message or messages conflicting with core PRC political positions

Recommendations for CISOs to Improve Risk Assessments

★ **Organizational Resiliency:** Assess organizational resiliency if there is a heightened threat of cyberattacks against specific countries, focusing on sectors most likely to be targeted. Evaluate the impact of a disruption on any local operations, the broader organization, and its supply chain. Assure that relevant organizational risk mitigation strategies exist for these scenarios.

★ **Cyber Risk Generated by Geography:** Incorporate geopolitical analysis into cyber risk assessment. Identify disputes between the PRC and other countries where your organization or its key partners operate. A higher likelihood of cyberattacks exists when the PRC—typically via formal foreign ministry statements—explicitly frames a national-level dispute as a threat to its core interests.

★ **Cyber Risk Generated by Sector:** The level of threat a sector faces from PRC actors differs by country based on the international relations context. The PRC has historically applied pressure via cyberattacks by targeting critical and politically significant sectors. For example, a politically significant sector might include semiconductors in the context of the Taiwan or oil and gas in the context of Vietnam.

★ **Cyber Risk Generated by Actions:** Incorporate cyber risk analysis into the organizational messaging risk management process, with the participation of operational, legal, and public relations stakeholders. The PRC has penalized organizations promoting messages perceived as critical of PRC territorial claims and internal political management. Problematic topics include the PRC's treatment of its Uighur minority, the Dalai Lama, the status of Taiwan, and corruption within the PRC government. Organizations face greatly heightened risk when their messages target a PRC-based audience (e.g., via publication in Mandarin). Online pressure tactics include heavy-handed censorship in China and coordinated social-media influence operations. Cyberattacks constitute a plausible, but yet undocumented additional method of applying pressure on companies.

PRIMARY PRC CYBERATTACK TACTICS

This chart synthesizes PRC attack operations in this report to characterize common threats and their impacts on targeted organizations, their partners, and the public. This chart and referenced case studies may serve as a basis for risk management activities, such as wargaming.

PRC CYBERATTACK THREATS	DISTINGUISHING CHARACTERISTICS WITH PRC	POTENTIAL IMPACTS	RELEVANT CASE STUDIES
Distributed Denial of Service (DDoS) attack 	<ul style="list-style-type: none"> ★ Often highly excessive volume for disrupting websites, indicating likely signaling objective ★ Often uses China-based IP addresses 	<ul style="list-style-type: none"> ★ Temporary loss of website and other online resource availability ★ Increased hosting costs ★ Inability to retain DDoS mitigation vendors 	#1, #2, #3, #4, #5, #6, #7, #9
Defacement of websites and digital signage 	<ul style="list-style-type: none"> ★ Blurred lines in public sources between independent hacktivists, government-encouraged hacktivists, and faketivists 	<ul style="list-style-type: none"> ★ Loss of communications with key audiences ★ Loss of consumer trust and public unrest ★ Exposure of confidential data 	#7, #8, #9, #10
Breach of industrial control systems 	<ul style="list-style-type: none"> ★ Energy and power sectors frequently targeted ★ Publicly unknown whether access has been used to disrupt systems ★ Unused access may represent reconnaissance, prepositioning, or signaling 	<ul style="list-style-type: none"> ★ Disruption of operational technology (OT) systems ★ Supply chain disruptions ★ Loss of power, water, or other utilities for customers 	#11, #13
Ransomware 	<ul style="list-style-type: none"> ★ A tactic rarely connected to PRC government aligned groups in public sources 	<ul style="list-style-type: none"> ★ Harm to integrity of data and availability of systems ★ Disruption of business operations 	#12



Recommendations for CISOs to Strengthen

Risk Management

★ **Supply Chain Resilience:** Conduct a full review of your supply chain to understand your dependencies and how you manage related risks. Layer geopolitical analysis on supply chain cyber risk analysis to understand how key scenarios—e.g., PRC cyberattacks that directly or indirectly target your suppliers—might cascade and impact your organization. Evaluate vendors several levels down and monitor risks on an ongoing basis. Ensure cybersecurity, procurement, and sourcing teams work together in a unified effort to support due-diligence, address supply chain cyber risk in the context of enterprise-wide risk management, and build resilience.

★ **Wargames:** Conduct executive-level wargames based on observed and plausible escalatory forms of attack operations by PRC adversaries. Most major U.S. organizations should wargame cyberattacks involving the PRC's long-term deterrence and coercion of Taiwan and any countries that might consider coming to its aid. Additionally, many U.S. organizations should consider wargaming cyberattacks supporting a hypothetical invasion of Taiwan, especially if their supply chains rely on it or they have operations there.

- Wargames should consider scenarios where an attack directly targets the organization, a partner or vendor (e.g., payroll processor), or third-party (e.g., power company). Wargames should also include a scenario where a cyberattack has already occurred, forcing all business operations units (e.g., legal, public relations) to respond to the aftermath. Utilize the case studies in this report and other sources of threat intelligence to create realistic scenarios. Based on these efforts, create or edit an organizational resilience response plan and update yearly.

★ **Prevention, Detection, and Response:** Understand the tactics, techniques, and procedures (TTP) associated with PRC threat actors and activity clusters listed in Appendix A. Audit or review security controls in place for potential threat activity by these adversaries. Develop detection routines using a TTP mapping framework like MITRE ATT&CK. Treat detected activity attributed to PRC-aligned threat groups as possible attack operations, weighing this analytical hypothesis using awareness of the current geopolitical context and the organization's profile. Test and validate response plans from in-house and managed service providers and their escalation processes up to the board of directors.

★ **Information Sharing:** Share information with peers, government organizations, and other companies to increase community awareness of current adversary activity and improve the visibility of your threat landscape. For U.S.-based private sector organizations, key government information sharing partners include the Cybersecurity and Infrastructure Security Agency (CISA), Department of Defense Cyber Crime Center (DC3), and the National Security Agency (NSA) Cybersecurity Collaboration Center (CCC). Engage with relevant sector-specific information sharing and analysis centers (ISAC); similar organizations exist in many countries other than the U.S. Leverage security information and event management (SIEM) and security orchestration, automation, and response (SOAR) capabilities to automate ingestion of shared information and decrease mean time to detect. Greater threat visibility increases the likelihood of clear, early indications and warnings of future threat activity.



The PRC's
"Three Basic Demands"
of the United States

“ The first is that the United States must not challenge, slander or even attempt to subvert the path and system of socialism with Chinese characteristics... ”

“ The second is that the United States must not attempt to obstruct or interrupt China’s development process... ”

“ The third is that the United States must not infringe upon China’s state sovereignty, or even damage China’s territorial integrity... ”

Source: “Wang Yi: Underline Three Bottom Lines of China’s Relations with the United States,” Embassy of the People’s Republic of China in the Republic of Liberia, n.d., accessed March 15, 2022, <https://www.mfa.gov.cn/ce/celr/eng/zgyw/t1895276.htm>.

ANALYTIC FRAMEWORK

The following section establishes a framework for understanding the conditions that may prompt China to launch cyberattacks, the missions of key cyber actors, and the purposes of their operations. Specifically, this section covers the following topics:

- ★ The core interests that the PRC vows to secure using all available instruments of national power
- ★ The discrete purpose and tasks of different PRC agencies in cyberspace
- ★ How the PRC likely perceives the strategic importance of its cyberattacks.

CORE INTERESTS

All PRC policy—military, economic, social, and technology—ultimately serves to secure the continuity and power of the CCP. Since the 1949 founding of the PRC, the CCP has held a political monopoly in China. As official party publications note, the CCP offers the people of the PRC social stability, economic growth, and international influence, in exchange for accepting a system designed to maintain the party and its leadership.¹⁵

The CCP thus seeks to sustain itself through policies that secure the PRC's so-called "core interests" ("核心利益," héxīn liìyì). However, the PRC does not define its core interests in a paramount strategic document. Its national planning documents, position papers, and leaders' statements since the early 2000s^{16 17} reveal essential national priorities labeled as "core interests," matters for which the PRC has "no possibility or intention of compromise or concession."¹⁸ The party is therefore likely willing to authorize offensive cyber operations when these core interests are under threat. Most commonly, the PRC categorically enumerates these interests as security, sovereignty, and development.^{19 20 21}

SECURITY

Also officially called "political security," "the people's security," "social stability," and "national unity,"^{22 23 24} the CCP sees internal stability as the bedrock of the country's success and its own persistence. Per state media, "the guarantee for China's long term social stability" is its political and social system, singularly and indisputably organized and led by the CCP.²⁵ The party sees numerous threats to this stability. Pro-democracy, anti-corruption, and reformist political movements directly call the CCP's legitimacy into question.

Natural disasters like earthquakes and the COVID-19 pandemic test the government's perceived competency. Economic slowdowns may suggest that China's mixed-economic system—shaped by state-planning and market forces^d—is not functioning.

SOVEREIGNTY

Also officially referred to as "national sovereignty," "territorial sovereignty," and "territorial integrity," the PRC claims ultimate, exclusive authority and control in various land and maritime areas. In addition to its undisputed mainland core, China asserts its sovereignty in Xinjiang,²⁶ Tibet,²⁷ Macau,²⁸ Hong Kong,³⁰ certain areas along the Sino-Indian border,³¹ much of the South China Sea,³³ and Taiwan.³⁴ In recognition of local social and legal circumstances, China designates some of these areas as "autonomous regions" or "special administrative regions," but affirms that the government of the PRC is the highest authority. China's senior-most leadership routinely unequivocally asserts that it will make no concessions on its territorial claims.³⁵ Among all these disputes, the Ministry of Foreign Affairs asserts that the inclusion of Taiwan within China is the most important and "China has the right to take any necessary measure to stop" Taiwan independence.³⁶

DEVELOPMENT

China seeks to secure its economic activities. The term "development interests" is relatively new to the PRC's political discourse³⁷ and has been elevated to an explicit core interest only in the past few years or so.³⁸ This evolution, as PRC government outlets note, reflects the emergence of "overseas China." The country's "overseas" development interests include offshore energy resources, overseas PRC companies and their investments, PRC citizens working abroad, and global supporting transportation channels and infrastructure.³⁹ Threats to the PRC's development include economic decoupling, restricted access to technologies like semiconductors, barriers to PRC investment, and physical threats to shipping lanes, personnel, and offices.

^d In PRC political parlance, China's economy since the 1980s has been structured as "**socialism with Chinese characteristics.**" Therein, the state allows a degree of market forces to shape the economy while still engaging in market planning. The specifics of this concept have varied with each successive head of state and party.

AGENCIES AND ACTORS

China's party-state^e uses organizations with varying remits and capabilities to secure its core interests through online action. These activities are often likely centrally directed and carefully synchronized. According to the U.S. Department of Defense, "the PRC's influence operations are coordinated at a high level within the party-state and executed by a range of actors, such as the United Front Work Department, the Propaganda Ministry, the State Council Information Office,^f the People's Liberation Army (PLA) and, the Ministry of State Security."⁴⁰ Most, if not all these actors, use a combination of conventional employees, contractors, and irregular agents like criminals and patriotic hackers. The specific relationship between these irregular agents and the state is often ambiguous in open sources. Consequently, this paper refers to groups acting in apparent support of China's interests as "state-aligned."

PEOPLE'S LIBERATION ARMY (PLA)

The PLA is the party's overt source of hard power for advancing its policy agenda globally and securing domestic peace. PRC leaders emphasize this purpose; as President Xi has observed, "the party commands the gun"⁴¹ and the army has "absolute loyalty to the party."⁴²

The military increasingly prioritizes information warfare. It conceptualizes information warfare as offensive and defensive activities that shape the information environment, from disrupting communications systems to undermining opponents' morale with targeted messaging.⁴³ To better compete in such non-geographic domains, consistent with the "evolution of warfare,"⁴⁴ China formed a new service branch, the PLA Strategic Support Force (PLA SSF), in late 2015.⁴⁵ Among its several changes, the PLA SSF unified the military's disparate cyber, electronic, and psychological operations capabilities—defensive, offensive, and reconnaissance—within an operational Network Systems Department.⁴⁶ The PLA SSF very likely maintains most of the PLA's pre-reform component cyber entities, including regionally focused sub-units affiliated with the PLA's five theater commands.^{47 48}

The PLA also controls "militias,"^g comprising commercial security specialists and members of academia, that conduct information warfare operations.⁴⁹ Some PLA militias likely receive money and training from the military. For example, in 2005, the government—possibly the PLA's Chengdu Technical Reconnaissance Bureau⁵⁰—asked a patriotic Chinese hacker to participate in the "Chengdu Military Militia Information Sub-Unit Network Attack and Defense Contest."⁵¹ Upon winning this competition, he and his teammates received intensive offensive operations training and won another larger PLA-run multiregion competition. They used their prize money to establish a company^h that developed zero-day exploits used in PLA operations.^{52 53}

MINISTRY OF STATE SECURITY (MSS)

The MSS is the party's secretive civilian security force. Its multipart mission includesⁱ tracking and countering foreign and domestic political threats to the party-state.⁵⁴ As one MSS defector has noted, the MSS's most important mission is "to control the Chinese people to maintain the rule of the Communist Party"⁵⁵ and promote its interests.⁵⁶ The MSS employs domestic contractors who engage in self-enriching criminal behavior (e.g., ransomware),⁵⁷ sometimes while simultaneously gathering digital resources for their government-contracted operations.^{58 59} Unlike the PLA, the organization of MSS cyber elements is poorly documented in public sources.



^g **Militias** are auxiliary paramilitary forces that the PLA may leverage to "[shoulder] the tasks of preparations against war and defence operations and [assist] in maintaining public order," per China's national defense law. They play a key role in projecting China's power abroad. The country's maritime militia is, for example, composed of fishermen who are often tasked to swarm and harass other countries' vessels in the South China Sea.

^h In 2009, the MPS reportedly arrested this recruited individual for targeting PRC organizations and shut down his company. The U.S. Department of Justice indictment alleges that since at least 2011 he and his reformed company have been involved in operations referred to as the **Chengdu-based individuals** activity cluster in Appendix A. (Sources: <https://www.justice.gov/opa/press-release/file/1317216/download>, <https://web.archive.org/web/20090925075518/http://www.hackbase.com/news/2009-04-09/24948.html>).

ⁱ More fully, the **MSS's acknowledged official mission** is counterintelligence, foreign intelligence, and "maintaining political security and overseas security." Its unacknowledged role in foreign intellectual property theft likely stems from its origin in 1983, being stood up to improve the state's non-military intelligence during a period of economic and political reopening and liberalization under head of state Deng Xiaoping. (Source: http://www.xsx.gov.cn/xwzx/tt/202101/t20210107_6607553.html).

^e The term "**party-state**" or a "**one-party state**" refers to a state organized around a single political party. The PRC is a party-state where the CCP has paramount authority and holds nearly all positions of power in the government and security apparatus.

^f The **State Council Information Office**, a.k.a. the **Central Office of Foreign Propaganda**, serves as a functional intermediary between PRC state media and global media. Since 2014, it has been a component of the Central Propaganda Department, as part of propaganda consolidation reforms. The office's historical responsibility for internet censorship moved to the new Cyberspace Administration of China in 2011.

KEY PRC ORGANIZATIONS WITH CYBER MISSIONS

This table characterizes several key PRC organizations with cyber missions. Significant overlaps in missions and authorities, joint operations, shared operational resources, and the use of common contractors contribute to the challenge of attributing PRC-aligned threat activity to specific organizations with high confidence.

ORGANIZATION(S)	MAJOR MISSION AREAS	ACTIONS IN CYBERSPACE
PEOPLE'S LIBERATION ARMY	★ National security ★ Military intelligence ★ Disaster relief ★ Peacekeeping	★ Warfare ★ Military espionage ★ Economic espionage
MINISTRY OF STATE SECURITY	★ Political security ★ Civilian intelligence ★ Counterintelligence	★ Political espionage ★ Economic espionage ★ Dissident surveillance and harassment
MINISTRY OF PUBLIC SECURITY	★ Domestic security ★ Public security ★ Law enforcement	★ Content monitoring enforcement ★ Shaping IT regulations to support CCP political needs
CYBERSPACE ADMINISTRATION OF CHINA	★ Internet governance ★ Internet regulation	★ Regulation of cross-border data transfer, to include censorship via the national internet boundary system
CENTRAL PROPAGANDA DEPARTMENT (CPD) AND THE UNITED FRONT WORK DEPARTMENT (UFWD)	★ National messaging	★ Social media influence operations
GOVERNMENT CONTRACTORS	★ N/A	★ Support for or execution of agencies' offensive activities ★ Self-enriching data theft and ransomware operations

MINISTRY OF PUBLIC SECURITY (MPS)

The MPS is China's national police force, responsible for maintaining public security and social order. Consistent with this mission, its online activities include enforcement of digital censorship and content monitoring.^{60 61} The MPS may use its law enforcement powers to compel technologists in China to become agents of the state. For example, in about 2006, shortly after security authorities in Henan province released members of one patriotic hacktivist group, its reportedly reformed members vowed to train "people for the state and [work] to improve the state's network security industry," indicating a continuing relationship with the state.⁶²

CYBERSPACE ADMINISTRATION OF CHINA (CAC)

The CAC is the party's internet governance agency. Originally a watchdog for socially sensitive content online and a digital censorship agency, the CAC now also serves as the party's broader internet gatekeeper for cyber companies seeking to enter the market in China.^{63 64} The CAC apparently regulates China's national internet boundary system, the so-called "Great Firewall," which blocks internet users in China from accessing websites deemed politically sensitive (e.g., foreign media critical of China).⁶⁵

CENTRAL PROPAGANDA DEPARTMENT (CPD) AND THE UNITED FRONT WORK DEPARTMENT (UFWD)

The CPD and UFWD are the party's secretive messaging organizations that seek to "engineer domestic and international climates favorable to the party's goals."⁶⁶ The CPD ensures the ideological correctness and promotional utility of state messaging, policing content on- and offline. The UFWD orchestrates overt and covert influence and disinformation campaigns domestically and abroad.⁶⁷ President Xi has referred to the UFWD as one of the CCP's three "magic weapons"⁶⁸ and encouraged China's citizens studying abroad to support the agency's efforts online.⁶⁹ The UFWD has likely employed local "marketing firms" and students to amplify messaging and disinformation with fake and hijacked social media accounts.^{70 71}

^j The **Publicity Department of the Central Committee of the Communist Party of China** is commonly known in English as the **Central Propaganda Department** or the **Propaganda Department**. Foreign commentary occasionally refers to it as the "Propaganda Ministry," although this label mischaracterizes the department's bureaucratic location in the PRC party-state, incorrectly implying that it is a state council-level executive department.

STRATEGY AND GOALS

No public strategic document or position paper claims to represent a unified PRC position on the shape and purpose of cyber operations beyond espionage. The available authoritative sources, mainly published by the PLA, officially represent their issuing organizations' perspectives on fulfilling their missions within their own capabilities. Though organizationally limited, they still provide a useful glimpse into how key actors perceive the greater mission and how cyberattacks fit into strategy. Given the high coordination and interconnected nature of the diverse cyber elements of China's party-state, these concepts are likely shared to some meaningful extent across agencies.

Since at least 2003, the PLA has developed an operational concept it calls the "three warfares," which is a model for shaping the information environment.^{72 73 74} This concept was originally conceived as shaping activities during wartime: mainly, coercing rival states, weakening their societies, and providing legal cover for military action. More recently, this information conflict has been framed as the perpetual shaping of conditions for China's political success domestically and globally within the "cognitive domain."⁷⁵ ^k

It is unknown in public sources whether other PRC security agencies conceive a similar operational framework, but it is somewhat likely. The PLA's concept describes activities by military and non-military agencies. The PLA similarly conceives of "integrated strategic deterrence," the comprehensive and centrally organized use of national power to achieve political ends, suggestive that agencies' cyber activities may be carefully coordinated with a unified vision.⁷⁶

INTEGRATED STRATEGIC DETERRENCE

Since about 2001, the PLA has advocated for the use of "integrated strategic deterrence," the centrally coordinated use of national-level capabilities to control China's external security environment. These capabilities are both military (e.g., nuclear, conventional, space, cyber) and non-military (e.g., diplomatic, economic, scientific) in nature. Although the term *weishè* [威懾] is normally translated as deterrence, in U.S. strategic parlance the "strategic deterrence" concept more closely equates to strategic coercion or compellence, indicating China's objective of changing its opponents' behavior, rather than maintaining the status quo.

THREE WARFARES

WARFARE TYPE	CONCEPT	CYBER SIGNIFANCE
PSYCHOLOGICAL	 The use or threat of force to affect an adversary's decision making. These actions demonstrate China's capabilities and resolve in order to achieve political outcomes, while minimizing the risk of conflict escalation. ^{77 78} Doctrinal PLA writings value limited high-profile sabotage attacks on select military, political, and economic targets to degrade the public and executive will to resist. ⁷⁹	Cyberattacks can be designed to signal China's position on key issues through controlled, non-escalatory destruction and disruption of specific significant targets.
PUBLIC OPINION	 The attempt to control information dissemination. This concept encompasses active information dissemination by China and its attempts to limit dissemination by others, such as through the disruption of foreign media outlets. ⁸⁰ These actions serve to shape domestic and international perspectives of China, its policies, and its positions in disputes.	Cyberattacks can hinder information dissemination, such as through the disruption of news websites, social media, and communications platforms. Espionage can enable leaks of sensitive, sensational, or damaging information. Coordinated inauthentic social media campaigns can project China's positions or distract from harmful narratives.
LEGAL	 The use of international and domestic laws and legal mechanisms for strategic offensive and defensive purposes. These actions serve to silence or discredit opponents, legitimize China's policies, gain foreign support, and delay organized responses to China's behavior.	China engages in legal and normative debates about acceptable behavior in cyberspace, such as "cyber sovereignty." ¹⁸¹

^k The growing emphasis on "cognitive domain" operations in PLA publications of recent years may be representative of broader changes across PRC ministries and agencies. It paralleled the growth of China-linked online disinformation operations in the late 2010s, which are largely out of this paper's scope as parallel issues.

^l "Cyber sovereignty" or "internet sovereignty" is a normative justification for governments monitoring internet activity within their borders and restricting the content that their residents access and transmit. This concept also justifies applying pressure on foreign companies to self-censor as a prerequisite to access certain national markets.

CASE STUDIES

We assess that China's party-state uses cyberattacks to secure its stated core interests. The following 13 case studies show how PRC-aligned actors conducted cyberattacks when China's domestic and international interests came under pressure. Based on the political context surrounding attacks, we identified four themes that likely framed the attacks from China's perspective: foreign information threats, the Hong Kong democracy movement, competing South China Sea claims, and Indo-Pacific competition. We have grouped the case studies by these themes. Themes do not rigidly align to "core interests"; themes often relate to multiple interests concurrently. For each case study, we describe the political conditions that may have prompted action, what happened online, who was responsible, and our analysis of the activity.

THREATS TO DOMESTIC INTERESTS

KEY FINDINGS

China uses cyberattacks to combat foreign and domestic condemnation of its internal affairs, its socio-political system, and the CCP.

★ China's immediate goal is likely to silence its opponents through direct disruption. Its opponents are mainly political organizers and news outlets that disseminate narratives considered dangerously influential to an audience in China. The PRC's preferred cyberattack response to such threats—distributed denial of service (DDoS)—reflects this goal of silencing. China's premier DDoS tool, the Great Cannon, functionally aligns with its censorship and state security apparatus. Likely reflective of this functional concept, the Great Cannon shares infrastructure with China's national internet border control, the Great Firewall.

★ China likely also aims to dissuade future condemnation by emphasizing its power and determination. In the reviewed examples, it used overwhelming force—often excessive from a tactical standpoint—likely seeking to shock and awe its opponents. Its DDoS attacks have sometimes had the greatest volumes observed up to that point in time, drawing global attention that China might consider a reputational benefit. Cyberattacks are often paired with other publicly observable tactics like asset seizure, detention, and large-scale social media trolling and disinformation campaigns, compounding the message.



1

THEME #1: FOREIGN INFORMATION THREATS

The CCP views the internet as a double-edged sword. In 2010, the party's official newspaper observed that the internet has an "irreplaceable role in accelerating" China's economy and development, but it must be administered to ensure "state security and social harmony, state sovereignty and dignity, and the basic interests of the people."⁸² In other words, the internet may enable destabilizing collective activism, threaten the party's monopoly on information within China, and undermine the ability of the party to advance its policies. For this reason, China has long advocated for international rules and norms that protect each country's ability to control the content of its local internet and maintain its "cyber sovereignty," consistent with the concept of legal warfare.⁸³



DISRUPTING ONLINE PETITIONS TO THE PRC (APRIL 2011)

Political Context

In December 2010, anti-authoritarian protests and revolutions facilitated by social media—known today as the Arab Spring—began sweeping the Middle East and North Africa. The following February, social media users in China began calling for their own pro-democracy protests.⁸⁴ China's

censorship apparatus quickly blocked relevant news and keywords on social media and search engines.⁸⁵ Overwhelming police force against the modest initial protests ended the movement within weeks.⁸⁶

And so in 2011, the threat of an Arab Spring-like movement in China, empowered by online organization, became the catalyst for the modern PRC state online information control apparatus. China's president called on the CCP to strengthen its control of the internet and its ability to shape online public opinion, to build a "harmonious socialist society."⁸⁷ In turn, the government announced on May 4 the consolidation of various agencies with internet jurisdictions into a single State Internet Information Office,⁸⁸ today effectively synonymous with the Cyberspace Administration of China (CAC).⁸⁹ The new agency would "direct online content management," have oversight of telecommunications companies and content providers, punish violators, and promote "government propaganda."⁹⁰

China also detained more than 50 prominent activists to further quell the unrest.⁹¹ The most high-profile activist was Ai Weiwei, a globally renowned artist and critic of the PRC government, arrested on April 3.⁹² The government stated on April 7 that Ai was being held on suspicion of committing "economic crimes," (later specified as tax fraud),⁹³ implying that he had been held for common criminal matters rather than for his high-profile political activism.⁹⁴

Online petitions soon began demanding Ai's release. On April 4, a California-based Twitter user launched a petition on Twitition (a now-defunct but then-popular website), which received about 2,000 signatures.⁹⁵ On April 8, leading members of the international art museum community launched a petition on Change.org,⁹⁶ which quickly gathered more than 100,000 signatures. On April 17, demonstrators supporting Ai held protests at PRC embassies worldwide.⁹⁷

Cyber Activity

Large, protracted DDoS attacks originating in China⁹⁸ targeted the two petition websites in this timeframe. Twitition experienced two waves of attacks, first from April 6 to April 8 and then resuming on April 18.^{99 100} The company's hosting provider described the attacks as "very sophisticated," without further public explanation.¹⁰¹ Also, on April 18, DDoS attacks began disrupting Change.org, periodically reappearing for the next 10 days, growing "in location and intensity"¹⁰² as the number of involved bots increased.¹⁰³

Attribution

These attacks have not been explicitly attributed, and the two DDoS attacks have not been linked to a single actor or botnet. Technical and circumstantial evidence indicates plausible PRC government shaping of the attacks or, at least, tacit consent.

- ★ All the IP addresses used by bots that targeted Change.org were China-based,¹⁰⁴ geolocated to Beijing and Hebei and linked to the internet service provider China Unicom.¹⁰⁵
- ★ On April 25, U.S. State Department Deputy Assistant Secretary Daniel Baer raised unspecified concerns about the attack with China's Ministry of Foreign Affairs in Beijing.¹⁰⁶ Publicly raising a concern at such a high diplomatic level likely reflected, at a minimum, U.S. suspicion of PRC responsibility.
- ★ If the adversaries were conventional pro-PRC patriotic hacktivists, it was very unusual that no individuals or groups observably claimed responsibility.^{107 108}

Assessment

The use of online petitions to signal global condemnation of Ai's arrest may have prompted an offensive cyber response by China. The attacks appeared to convey China's disapproval of organized foreign criticism of its internal affairs. As China's official English-language outlet *China Daily* noted on April 14, "whether Ai has violated the laws of [China] is of no importance to...Westerners, who delight in voicing their opinions about China's treatment of those they choose to consider political dissidents."¹⁰⁹ The attack may have also served as a warning to organizing platforms, heretofore unaccustomed to PRC pressure: Change.org said this was the first time it had been a DDoS attack target,¹¹⁰ and Twitition expressed surprise that anyone would want to disrupt them.¹¹¹



DISRUPTING ANTI-CENSORSHIP EFFORTS (MARCH 2015)

Political Context

Since the internet's arrival on the mainland in April 1994,¹¹² the CCP has sought to reap the benefits of a connected economy, while protecting its authoritarian system from free-flowing criticism and political organizing online. China manages this balancing act with a combination of laws,

policing, and censorship infrastructure—including two key parts:

- ★ The **Golden Shield Project (GSP)** is a domestic surveillance program under the MPS. It provides authorities with ubiquitous and centralized monitoring capabilities, including internet monitoring.^{113 114}
- ★ The **Great Firewall (GFW)** is an unofficial name for China's national internet boundary system. It serves to limit China's internet users' access to foreign content deemed objectionable by PRC authorities.¹¹⁵ The system routinely blocks mainland access to social media, video sharing, search engines, news, and encyclopedias. Public sources conflict about which PRC government organization is ultimately responsible for the GFW (e.g., the PLA, the MSS, or the Propaganda Department).^{116 117 118}

Anti-censorship nonprofit GreatFire helps internet users in China circumvent the GFW, mainly using a “collateral freedom” strategy.¹¹⁹ In this way, the organization hosts mirrors of banned news outlets on “unblockable” internet services like GitHub where censorship might be unacceptably disruptive to China.¹²⁰ As a case in point, China blocked GitHub in January 2013, possibly in response to its enablement of online political organizing but relented a week later amid outcries by disrupted technologists in China.^{121 122}

In early 2015, PRC authorities faced off with GreatFire. In January, GreatFire alleged that China may have compromised its email server that month,^{m 123} and the CAC shot back, decrying GreatFire as a “foreign anti-Chinese organization.”¹²⁴ Also that month, Deutsche Welleⁿ announced a partnership with GreatFire to make its content available in China.¹²⁵ In February, China removed *The New York Times'* last official online presence in China, suspending several verified Weibo accounts associated with the company.¹²⁶ In April, reporting noted that the GFW had been forced to undergo several upgrades over the previous year due to “[overseas who] upgraded their service to help mainlanders bypass the blockages.”¹²⁷

^m On March 20, 2015, Google determined that CAC certificates were being abused for man-in-the-middle attacks, and, a week later, declared that CAC root certificates could not be trusted. CAC blamed a contractor for the incident. (Sources: <http://googleonlinesecurity.blogspot.com/2015/03/maintaining-digital-certificate-security.html>, <https://web.archive.org/web/20150412080258/https://zh.greatfire.org/blog/2015/jan/outlook-grim-chinese-authorities-attack-microsoft>).

ⁿ Deutsche Welle is a German state-funded international broadcaster, akin to the U.S.'s Voice of America, Japan's NHK World, and the UK's BBC World. Its website has been periodically censored in China since at least 2001. (Source: <https://www.dw.com/en/china-censors-dw-world/a-1139700>).

Cyber Activity

In March 2015, two protracted DDoS attacks targeted GreatFire. These employed the so-called Great Cannon, an attack tool that injects malicious code into traffic passing through the GFW. In this case, the Great Cannon hijacked attempts to load a Baidu analytics script on certain popular websites, causing visitors' browsers to launch DDoS attacks against GreatFire.^{128 129} GreatFire reported that this was its first experience with a DDoS attack.¹³⁰

The attacks were likely pre-meditated, rather than in response to the news cycle. Starting in early March, the Great Cannon's operators appeared to conduct tests in preparation for the attacks against GreatFire.¹³¹ From March 4 to March 6, the Great Cannon first conducted limited and then large volume attacks against a Shanghai-geolocated IP address.¹³² The following week, from March 10 to March 17, it targeted a Hong Kong-geolocated IP address.¹³³

The first attack against GreatFire, from March 18 to March 23, hit its news content mirror-hosting located on Amazon CloudFront,¹³⁴ but ignored GreatFire's website.¹³⁵ The attack measured 2.6 billion requests per hour (2,500 times GreatFire's normal traffic level)¹³⁶ at times and increased the organization's CloudFront hosting costs to \$30,000 per day.¹³⁷ The second attack, from March 25¹³⁸ to March 31,¹³⁹ o targeted GitHub pages belonging to GreatFire and a mirror host of *The New York Times*.^{140 141} GitHub, a frequent target for DDoS attacks,¹⁴² reported that the incident had been the largest DDoS it had experienced to that point.¹⁴³ The attack evolved over multiple days—likely attempts to outmaneuver defenders—resulting in traffic surges.¹⁴⁴



^o These dates reflect local time for GitHub, a San Francisco-headquartered company. Per GitHub, the attack began at about 2 AM UTC on March 26, 2015. This is equivalent to 6 PM PT on March 25. The company tweeted at 4:11 AM PT on March 31 that its systems had returned to normal.

Attribution

The PRC almost certainly controls and operates the Great Cannon. The tool shares infrastructure and source code with the GFW¹⁴⁵ and is consistently employed to attack organizations that threaten PRC interests, which are discussed on several occasions in this report. Multiple knowledgeable sources speaking with a credible Hong Kong newspaper, *South China Morning Post*, in April 2015 confirmed that the Great Cannon had been under development for about a year.¹⁴⁶ These sources stated that the tool was part of a “new strategy...taking an offensive attitude rather than the Great Wall’s tactics of focusing on defence” by disrupting websites “deemed unfriendly to the Communist Party.”¹⁴⁷

Assessment

The attacks marked a major shift toward China taking offensive control of its domestic information environment. Further, it demonstrated China’s high tolerance for reputational and economic blowback in pursuit of political priorities. The attacks risked embroiling Baidu, one of the world’s largest technology companies and a highlight of China’s innovation economy,¹⁴⁸ in a public political dispute. The attacks disrupted GitHub, a globally used code-development website; owing to its critical importance to businesses in China, GitHub is one of just two foreign-owned platforms accessible in China that allow user-generated content,¹⁴⁹ despite efforts to launch local alternatives.¹⁵⁰ These attacks sharply contrast with the 2011 DDoS attacks against online petition platforms, where the government’s hand was unclear and involved entities with comparatively minor public profiles.



CONFRONTING PERSISTENT CORRUPTION ALLEGATIONS (2017–2018)

Political Context

In late January 2017, *MingJing News*, a U.S.-based outlet that covers affairs in China, announced that it would soon air a bombshell interview. The site has frequently drawn Beijing’s ire for its publication of sensitive, controlled political information and is consequently blocked in China.¹⁵¹ The interviewee was Guo Wengui, a real estate magnate from China highly connected to the party’s top echelons and now living in the U.S.^{152 153} In this interview and ones with *MingJing* over the following years, Guo alleged widespread and specific acts of corruption by China’s political and business elites.¹⁵⁴

Regardless of the validity of these claims,^p China’s government has attempted to intimidate *MingJing* and Guo. He has been pressured by undeclared PRC security officials in the U.S.,¹⁵⁵ targeted by two Interpol arrest requests,¹⁵⁶ and had his assets in Hong Kong seized.¹⁵⁷ Perhaps to sway international opinion against Guo, PRC law enforcement uncharacteristically spoke with the Associated Press, accusing him of assaulting an assistant;¹⁵⁸ PRC law enforcement rarely speaks directly with unaligned foreign outlets. Security forces allegedly kidnapped the wife of Guo’s frequent interviewer at *MingJing* while she was in China; she resurfaced months later in a video denouncing her husband’s work.¹⁵⁹

Cyber Activity

Immediately after *MingJing* announced the first interview, its websites and TV channels began suffering unspecified “attacks.”¹⁶⁰ Concurrently, a persistent phishing operation repeatedly targeted U.S.-based *China Digital Times*,^q claiming to have “insider information” about the “hacker attacks” against *MingJing*.¹⁶¹



^p In 2021, social media intelligence firm Graphika assessed that Guo Wengui is “at the center of a vast network of interrelated media entities which have disseminated online disinformation and promoted real-world harassment campaigns.” (Source: https://public-assets.graphika.com/reports/graphika_report_ants_in_a_web.pdf)

^q *China Digital Times* is a U.S.-based media organization that focuses on news from China that would otherwise be blocked by censors.

Great Cannon DDoS attacks targeted *MingJing* at least twice over the next two years. These attacks may have been coordinated with other overt forms of government pressure. The first attacks in mid-August 2017^{162 163} were contemporaneous to the Associated Press interview and the seizure of the *MingJing* interviewer's wife. Another attack in mid-November 2018¹⁶⁴ may have occurred on the same day that a Beijing-friendly Hong Kong news outlet revealed that more than a billion dollars of Guo's assets had been frozen by local authorities.¹⁶⁵ Also that day, Guo held a scheduled press conference alleging specific and widespread acts of murder, politically motivated imprisonment, and torture by the PRC government.¹⁶⁶

In addition, starting in April 2017 and continuing for at least two years, coordinated disparaging, inauthentic Twitter campaigns have targeted Guo. Researchers have noted that the campaigns generated "significantly larger" tweet volumes than those targeting massive democracy protests in Hong Kong, an object of immense scorn for Beijing.¹⁶⁷

Attribution

The use of the Great Cannon implicates China's government in the DDoS attacks. It is another example of China using the tool to disrupt sources of information that spread narratives counter to its political interests.

These inauthentic Twitter campaigns' ebbs and flows closely aligned with the working week and public holidays in China.¹⁶⁸ This pattern suggests likely attribution to a professional, China-based organization.

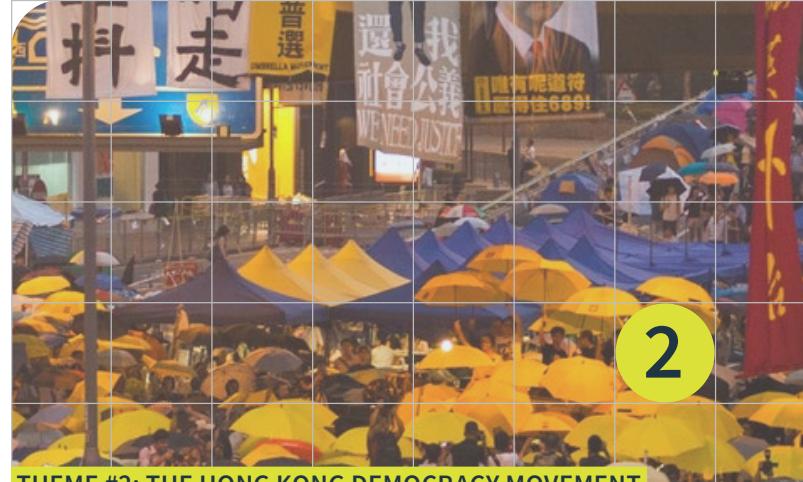
Based on infrastructure pivoting and malware, academic cybersecurity research group The Citizen Lab assessed that the same adversary phishing *China Digital Times* likely also targeted several other Beijing-critical Chinese-language news sites in this period.¹⁶⁹ The Citizen Lab assessed that the Winnti Group^r or a closely related adversary had also likely targeted government and civil society groups in Asia.¹⁷⁰

For more information on related activity clusters, see *Chengdu-based Individuals* in Appendix A.

Assessment

These activities appear to show multiple forms of China's power, including financial seizure, detention, information operations, digital surveillance, and cyberattack, being used in tandem to shape the information environment. Variously, they served to discredit, intimidate, defund, and drown out Guo and his persistent string of allegations. The repeated proximate timing of the application of different capabilities suggests a high degree of interagency coordination, rather than different actors independently acting toward a shared goal.

^r For more information about the attribution and nomenclature challenges associated with the "Winnti Group," refer to Appendix A: *Chengdu-based Individuals*.



THEME #2: THE HONG KONG DEMOCRACY MOVEMENT

The democratization of Hong Kong has long been a fraught issue for China. In 1984, the United Kingdom (UK) and China agreed, after decades of on-and-off discussions,¹⁷¹ to the conditions by which the UK would relinquish its Hong Kong colony in 1997.¹⁷² The territory would accordingly retain a "high degree of autonomy" regarding its domestic affairs, preserving many legal freedoms until 2047 and aspire to the "ultimate aim" of universal suffrage.¹⁷³ ^s Going further, in 2007, Beijing declared that Hong Kong could begin electing its chief executive by universal suffrage in 2017.¹⁷⁴ For the past decade, disagreements about the realities of these statements have been at the core of tensions over the political future of Hong Kong. The PRC has explicitly stated that Hong Kong's governance and electoral system is a core interest that must be protected as a matter of national sovereignty and territorial integrity.¹⁷⁵



^s Universal suffrage is commonly understood outside China to refer to all adult citizens having the right to vote in elections, regardless of their sex, political affiliation, wealth, or almost all other discriminating attributes. Officially, universal suffrage has always existed in the PRC, but, in a practical sense, this only applies to the election of local officials. All other levels of government are elected through hierarchical tiers of legislative bodies called "assemblies." Although Communist Party membership is not required to run for office, pressure from the government ensures that no meaningful opposition exists.



DISRUPTING A REFERENDUM ON HONG KONG'S ELECTIONS (JUNE 2014)

Political Context

By 2014, pro-democracy groups in Hong Kong had grown restless over a perceived lack of progress toward universal suffrage. One group, Occupy Central,^t commissioned the University of Hong Kong (UHK) to organize an unofficial poll (dubbed a “referendum”), asking Hong Kongers how they wanted to choose their next chief executive in 2017. Crucially, all three options would allow citizens to nominate their own candidates. The polling was scheduled to occur from June 20 to June 22, concluding a week prior to annual July 1 pro-democracy protests on the anniversary of the British handover of the colony.¹⁷⁶ Voting would occur at in-person polling stations, as well as via the electronic voting system (“PopVote”) on the UHK website and a smartphone app. To prevent repeat voting, votes were tied to residents by their Hong Kong ID numbers. Ultimately, 792,808 votes were cast, representing more than 10% of the population.¹⁷⁷

Beijing stood firm. On June 14, the PRC State Council^u issued a white paper asserting that China had “comprehensive jurisdiction” over the Hong Kong Special Administrative Region (SAR) and that “loving the country is a basic [political] requirement for Hong Kong administrators.”¹⁷⁸ On June 20, PRC authorities stated that such referendums were illegal, unconstitutional, and invalid and that “citizen nomination” of candidates lacked “broad social consensus.”¹⁷⁹ On June 23, the State Council ordered all news organizations and content hosts to delete all articles, blogs, comments, and other references to the referendum.¹⁸⁰

^t **Occupy Central with Love and Peace** (Occupy Central) was a civil disobedience movement that advocated for democratic reforms in Hong Kong (e.g., one-man-one-vote principles, lower restrictions on standing for election).

^u The **State Council of the People's Republic of China** (State Council) is the executive cabinet of China's government. Its parallel center of power is the Politburo Standing Committee, representing the Communist Party. The PLA's bureaucratically resides under the party's Central Military Commission, not the government.

Cyber Activity

Massive DDoS attacks repeatedly targeted PopVote. Two weeks before polling began, DDoS attacks of undisclosed sizes disrupted PopVote’s server for two days, congesting the university network and crashing its email system.¹⁸¹ On June 14 and 15, shortly after polling registration opened, two more waves of large DDoS attacks¹⁸² crashed PopVote’s website.^{183 184} The organization’s three hosting services recorded large traffic volumes; they variously counted 10 billion requests in 20 hours, 75 Gbps, and 10 Gbps traffic loads, causing all three to suspend support.¹⁸⁵ When online polling began on June 20,¹⁸⁶ only one provider resumed service, reporting that the attacks had swelled to more than 300 Gbps,¹⁸⁷ one of the largest DDoS volumes reported up to that point globally.¹⁸⁸ Despite PopVote planning for such targeted threats,^w the attacks substantially disrupted polling,¹⁸⁹ compelling organizers to extend the polling period from three to 10 days.¹⁹⁰

HKU and PopVote faced additional cyber and information threats related to the poll. Text-message phishing (SMSishing) targeted the message provider supporting the poll, several fake websites imitating the polling website appeared, and rumors swirled about data leakage and poll response duplication.¹⁹¹ A telephonic denial-of-service (TDoS) attack flooded PopVote’s hotline and fax number with calls almost every second for two days.¹⁹² The university also detected suspicious logins to its intranet accounts, indicative of a likely breach.¹⁹³

Similar offensive cyber activity concurrently targeted *Apple Daily*, a major Hong Kong newspaper that strongly supported the democracy movement.^x DDoS attacks, whose volumes escalated over several days,¹⁹⁴ targeted the outlet’s Hong Kong and Taiwanese websites; on June 18, the DDoS volume

^v One local hosting company severed its contract on June 16, while Occupied Central stopped using the other global hosting provider because the pay-as-you-go hosting prices could have bankrupted the movement. (Source: <https://advox.globalvoices.org/2013/10/26/hong-kong-activists-organize-prepare-for-online-attacks/>)

^w During a **lower profile poll in 2012**, PopVote was the target of small, but disruptive sustained DDoS attacks, which Hong Kong police attributed to a local man. An unknown adversary also breached the email accounts of two PopVote IT staff members. This experience caused PopVote to anticipate possible disruption of the 2014 poll. (Source: https://popvote.hk/doc/popvote622_activity_report_tc.pdf?v=20150216) Interestingly, an unknown adversary also spear-phished the PopVote information technology (IT) staff members, hijacking their email accounts. (Sources: https://popvote.hk/doc/popvote622_activity_report_tc.pdf?v=20150216, <https://www.hkupop.hku.hk/english/columns/columns153.html>)

^x In the summer of 2021, Hong Kong authorities successfully compelled *Apple Daily* to cease operations. Police arrested many of its key leadership and senior editorial staff, charging them with collusion with external forces to endanger national security for publishing op-eds demanding international sanctions on China and Hong Kong. The government also froze the company’s and its founder’s assets. (Source: <https://hongkongfp.com/2021/06/17/breaking-hong-kong-police-raid-apple-daily-office-editor-in-chief-among-5-arrested-under-national-security-law/>)

reached 40 million requests per second,¹⁹⁵ knocking both sites offline for 10 hours.^{196 197} *Apple Daily* reported that an adversary had deleted part of its news archive¹⁹⁸ and a network switch's password had been inexplicably changed,¹⁹⁹ indicating possible intrusion activity.

An adversary conducted a hack-and-leak operation to discredit the referendum. At some point in 2014, an adversary breached the personal email account of the academic who organized the referendum. The adversary then leaked his correspondence to pro-Beijing media in batches in October 2014.²⁰⁰ The emails embroiled the academic in a scandal related to the referendum's funding, resulting in HKU imposing penalties on him. Other HKU administrators and academics who supported Occupy Central were contemporaneously targeted via phishing and smear campaigns.^{201 202}

Attribution

The PRC is believed to have sponsored the DDoS attacks. CrowdStrike, for example, assessed likely PRC involvement based on connections between the DDoS and unspecified "China-based" intrusion activity and the contemporaneous development of another DDoS tool linked to the PRC.²⁰³ *Apple Daily*'s chairman publicly blamed China's government without providing supporting evidence.²⁰⁴ The relevant adversary or adversaries clearly supported China's interests by attempting to disrupt the poll, silence its largest media supporter, and suppress Hong Kong's pro-democracy movement. Publicly available technical data is also consistent with, but does not confirm, PRC state involvement.

★ 30%–40% of the IP addresses associated with DDoS activity targeting PopVote were registered to undisclosed mainland China companies with offices in Hong Kong.²⁰⁵ Similarly, *Apple Daily*'s sister outlet *Next Magazine* reported that another 50% of the attacker IP addresses were associated with three entities (China Mobile and research institutes at the Chinese Academy of Sciences and the Russian National Academy of Sciences) with 40% of the attack volume coming from the two PRC organizations.²⁰⁶ All three are unusual sources of attacks because reportedly neither research institute sells access to its IP space and China Mobile sold only mobile internet access, a poor option for launching DDoS attacks. China Mobile threatened to sue *Next Magazine* for making this claim.²⁰⁷

★ The attacker's ability to generate one of the largest volume DDoS attacks up to that point²⁰⁸ against multiple targets for a sustained period is a strong indicator of the adversary being either a state actor or an enlisted top-tier criminal organization, rather than common patriotic hacktivists. It is unknown if these DDoS attacks were conducted by Hurricane Panda, the adversary who conducted even larger DDoS attacks against *Apple Daily* later in 2014, which are described in the proceeding section.

★ The developers of the imitation polling sites may have been from mainland China. The sites referred to the Chinese-language version of the site with the filename "zhongwen," the romanized spelling of the Mandarin word for the Chinese language, rather than "Chinese" or "Chin," which local technologists reported are the norm for web development in Hong Kong.^{209 210} The Cantonese language is much more commonly spoken than Mandarin in Hong Kong.

Assessment

China likely sought to slow or intimidate into submission Hong Kong's growing pro-democracy movement by disrupting PopVote's poll, discrediting its organizers, and silencing its media supporters. This operation likely involved the coordination and execution of multiple components, such as DDoS, TDoS, intrusion operations, and weaponized leaks.

Much like the previously discussed DDoS attacks against foreign information threats, these attacks used overwhelming power, drawing international attention to China's resolve and its ability to disrupt a prepared target. Therein, China may have secondarily sought to dissuade other foreign technology companies from supporting the democracy movement.





Case Study #5

SUPPRESSING HONG KONG'S DEMOCRACY MOVEMENT (SEPTEMBER TO OCTOBER 2014)

Political Context

In late 2014, massive pro-democracy demonstrations known as the Umbrella Revolution^y embroiled Hong Kong. In August, Beijing proposed allowing all eligible voters to participate in the local 2017 elections, but candidates would be nominated by a committee disproportionately representing pro-Beijing elements in Hong Kong.²¹¹ Weeks of sporadic reactionary protests evolved at the end of September into large-scale acts of civil disobedience as protestors, initially students, began occupying major roadways and areas outside government buildings, thus overtaking Occupy Central's plan to wait until October 1.^z Activity peaked in October as police violently clashed with protestors, and Hong Kong's leadership agreed to meet with organizers.²¹² The protests ultimately ended on December 15, after public support for the disruptive sit-ins waned and police swept remaining encampments.

Cyber Activity

Alongside likely domestic security cyber surveillance operations,^{213 214 215} disruptive cyberattacks also targeted the protest movement. For example, on October 14, DDoS attacks on *Apple Daily* and its parent company, *Next Media*, resulted in a "total failure" of their networks. *Next Media* and *Apple Daily*'s websites, mobile app, email, and business operations systems were unusable, "severely affecting" the delivery of newspapers.²¹⁶ Another DDoS targeted and reportedly crashed HKGolden,^{217 218} a general interest forum locally leveraged for political organizing. CloudFlare, which

provided DDoS mitigation services for *Apple Daily*, PopVote, and other unspecified affected Hong Kong entities' websites, reported that the attacks reached a then-extremely high rate of 500 Gbps.²¹⁹ Arbor Networks observed other major surges in DDoS attacks against Hong Kong entities on October 17 and October 19.²²⁰ Then, on October 24, the attackers sent commands to the primary botnet, ordering it to stop,²²¹ but Hong Kong entities continued to experience intermittent, higher-than-normal rates of DDoS attacks into November.²²²

Attribution

Several threat intelligence firms linked the DDoS attacks to the PRC-aligned Poisoned Hurricane activity cluster. The threat actor behind the cluster, most widely known as Hurricane Panda, primarily engaged in espionage and intellectual property theft in East Asia and the U.S.^{223 224} Based on overlapping tools and infrastructure, at least some of the domestic security surveillance operations in Hong Kong were likely conducted by the same actor or a similarly resourced actor.²²⁵

For more information on this activity cluster, see Hurricane Panda in [Appendix A](#).

Assessment

Once again, China very likely attempted to disrupt Hong Kong's democracy movement by continually disabling its organizing platforms, media supporters, and other civil society affiliates with then-massive DDoS attacks for most of October.

It is unclear, however, what prompted the attacks to seemingly slow down on October 24. On October 23, the United Nations (UN) Human Rights Committee warned China that its actions were incompliant with the International Covenant on Civil and Political Rights.²²⁶ In response to the warning, China conceded that this treaty still applied to Hong Kong, but not this situation.²²⁷ aa China may have relented slightly in response to this legal challenge.

^y The name **Umbrella Revolution** refers to protestors' use of umbrellas to block riot police pepper spray. These umbrellas became icons of the movement. In response, for example, local Macau authorities banned reporters from using umbrellas when President Xi arrived on a rainy day in December 2014 to commemorate Portugal's handover of Macau. The name, when written with Chinese characters, also contains a subversive play on words, owing to the different readings of the characters by Mandarin and Cantonese speakers (a mainland China vs. Hong Kong difference). (Source: <https://www.theguardian.com/world/2014/dec/19/umbrella-ban-macau-china-xi-jinping-visit>)

^z **October 1 is China's National Day**, commemorating the establishment of the PRC in 1947, and a public holiday in Hong Kong.

^{aa} China signed the **International Covenant on Civil and Political Rights** (ICCPR) in 1998 but has not ratified it. Hong Kong, however, is a signatory, owing to the terms of the British handover and the enshrinement of the ICCPR in the city's de facto, Beijing-approved constitution.



DISRUPTING HONG KONG'S PRO-DEMOCRACY PROTESTS (2019–2020)

Political Context

In April 2019, Hong Kong's Legislative Council introduced revised extradition laws. The amendments would allow, for the first time, the extradition of criminal suspects in Hong Kong—be they Hong Kongers, PRC nationals, or foreign residents—to mainland China.²²⁸ Many business, legal, and human rights groups opposed the bill, arguing that it would erode Hong Kong's legal independence and legitimize China's use of extraordinary rendition, an increasingly visible threat in recent years.^{229 230} It would enable China to demand the handover of its opponents living in or traveling to Hong Kong.²³¹

Despite pundits' perceptions of "protest fatigue" following the 2014 Umbrella Revolution, massive demonstrations starting in mid-June drew upward of 1 million people, potentially the largest protests since the 1997 handover.²³² Facing continued widespread pushback, Hong Kong's legislature ultimately withdrew the extradition proposal in October.²³³ On November 24, pro-democracy Hong Kong candidates posted overwhelming victories over the pro-Beijing opposition in 17 out of 18 district-level elections.^{234 235} The mass protest movement then rapidly slowed in early 2020 amid the growing threat of the COVID-19 pandemic.

Cyber Activity

At least four large DDoS attacks targeted communications platforms used by the Hong Kong protest movement in 2019. These attacks consistently occurred on the dates of scheduled mass protests or, in the case of Hong Kong's election day, when protests were likely to break out.

← Tweet

LIHKG 討論區 @lihkg_forum · Nov 23, 2019

11/24 is the election day of Hong Kong District Council. Be a good citizen and don't forget to get up earlier for voting

相關討論 - 戰係一個有得投票嘅中學生
lihkg/1745924

#DistrictCouncil #vote #HongKong #LIHKG

11.24
區議會投票日

fast13711
@fast13711

Replying to @lihkg_forum

準時 6 點 ddos

9:28 AM · Nov 24, 2019 · Twitter for Android

Figure 1. On November 23, LIHKG encouraged Hong Kongers to vote in the next day's election. A DDoS disrupted LIHKG shortly before polls opened, leading one Twitter user to dryly joke about the DDoS's punctuality, apparently comparing it to a bus or train running on time.

DDOS ATTACKS TARGETING THE 2019 HONG KONG DEMOCRACY MOVEMENT			
DATE	TARGET	DDOS TECHNICAL DETAILS	RECENT POLITICAL CONTEXT
June 12, 2019	Telegram , ²³⁶ an encrypted messaging app popular among protest organizers. ²³⁷	200 to 400 Gbps, mostly composed of IP addresses geolocated to China ²³⁸	Large protests and a general strike were scheduled for that day, attempting to dissuade the Legislative Council from initiating a critical parliamentary step toward passing the extradition reforms. ²³⁹
August 31, 2019	LIHKG , ^{ab} a web forum, primary protest organizing space, and successor to HKGolden.	Great Cannon. More than 1.5 billion requests in 16 hours, at a maximum rate of 260,000 per second. ²⁴⁰	Widespread protests were planned for the fifth anniversary of Beijing announcing a plan for electoral reforms. ²⁴¹
October 1, 2019	LIHKG ²⁴²	Over 13 hours (9 a.m. to 10 p.m. local), the site received 29 billion requests with a maximum rate of 700,000 requests per second. ²⁴³	Widespread protests were planned to occur on China's National Day, the 70th anniversary of the country's founding. ²⁴⁴
November 24, 2019 ^{ac}	LIHKG ²⁴⁵	Great Cannon. Size and duration unknown (~7:20 am to UNK local) ²⁴⁶	Election day for the Hong Kong District Council. DDoS starting minutes ^{ad} before polls opened. ²⁴⁷

Also during this period, influence operations on various social media platforms and attributed to the PRC government²⁴⁸ attempted to discredit the protests, characterizing them as violent mobs.²⁴⁹ In addition, likely state-sponsored domestic surveillance operations frequently targeted people and entities related to the protest movement.^{250 251}

Attribution

The use of the Great Cannon directly links two of these DDoS attacks to China's government. The similar targets and timing of the other two 2019 DDoS attacks point to an unidentified actor supporting the PRC's interests.

Assessment

These DDoS attacks, combined with information and surveillance operations, likely served to mitigate the threat to China's political stability of a growing domestic democratic movement. These attacks specifically attempted to undercut the Hong Kong democracy movement by disrupting its organizing platforms; attacks consistently coincided with scheduled and sudden political developments that typically led to protests. In addition to the tactical effect of hindering political organizing, the attacks may have had the intended effect of signaling China's intent to use overwhelming force to stop the protest movement, if necessary.

^{ab} In recent years, **LIHKG** had risen as the spiritual successor to HKGolden, after that site cooperated with law enforcement to disclose a protestor's IP address in 2014 and began limiting political content. Its acronym name directly references HKGolden.

^{ac} The date of the attack was determined using primary source DDoS reports by users. Some English-language reporting dated the attack to November 25, which may be the result of not converting between Hong Kong's time zone and a researcher or reporter's local time.

^{ad} The earliest observed examples of social media users commenting on LIHKG being down started at 7:23 a.m. Hong Kong local time, minutes before polls opened. One early poster noted that "the 6 o'clock DDoS is on time." This statement reads like a comment about the punctuality of a train or bus. The tweet could be interpreted then as a joke that DDoS attacks targeted Hong Kong with such consistency and predictability as to be comparable to a train running on time.



THREATS TO FOREIGN INTERESTS

KEY FINDINGS

According to President Xi, China establishes its foreign policy goals and manages its relationships in different ways based on power dynamics.²⁵² In 2014, he said China sees foreign entities in four categories: major powers, neighbors, developing countries, and multilateral organizations. This dynamic plays out in China's differing uses of hard power in cyberspace, especially with respect to its less militarily powerful neighbors and its major global competitors.

China uses disruptive cyberattacks to manage its maritime claims with militarily inferior competitors in the South China Sea. Its cyberattacks can be retaliatory responses to assertions of competing territorial claims. Alternatively, they can also be provocative digital extensions of China's physical assertions of its claims. Cyberattacks likely serve to deter other countries from solidifying their claims while China grows its presence in the region. The adversaries behind these attacks typically present themselves as patriotic, unaffiliated hacktivist groups, but some of them are very likely directly affiliated with the PRC, possibly as undeclared PLA units or as militia units.

★ China primarily asserts its maritime claims through harassment by nominally patriotic hacktivist groups. Over the past decade, this harassment has evolved from simple defacement and DDoS attacks to multifaceted operations encompassing persistent access, targeted data leaks, exploitation of public address systems, and possibly disinformation. This change parallels the broader maturation of the PLA's cyber forces, which may enable more organizationally complex operations, involving multiple coordinated aspects executed over long periods.

★ This digital harassment closely mirrors Beijing's broader gray-zone strategy in the region. The PRC often exerts force against its territorial opponents via non-explicit military surrogates; it allegedly encourages fishermen from China to swarm and ram boats in disputed waters.^{253 254} These operations delay settlement of territorial disputes by maintaining a state of constant low-level conflict.²⁵⁵ Crucially, this cyber and physical harassment strategy causes minimal tangible damage and does not greatly endanger lives or critical sectors, managing the risk of escalation.

China also uses destructive cyberattacks to signal a position of strength to its regional peer and superior military competitors. It tends to conduct these operations when there is a growing—even if sometimes distant—likelihood of direct military conflict, such as the U.S.' pivot to Asia, Taiwan resisting a closer relationship with the PRC, and the reinvigoration of the persistent Indo-China border conflict.

- ★ China asserts its strength through targeted operations against critical infrastructure operators, such as in the energy, power, and ports-and-maritime-transportation sectors. These operations sometimes seek to gain access to industrial control systems, holding them at risk; it is unclear whether China has used this access to produce destructive effects. It is likely, however, that China is responsible for destructive attacks on business systems at energy and critical technology manufacturers.
- ★ These operations likely serve to rebalance power dynamics when China lacks clear military superiority. PLA doctrinal writing emphasizes the importance of using long-range attacks, including cyberattacks, to supplement the PLA's admitted "inadequacies," "promulgate strength," and thus achieve strategic goals.²⁵⁶ Also, this writing notes that such operations and preparations for large-scale conflict may deter war, enable PRC control of situations, and "create military conditions" for acceptable resolutions of conflicts. This strategy contrasts with China's use of less potent faux-hacktivist attacks against Vietnam²⁵⁷ and the Philippines,²⁵⁸ where China has a military superiority.





Figure 2. Competing National Claims in the South China Sea

3

THEME #3: COMPETING SOUTH CHINA SEA CLAIMS

China has long held disputed claims in the South China Sea. This body of water is encircled by the mainland territories of (clockwise from the north) China, Taiwan, the Philippines, Malaysia, Brunei, Indonesia, and Vietnam. China asserts that its maritime territory extends far south of its mainland, through much of this area, owing to a mixture of legal, historical, and geographic justifications. The territory holds much strategic value as a throughfare for commercial shipping and China's navy, a productive fishing area, an untapped source of hydrocarbons, and a military buffer zone with the U.S. and its partners.

In the past decade, China has urgently shored up its claims in the region. In 2010, PRC officials reportedly first began referring to the region as a "core interest" in closed diplomatic meetings, greatly expanding beyond China's more limited historical territorial claims to Taiwan and Tibet.²⁵⁹ The PLA has since stated that its South China Sea claims must be enforced as a matter of sovereignty, security, and development.²⁶⁰ Numerous factors contribute to this urgency: the economic and military development of China and rival claimants, internal demands that China restore its national prestige through control of its vicinity,²⁶¹ and the U.S. strategic pivot to the region.



CASE STUDY #7 RETALIATING AGAINST VIETNAM'S ASSERTION OF DRILLING RIGHTS (2011)

Political Context

On May 26, 2011, China sabotaged a Vietnamese offshore oil-and-gas survey. About 80 miles off Vietnam's coast, a trio of China Marine Surveillance patrol boats^{ae} repeatedly zipped past a PetroVietnam vessel, ignoring the ship's warnings and slicing through a mile-long seismic exploration cable.^{262 263} Beijing did not dispute the incident and insisted that Vietnam's oil-and-gas exploration had "undermined China's interests and jurisdictional rights" in the area.²⁶⁴ This incident was one of at least a dozen between 2009 and 2013 where military, law enforcement, and militia vessels from China allegedly attempted to ram, board, slice the cables towed by, or otherwise harass and intimidate non-PRC vessels in the South China Sea.²⁶⁵

Shortly thereafter, from June 3 to June 5, China participated for the first time at the ministerial level in the Shangri-La Dialogue, an annual Asian security summit attended by top defense and political leaders. At the conference, China's defense minister spoke about the need to resolve the claims in the South China Sea,²⁶⁶ reflecting a new PRC assertiveness and prioritization of this issue.

Cyber Activity

On June 2, a pair of self-described patriotic Vietnamese hackers defaced multiple PRC government websites with images and messages refuting China's claims in the South China Sea.^{267 268} For the next week, several ostensibly patriotic pro-PRC hacktivist groups mobilized to deface and disrupt with DDoS more than 200 Vietnamese government and commercial websites.^{269 270 271}

Attribution

Several involved hacktivists used the identities of prominent—but, at the time, allegedly retired—pro-PRC hacktivist

^{ae} China Marine Surveillance (CMS) is a paramilitary law enforcement agency that was absorbed by the PRC's coast guard in 2013. Its mission has been broadly characterized by its foreign detractors, including the U.S., as to harass other countries into acquiescence of the PRC's maritime sovereignty claims.

groups. Most notably, the attack allegedly included participation of the Honker Union of China (HUC),^{af} a collective of prolific patriotic hackers founded in the late 1990s, which, according to a statement posted on its website, dissolved in 2004.²⁷² At least three times between 2004 and 2010, seemingly different groups used the HUC name while launching patriotic attacks on foreign organizations.²⁷³ Then, in September 2011, after the attacks on Vietnam, the original group appeared to re-form; the founder of the original HUC re-launched its defunct website, under the auspices of being a network security company.²⁷⁴ For several years afterward, attackers calling themselves HUC periodically reappeared during international disputes, often involving the South China Sea, conducting DDoS and defacement attacks.^{275 276}

The exact relationship between HUC and the PRC is indeterminate in public sources. At a minimum, China's cyber apparatus has benefited from HUC's existence, historically using tools it developed, for example.²⁷⁷ A meaningful portion of the HUC community likely was eager to act at the government's request; in 2005, members of HUC's forum discussed their hope that the government would enlist HUC as an official cyber offensive unit.^{278 ag} Yet, at the same time, official party mouthpieces have occasionally chastised the patriotic hacktivists, referring to their activities as "Web terrorism ... unforgivable acts violating the law."²⁷⁹

Assessment

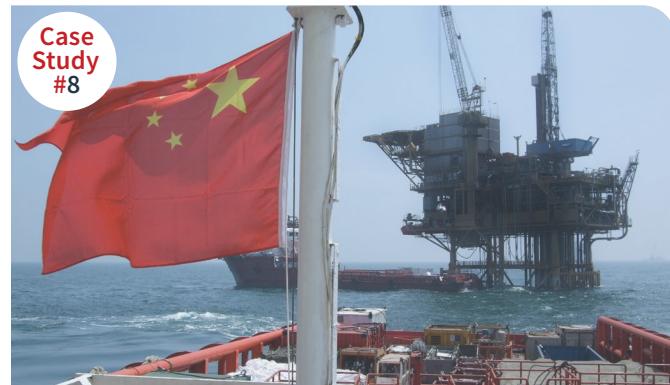
The actions of HUC, regardless of its specific relationship with the PRC state, mirror the PRC's broader use of gray-zone tactics in the South China Sea. China uses semi-state and irregular^{ah} actors, like the China Marine Surveillance and People's Armed Forces Maritime Militia, to harass countries disputing China's maritime claims. One PRC general described in 2013 how China exerts force in the South China Sea through non-military entities: surrounding contested

^{af} The Honker Union of China [中国红客联盟] (a.k.a. HUC, Red Hacker Alliance) is one of China's oldest and most prominent patriotic hacktivist groups. Honker is a Chinese internet slang term for a patriotic hacker. The word for a malicious hacker in Chinese, hōlikè (黑客), literally means a "black guest," akin to the English language concept of a "black hat hacker." The Chinese term "hóng kè" (红客, romanized as honker) means a "red guest," evoking the red color symbolic of the PRC and the CCP.

^{ag} According to one HUC forum user, "We need to move toward standardized honker unions. We can't wait until the nation has a crisis to act; we must be prepared to do something meaningful for the motherland. Why can't we become a government-approved network technology security unit?" (<https://web.archive.org/web/20090811031100/http://www.beijing2008conference.com/articles.php?id=101#3>)

^{ah} "Irregular" refers to the use of force by entities other than a state's combat forces. Formal definitions vary, but essentially "regular" forces by contrast are directly controlled by a state, openly acknowledge their affiliation with a state (e.g., through marked uniforms), openly represent themselves as combatants, and are held responsible by the laws of war.

territory with fishing boats, fishing enforcement agencies' ships, the coast guard, and naval warships, "wrapp[ing] territory] layer by layer like a cabbage."²⁸⁰ Through these tactics, China maintains a constant state of low-level, non-escalatory conflict, preventing its opponents from solidifying their claims either in practical or perceptible terms.



ASSERTING THE PRC'S DRILLING RIGHTS (2014)

Political Context

China launched its first deep-water oil rig in 2012. At a celebration of this accomplishment, the head of the country's national oil company declared that its large oil rigs constituted "mobile national territory and a strategic weapon."²⁸¹ This concept of a mobile platform as national territory is a political and legal gray area. By using a platform in such a way, China can establish an "aura of authority and control," establishing its claims in the South China Sea.²⁸²

On May 2, 2014, China deployed its deep-water oil rig, along with three service ships, for the first time into Vietnamese-claimed waters.²⁸³ China Marine Surveillance announced that the rig would drill until August 15 and that it was establishing a 1-mile-radius exclusionary zone.²⁸⁴ Over the following weeks, China repeatedly expanded this security cordon, ultimately to 10–15 miles. The two countries deployed vessels and aircraft to the zone, both sides accused the other of ramming attacks, and, unusually, anti-China protests broke out across Vietnam. Despite apparently attempting to intimidate and escalate, China abruptly relented by withdrawing the rig on July 15, a month early.²⁸⁵

Cyber Activity

The dispute quickly spilled into cyberspace, as patriotic attacks commenced. On May 9, 2014, hacktivists claiming to be from Vietnam attacked dozens of PRC government and commercial websites, mostly using DDoS.²⁸⁶ Over the following few days, attackers claiming to be part of the established pro-PRC hacktivist group 1937CN defaced in retaliation hundreds of Vietnamese commercial, educational, and government websites.^{287 288} The defacements declared, "since ancient times, the South China Sea belongs to China!"²⁸⁹

The rate of pro-China defacements in Vietnam surged again in late August. Between August 28 and September 4, attackers claiming affiliation with 1937CN and Sky-Eye Team defaced about 750 commercial, educational, and government websites.²⁹⁰ No corresponding political developments were observed during this period, but the operation appeared political, because it overlapped with Vietnam's Independence Day (a long weekend of August 30 to September 2 that year).²⁹¹ The defacements more explicitly mimicked official PRC messaging, referring to opportunities for "win-win" Development" and their shared histories being the victims of "unequal treaties" with mostly Western powers.²⁹² Vietnam CERT (VNCERT) observed that the attacks were different from the May defacements, because the attackers had "installed" unspecified malicious code in the websites.²⁹³

Reviewed sources do not detail the code's capability.



Figure 3. During Vietnam's 2014 Independence Day weekend, nominally pro-PRC hacktivist groups defaced hundreds of websites in Vietnam with statements echoing PRC policy slogans and messages.

Attribution

1937CN was a self-described patriotic pro-PRC hacktivist group, active from roughly June 2012 to July 2016. It conducted defacements that explicitly and consistently supported the PRC's maritime claims. Its targets were principally countries with competing maritime claims in the South and East China Seas: Vietnam,²⁹⁴ Philippines,²⁹⁵ and Japan.²⁹⁶ Its activity surged around periods of heightened geopolitical tensions over these claims but not other PRC geopolitical disputes. Speaking with China's Global Times, a 1937CN co-founder stated that "[m]any of the members work in" cybersecurity companies,²⁹⁷ and the QQ page of another co-founder stated that he attended the PLA Air Force's Command College, a prestigious mid-career officer training institution.²⁹⁸ ^{ai}

Commercial threat intelligence firms widely and credibly assess that 1937CN is effectively interchangeable with the mainly espionage-focused, PRC-aligned actor often called Goblin Panda. Just like the purported hacktivist group, Goblin Panda targets entities in Southeast Asia, mainly in Vietnam and frequently during periods of tension over the South China Sea.^{299 300 301} The two share overlapping histories; like 1937CN, Goblin Panda has been active since mid-2012.^{302 303 304}

For more information, refer to activity cluster 1937CN/Goblin Panda in Appendix A.

Assessment

The so-called hacktivist group 1937CN was most likely a formal offensive entity with a defined remit and mission. 1937CN demonstrated a narrow focus on China's maritime disputes—ignoring other geopolitical flare-ups involving China—and closely mirrored Goblin Panda's focus on the region and topic area. Based upon its overt, traceable organizational identity, complete with public faces and long-active forum, 1937CN may have been closer to a militia-like group composed of technologists that could be activated as needed by the state, rather than a traditional uniformed unit.

^{ai} **The Chinese People's Liberation Army Air Force Command College** (中国人民解放军空军指挥学院) is the PLAAF's highest academic institution. It trains mid- and high-level command officers, staff officers, and graduate students. It is analogous to the U.S. Air Force's Air War College. (Source: https://web.archive.org/web/20190610155031/http://www.mod.gov.cn/reports/201403/wzry/2014-09-12/content_4536788.htm)

**Case
Study
#9**



DISPUTING SOUTH CHINA SEA ARBITRATION FAVORING THE PHILIPPINES (JULY 2016)

Political Context

In January 2013, the Philippines asked the Permanent Court of Arbitration^{aj} (PCA) in the Hague to consider various South China Sea claims made by the Philippines and China.³⁰⁵ Beijing refused to participate. In a position paper, it argued that the UN treaty under which the Philippines sought to dispute the claims was irrelevant and beyond the court's jurisdiction. From China's stated perspective, the treaty covered sovereignty matters, not resource exploitation rights, and its asserted sovereignty in these areas was therefore not open to debate in this court.³⁰⁶

Regardless, in October 2015, the court agreed to consider the Philippines' case³⁰⁷ and, on July 12, 2016, fully ruled in its favor with unanimous consent on almost all counts.³⁰⁸ The tribunal found that China had no lawful claim to the Philippines' exclusive economic zone, it lacked any "historic rights" based on its "nine-dash-line" map,^{ak} and the so-called "islands" it claimed legally constituted "rocks," affording China very limited economic rights.³⁰⁹ China promptly refused to accept or recognize the ruling.³¹⁰

Cyber Activity

Immediately after the July 12 ruling, DDoS attacks targeted at least 68 Philippine government websites including national security agencies, the office of the president, the national

bank, and the government's top-level-domain registrar, as well as city governments, a hospital, and web portals of smaller towns.³¹¹ According to local media, the DDoS attacks "continued and surged again" the next day³¹² and concluded a few days later.³¹³

Also on the day of the decision, the PCA's website crashed for at least five hours^{314 315} and was intermittently available thereafter.³¹⁶ According to many Twitter posts, the website of the International Court of Justice (ICJ) was also temporarily offline;³¹⁷ the site eventually posted a message in English and Chinese noting that the ICJ shares space with the PCA but is otherwise unrelated,³¹⁸ having had "no involvement" in the ruling.³¹⁹ Reviewed sources do not detail the cause of these disruptions.

On July 16, two small Philippine municipal portals were defaced with Anonymous hacktivist imagery and language and signed "- Chinese Government."³²⁰ No specific group took credit for the defacements. Despite mentioning the "Chinese government," the defacement in no way referenced the PCA ruling or the South China Sea, offering only generic Anonymous-style language about the need for individual action to obtain freedom and justice.

Attribution

Based on a review of available public sources, neither the Philippine government, nor any other knowledgeable entity, has publicly attributed any of these attacks. The adversary or adversaries acted in China's interest and, in the case of the defacements, expressed support for its government. Based on the choice to deface two minor municipalities with little symbolic value, rather than the DDoS attacks against major Philippine government sites, the two activity clusters are likely unrelated. It is plausible that the PRC directed only the DDoS attacks (or even none of these attacks), whereas a sympathetic but otherwise unrelated actor may have conducted the defacements.^{321 322 323 324}

Assessment

The attacks were likely intended to signal PRC displeasure with the court for its unfavorable decision and with the Philippine government for initiating the proceedings. It is unclear, however, what responsibility Beijing had for any of the attacks. The attack on the ICJ, for example, which appeared to show a poor fundamental understanding of the dispute by the adversary, is unlikely to have occurred through specific, direct government tasking. The PCA's website was an established target of likely PRC state-sponsored activity, having been compromised in July 2015 to infect visitors to two pages devoted to the case's proceedings.³²⁵

^{aj} The **Permanent Court of Arbitration** (PCA) is a multinational institution offering legal resolution services to international parties—countries, organizations, and individuals. The PCA hears disputes among Hague Convention members, issues decisions, and assigns arbitral awards. Common disputes involve territorial and maritime boundaries, investment, trade, and human rights. The PCA is often confused with the co-located **International Court of Justice** (ICJ). The ICJ is a UN agency with the authority to issue rulings that can be enforced by the UN Security Council. By contrast, the PCA lacks an enforcement mechanism beyond shaming convention members who fail to abide by decisions.

^{ak} The "**nine-dash-line**" (九段線, jiǔduàn xiàn) is a demarcation line for China's territory in the South China Sea, first proposed by the Republic of China (now, Taiwan) and later the People's Republic of China (PRC). The line is a rare area of foreign policy on which Taiwan and the PRC collaborate.



DISRUPTING VIETNAM'S AVIATION SECTOR (JULY 2016)

Political Context

Since 2012, China has printed its nine-dash-line territorial claim on three pages of its passport. Vietnam's policy has been to not stamp these passports but rather stamp a removable piece of paper (i.e., a landing slip).³²⁶ According to China's press, on July 23, 2016, a group of four friends from China entered Vietnam by flying into Ho Chi Minh City's international airport. Allegedly, while passing through customs, an official defaced their passports.³²⁷ Pictures of the passports show that a common vulgar English-language expression of distain or contempt ("[Expletive] you") had been written over two of the pictures of the nine-dash-line.^{328 329} The incident broke in the press on July 27.³³⁰

No reports from Vietnam or statements by Vietnamese officials were identified that confirmed that any such passport defacement had occurred, but it was plausible given the current socio-political climate. Vietnamese displeasure about the line ran high. Earlier that week, Vietnamese press reported that, in the first half of 2016, border guards in one province had refused to stamp 6,703 PRC passports bearing the nine-dash line.³³¹ Concurrently, Vietnamese netizens called for boycotts on PRC celebrities who had promoted the nine-dash-line ruling.³³²

Cyber Activity

On July 29, self-described patriotic pro-PRC hacktivists affiliated with 1937CN conducted a series of attacks against the Vietnamese aviation sector. Despite appearing to be a response to the July 23 passport defacement incident, the attack leveraged data likely stolen in March. It is possible that the adversary purchased this data for the purpose of leaking it, but it is more likely that the attackers used persistent access to conduct this complex, highly coordinated operation against multiple related targets.

The adversary hijacked communications systems at airports by compromising an administrator's computer and gained persistent access throughout the network.³³³ The information screens at international airports in Ho Chi Minh City and Hanoi displayed messages in English declaring ("[EXPLETIVE]

VIETNAM PHILIPPINES JOINT ACTION"^{al}), denouncing their maritime claims, and claiming China's "territorial inviolability."^{334 335} For four minutes, the public address systems broadcast pro-China messages in English³³⁶ with similar content to the defacement³³⁷ and played patriotic music.³³⁸ The attack forced these airports to shut down computer systems and manually process customer check-ins,³³⁹ delaying more than 100 flights countrywide by up to two hours.^{340 341} Reportedly, up to 19 other airports across Vietnam experienced unspecified technical problems that day.³⁴²

The group also targeted Vietnam Airlines, the country's state-owned flagship carrier. Also on July 29, the attacker defaced the airline's website with imagery identical to the airport's information screens^{343 344} and directed visitors to Pastebin. The site hosted a download link to a file containing the personal information of more than 400,000 members of the airline's frequent flyer club.^{345 346} The file's timestamp indicates that it was created on March 25, 2016, using the airline's business management system.³⁴⁷ In response, several major Vietnamese banks temporarily froze credit cards.³⁴⁸



Figure 4. In July 2019, the 1937CN Team defaced airport information screens and Vietnam Airlines' website with anti-Vietnam and anti-Philippines messages.

Attribution

The Vietnamese government attributed these aviation attacks to Goblin Panda.³⁴⁹ This attribution is consistent with other private sector research that tracks Goblin Panda as the actor behind certain PRC-aligned espionage against Vietnamese entities. This assessment is further supported by reviewable technical evidence: attackers, for example, leveraged command-and-control servers^{350 351 352} repeatedly used by Goblin Panda in targeted operations against Vietnam since at least 2014.^{353 354 355 356}

Beyond the imagery used in the attacks, 1937CN did not take

^{al} The phrase "Vietnam Philippines Joint Action" may specifically refer to the **"Philippines-Viet Nam Action Plan 2017-2022,"** a strategic memorandum of understanding between the two countries being drafted in 2016. The two countries had signed another action plan six years earlier, concerning naval cooperation, information sharing, and other security matters.

credit in other channels. The group's leader, a publicly known PRC-based individual, denied that his group was behind the attacks but told a PRC news outlet that the attacks were consistent with his team's political agenda. He noted that at "a time when the definition of a cyber crime remains vague in China, our team will start a cyber war to defend the country and the people when their sovereignty and rights are violated by foreign countries."³⁵⁷ Unusually for them, neither this individual, nor 1937CN, reported the defacements on public defacement registration websites.^{358 359} By approximately October 2016, 1937CN disbanded its public presence, closing its forum, security blog, and social media accounts.^{360 361}

Assessment

This operation was very likely a highly coordinated and carefully planned cyber-enabled information operation, employing data leaks, defacements, and exploitations of public address and information systems. Collectively these appear designed to intimidate Vietnamese popular, commercial, and government audiences. The defaced passports story is suspect, as evidence suggests that the cyber operation began before this precipitating incident. It is therefore somewhat likely this story was disinformation.



THEME #4: INDO-PACIFIC COMPETITION

China perceives an increasingly antagonistic regional community.³⁶² In the past decade, other major regional players—the U.S., Japan, India, and Australia—began speaking of an "Indo-Pacific" geographic and political region centered on the Indian and Pacific oceans. This geopolitical perspective highlighted the region's growing strategic importance, owing to the emergence of the Indian Ocean as the world's busiest trade route, the development of China and India as the world's second and third largest economies,^{363 am} and the re-emergence of China as a geopolitical force. These major regional powers have strengthened their partnerships and advanced an increasingly coordinated technical, economic, and military agenda that China perceives as hostile containment.³⁶⁴ As *China Daily* warned this "sinister gang" of countries, "Once they step on the red line of China's core interests, China will not care about their relations with the U.S., and China will not hesitate to punish them."³⁶⁵



^{am} By all major macroeconomic measures, the U.S. and China are presently the world's first and second largest economies. India's ranking within the top 10 depends on the measure. By 2030, India is generally projected to become the third-largest economy by most measures.



PREPARING FOR THE U.S. PIVOT TO ASIA (2011–2013)

Political Context

At the start of the 21st century, the U.S. was cautiously optimistic about its increasingly important relationship with China. In 2000, the U.S. granted China permanent normal trade relations, allowing it to join the World Trade Organization.³⁶⁶ The 2006 National Security Strategy characterized China as a rising country in economic and political transition that could emerge as “peaceful and prosperous” and would face growing pressure to “follow on the path of East Asia’s many modern democracies.”³⁶⁷ Meanwhile, the U.S. focus on terrorism overshadowed China affairs or, as it has been widely characterized, “distracted” the U.S.^{368 369 370}

In the fall of 2011, the U.S. sharply changed its position. After more than a decade of deprioritizing the region, the secretary of state published a position paper arguing that the Asia-Pacific region must be a top “diplomatic, economic, strategic, or otherwise” focus of the U.S.³⁷¹ In November, President Barack Obama launched a regional tour affirming this new strategic prioritization, announcing the first long-term expansion of the U.S. military presence in the region since the Vietnam War.^{372 373} Beijing became visibly concerned. State media asked whether this pivot was “an attempt at containment,”³⁷⁴ and the Foreign Ministry diplomatically noted that military intensification in the region “may not be quite appropriate.”³⁷⁵

Cyber Activity

Starting in late 2011, an intrusion campaign targeted numerous U.S. natural gas pipeline operators. Between December 2011 and February 2012, the adversary attempted to gain access through spear-phishing and by social engineering phone calls to asset owners, such as to their network engineering departments.³⁷⁶ Out of 23 known targets, 13 were successfully breached. Remediation concluded in 2013. While inside networks, the adversary sought data related to the operators’ ICS, such as manuals and documents using the string “SCAD*,” which would identify references to supervisory control and data acquisition (SCADA) systems.³⁷⁷ One company established a honeypot containing sensitive decoy information; the adversary exfiltrated the SCADA-related information and ignored the business and financial documents.³⁷⁸

In September 2012, the APT1 threat group breached Telvent³⁷⁹ and stole customer project files related to its OASys SCADA project, a pipeline management system.^{380 381} The systems are typically customized for each customer’s requirements and therefore may contain substantial information about pipeline operators’ environments.³⁸²

Attribution

The U.S. government publicly attributed the late 2011 pipeline operator intrusions to unspecified “Chinese state-sponsored actors.”³⁸³ The U.S. assessed that the adversary sought to obtain the ability to disrupt physical operations through the remote manipulation of industrial control systems and thus hold infrastructure at risk.³⁸⁴

Meanwhile, the theft of pipeline management software from Telvent is attributed to PLA actors tracked as APT1.³⁸⁵ According to the U.S. government, APT1 was affiliated with the PLA General Staff Department’s Third Department (3PLA) and used military cover unit designator Unit 61398.³⁸⁶ Historically, the PLA’s cyberattack capabilities resided within 4PLA, rather than the collections-focused 3PLA.³⁸⁷ It is plausible then that APT1 was playing a supportive role to a parallel 4PLA destructive team. The stolen SCADA files probably held little economic espionage value but would very likely be useful for offensive operations against pipeline operators.

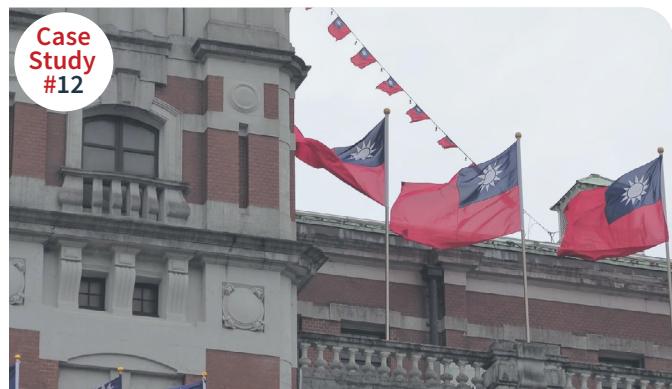
The pipeline intrusion actor may be affiliated with the actors that breached RSA around the same time. In March 2011, according to the U.S. government, a PRC-affiliated threat actor compromised RSA’s SecureID hard tokens and used them to target U.S. defense contractors.^{388 389} The RSA intrusion and the late 2011 oil-and-gas intrusions share indicators of compromise related to tools and command-and-control domains.³⁹⁰ This overlap indicates that the two operations were likely conducted by related actors with a common tooling and infrastructure source. RSA assessed that the breach was likely a joint operation by two state-backed groups.³⁹¹ Knowledgeable security firms also assessed a joint PLA and MSS operation, possibly involving the MSS-linked³⁹² APT17^{393 394} and an unspecified PLA group other than APT1.^{395 396}

This 2011–2012 oil and gas operator intrusion and Telvent breach are likely not directly related to the then-long running Night Dragon campaign. From at least 2009 until 2011, a PRC-aligned threat group conducted targeted intrusions against global energy companies. Inconsistent with the honeypot anecdote, these actors sought project-financing information for oil-and-gas operators, as well as data from field production SCADA systems.³⁹⁷ This behavior suggests Night Dragon had a likely economic espionage objective rather than pre-positioning. In addition, Mandiant assessed that its APT1 group did not relate to Night Dragon.³⁹⁸

For more information, refer to the activity cluster APT1 in Appendix A.

Assessment

Concerns over the U.S. pivot to Asia may have prompted China's desire to establish pre-positioning within the U.S. energy sector. At the time, China had only recently begun its military modernization and had few policy options to threaten harm or signal strength to the U.S. through hard power projection.^{399 400} Relative to other options, cyber pre-positioning might more quickly give China the ability to influence U.S. decision makers through a hold-at-risk strategy. This action could then be seen as a strategic prelude to China's establishment of new bases throughout the South China Sea over the next decade, enabling rapid strike capabilities throughout the region.^{401 402}



ATTEMPTING TO INTIMIDATE RESISTANT POLITICIANS IN TAIWAN (MAY 2020)

Political Context

Taiwan, officially the Republic of China, is a democracy with unclear sovereignty. The changing administrations in Taiwan over the decades have had differing opinions on Taiwan's relationship with the PRC, but the current administration of Tsai Ing-wen has been less conciliatory. After her first 2016 election, she declined to explicitly reaffirm the ambiguous "One China"^{an} concept that had been the basis of cross-strait relations for decades.⁴⁰³ In retaliation, the PRC ended diplomatic contact with Taiwan.

In January 2020, President Tsai and her party won landslide victories in national elections. They ran on a platform firmly opposed to PRC's offer of a "One Country, Two Systems" relationship, like the PRC and Hong Kong.⁴⁰⁴ Her reelection alarmed Beijing, which warned that Tsai had a "persistent penchant for provocative moves" and would "push her

^{an} Allegedly, in 1992, the PRC and Taiwan verbally agreed to a political baseline for their relationship: there is only "**One China**." However, the supposed agreement left this phrase's meaning open to interpretation. The PRC holds that there is only China and Taiwan has always been part of China. For many years, Taiwan's official interpretation was that a singular China exists, but there is no consensus about which government represents China.

pro-independence agenda at whatever cost."⁴⁰⁵ Via the Taiwan Affairs Office,^{ao} the PRC vowed to uphold China's "territorial integrity [and] resolutely oppose separatist attempts and acts for 'Taiwan independence' in any form."⁴⁰⁶ On May 20, Tsai was re-inaugurated.⁴⁰⁷

Cyber Activity

At some point in early 2020,^{ap} an adversary breached at least 10 Taiwanese companies in strategically important sectors using diverse means and obtained persistent access.^{409 410} Victims included Taiwan's national gasoline, natural gas, and petrochemical company; one of the world's largest chemical companies; Taiwan's largest telecommunications provider; and three semiconductor firms (one of which is one of the world's largest semiconductor assembly and testing services).^{411 412 413 414}

Over the May 1 to May 3 Labor Day holiday weekend, the adversary used backdoors to distribute ransomware using victims' centralized management and configuration systems.^{415 416} The ransomware contained a logic bomb, activating on systems starting on May 4 if their system times were after noon. The ransomware note provided an email address, but no demanded ransom amount or threat to leak files.^{aq} Investigators identified a newer variant of the ransomware after the attack that omitted contact and payment information, reducing the malware to a purely destructive tool.⁴¹⁷ The attack's publicly observable effects included partially disrupting payment systems at many of Taiwan's gas stations, causing some to temporarily shut down.^{418 419}

Attribution

The U.S. government has attributed the ransomware attacks to Chengdu 404, a self-described cybersecurity firm located in Chengdu, China.⁴²⁰ The U.S. government stated that the operators were affiliated with the **APT41** threat group, a group often also tracked as the Winnti Group. This assessment aligns with earlier attribution by the Taiwanese government, which linked the attack to the Winnti Group or another closely related threat group.⁴²¹

^{ao} The **Taiwan Affairs Office** is the government agency responsible for setting and implementing mainland the PRC's policies regarding Taiwan.

^{ap} Reviewed public sources have not specified the start of this campaign beyond it occurring "several months" before the early May disruptions.

^{aq} **Ransom demands:** A senior Taiwanese government investigator, speaking shortly after the incident, mentioned that victims' computers had displayed a message demanding 3,000 USD. Neither this message nor figure were repeated by any known involved incident response firm, generated by any known samples, or repeated by any other reliable source. The Taiwanese government media's English and Mandarin-language versions of the same reporting differ on several specific points, adding to the confusion. (Sources: <https://tw.news.yahoo.com/中油台塑化遭駭-調查局-駭客擬再攻擊10企業-081347026.html>; <https://www.taipeitimes.com/News/taiwan/archives/2020/05/17/2003736564>)

Chengdu 404 likely engages in a mixture of for-profit crime and contracting for the PRC security apparatus. Its work likely includes a mixture of surveillance and espionage. The firm has reportedly targeted government organizations in Vietnam, India, and Hong Kong; nonprofit entities, such as think tanks and a news organization that covered Uighur issues; and pro-democracy activists and politicians in Hong Kong.⁴²² The U.S. alleges that the company has a long history of working with the MSS.⁴²³ The company's website further stated that its customers included "public security, military, and military enterprises,"⁴²⁴ presumably referring to the MPS, PLA, and PRC defense companies.

The line between Chengdu 404's contracted work and for-profit crime is blurry. The U.S. states that Chengdu 404 frequently targeted video game companies.⁴²⁵ The operators allegedly stole "digital items of value" (e.g., video game currencies), disrupted competing criminal groups, and stole customer databases.⁴²⁶ Private sector tracking of Winnti^{427 428 429 430} documents this recurring targeting of video game companies, often resulting in the theft of code-signing certificates.^{ar} Some of these certificates have been used for surveillance activities closely aligned with PRC government interests, such as targeting Uighur and Tibetan activists.⁴³¹ It is plausible that the PRC tasks the group to perform specific activities, while allowing it to perform criminal activities on the same victim networks.

For more information, refer to the activity cluster Chengdu-based individuals in Appendix A.

Assessment

This attack in Taiwan was likely orchestrated to intimidate the reelected Tsai administration and express displeasure with its handling of the cross-Straits relationship. The targets all had cross-Straits geopolitical significance as critical members of Taiwan's technology and energy sectors. The adversary also patiently waited for many months to act on objectives; the operational timeline loosely overlaps with the reelection and inauguration of President Tsai. A parallel incident might then be China deploying warplanes near Taiwan on January 23, 2021, widely seen as a signal directed at President Joe Biden, inaugurated days earlier. The actions were described by the U.S. as part of a "pattern of ongoing PRC attempts to intimidate its neighbors, including Taiwan."⁴³²

Chengdu 404's known criminal behavior may have served as a useful veneer of plausible deniability for Beijing. This scenario fits into the broader pattern of China using semi-state actors, like militias and enlisted patriotic hacker groups, to exert pressure on its competitors.



**Case Study
#13**

DISPUTING THE BORDER WITH INDIA (2020–2022)

Political Context

For decades, China and India have disputed the specific location of their 2,100-mile border. On several occasions, the countries have come to blows or nearly so, as troops have mobilized, conducted skirmishes, and, as happened in 1962, even engaged in a short war. This persistent conflict has compelled these nuclear-armed neighbors to improve infrastructure near the border, installing roads, building airbases, laying railroads, and reportedly deploying air defenses.⁴³³

A new period of heightened tensions began in May 2020. Troops clashed repeatedly, escalating over several weeks from brawling and stone-throwing^{434 435} to incidents resulting in dozens of fatalities, as China occupied a new section of disputed territory.⁴³⁶ This was the first fatal military conflict between the two countries since 1975.⁴³⁷ The conflict has persisted into 2022, as small skirmishes occurred periodically,⁴³⁸ talks broke down,⁴³⁹ and new forces were detached to the region.⁴⁴⁰

Cyber Activity

As cross-border relations deteriorated, a targeted intrusion operation against the Indian power grid and port operators picked up momentum.⁴⁴¹ Between mid-2020 and March 2021,⁴⁴² an adversary breached 10 power sector organizations and two ports in India, based on analysis of ShadowPad command-and-control traffic by Recorded Future.⁴⁴³ In November 2020, India's CERT sent out a warning about the threat of ShadowPad malware to POSOCO's^{as} regional electric-grid load-balancing centers (a.k.a. dispatch centers).⁴⁴⁴ In March 2021, the Indian government confirmed that, in an unspecified timeframe, "cyber incidents" had occurred at four of the five regional dispatch centers under POSOCO's management.⁴⁴⁵

It is unclear whether a cyber intrusion facilitated an October 2020 power outage in Mumbai. Indian government authorities have offered conflicting root cause assessments for this incident. India's power minister rejected claims of any

^{ar} Software developers use **code-signing certificates** to establish that they published some code and that this code has not been altered after publication. By signing malware with a trusted organization's certificate, an adversary might slip by defenses that check code-signing against trusted developer lists before allowing installation of new software.

^{as} **Power System Operation Corporation** (POSOCO) is the Indian state-owned enterprise responsible for integrated operation of the national power grid, its security, and load balancing among regional dispatch centers.

cyber-facilitated sabotage, blaming human error alone, sourcing two investigations.^{446 447 448} He did however note that, at that time, unattributed “cyberattacks^{at...} [had]... happened on SCADA systems” in Mumbai and data theft had occurred at the city’s power company.⁴⁴⁹ Furthermore, targeted intrusions had occurred at regional dispatch centers without breaching operational systems.^{450 451 452} At the same time, the regional energy minister responsible for Mumbai insisted in the contrary that cyber-facilitated sabotage had indeed occurred.⁴⁵³ At a minimum, these reports consistently indicate that an adversary or adversaries targeted operational systems for India’s power grid in 2020, regardless of their disputed hand in the disruption.

At an unknown time, a suspected PRC-aligned threat group breached an Indian⁴⁵⁴ managed service provider (MSP) and operational technology (OT) vendor; the breach was identified in April 2021.⁴⁵⁵ It is plausible, but unknown, whether the adversary abused the vendor’s ongoing VPN access to major electric and water utilities in the UK or any other organizations in the vendor’s global customer base.⁴⁵⁶

Between approximately September 2021 and March 2022, another suspected PRC-aligned threat group breached at least seven Indian state power dispatch centers near the disputed border, the Indian subsidiary of a multinational logistics company, and an Indian national emergency response system. Recorded Future reported observing no evidence of adversary access to ICS environments.⁴⁵⁷

Attribution

Although Indian officials noted that they had considered PRC involvement in the initial 2020–2021 intrusions at ICS operators, no Indian agency or other public government source has publicly attributed them. Based on the target set, affiliations of technically related threat actors, and statements by Indian law enforcement, at least some of the threat activity is plausibly linked to the Western Theater Command of the PLA.

★ In November 2020, Indian law enforcement reported observing a recent uptick of DDoS, IP hijacking, and phishing originating in Chengdu, China, targeting critical infrastructure, banking, and “information” sectors, leading them to consider China’s possible involvement.⁴⁵⁸ Possibly of relevance, the Western Theater Command of the PLA is responsible for executing the kinetic aspects of the standoff with India and has a joint operations command center^{au} in Chengdu.⁴⁵⁹

★ Recorded Future research supports the Indian government’s assessment that the intrusions may have originated in Chengdu. The security firm attributed the activity to RedEcho, whose infrastructure and targeting reportedly strongly overlaps with Chengdu-based⁴⁶⁰ APT41⁴⁶¹ and the possibly Shenyang-based⁴⁶² Tonto Team.

Less is known about the adversaries responsible for the Indian OT vendor breach or the state dispatch center breaches. Limited overlaps in infrastructure and tooling indicate that the adversary or adversaries are probably also PRC state-linked, but not enough reviewable evidence is available to attribute the activity to existing threat groups.⁴⁶³

In apparent reference to the September 2021 to March 2022 activity, the Indian government unequivocally stated in April 2022 that “Chinese hackers” had twice targeted electricity distribution centers in the Ladakh region, which borders China.⁴⁶⁴

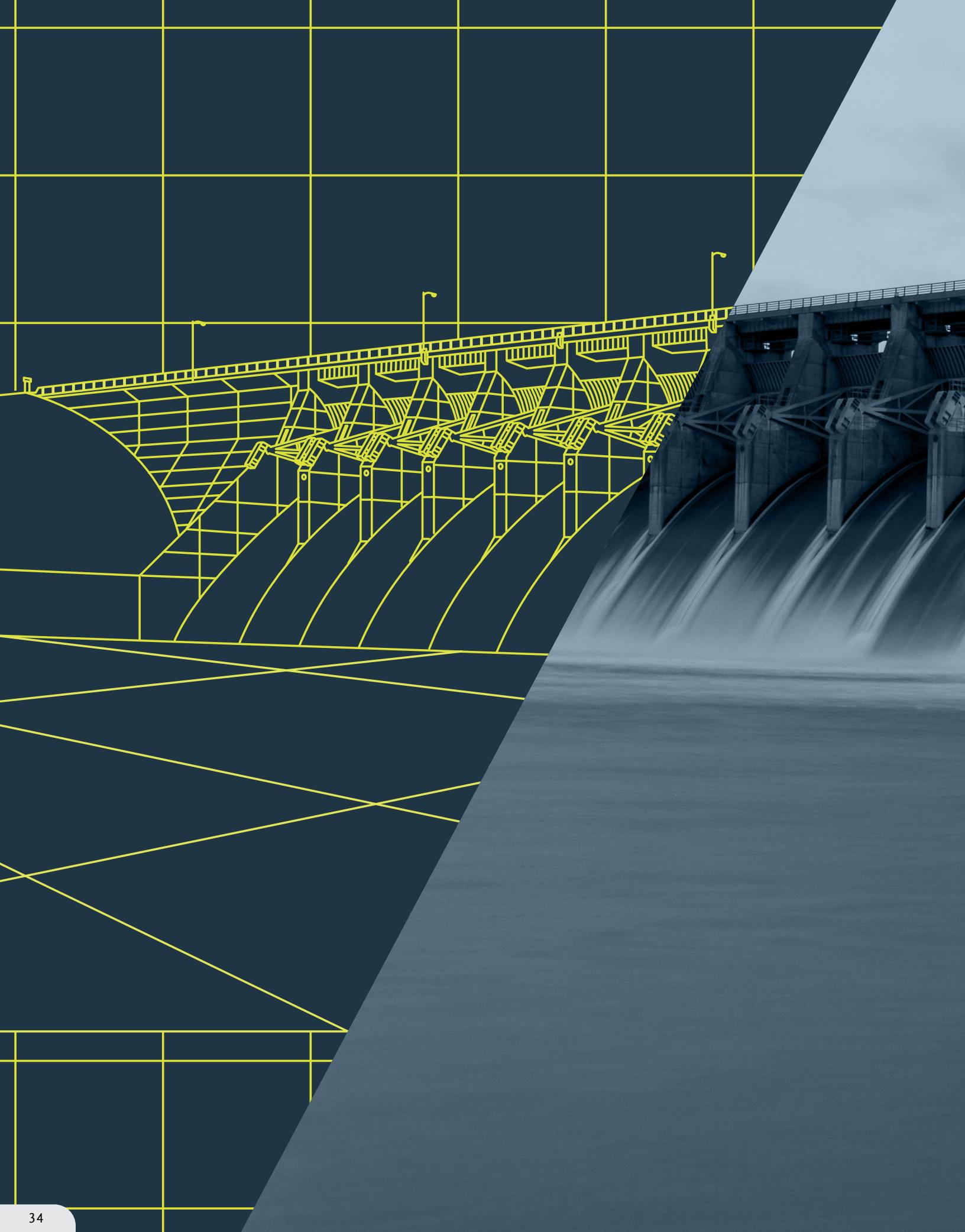
For more information, refer to threat actors and activity groups RedEcho, Chengdu-based individuals, and Tonto Team in Appendix A.

Assessment

★ Some of these intrusions likely served to degrade Indian public and executive will to continue or escalate the border conflict. PLA texts have long advocated for the targeting of an opponents’ critical infrastructure during conflicts, historically by artillery⁴⁶⁵ and later cyberattacks.⁴⁶⁶ As a 2013 doctrinal publication noted, “effective strikes against important strategic targets, including enemy military, economic, and political targets” can shape an opponent’s public opinion and executive decision making. These operations force an opponent to “[lose] confidence, [lose] the will to fight and...submit.”⁴⁶⁷ These intrusions align with this advocated strategy, targeting India’s utilities, ports, banking, and “information sectors” and, in some cases, likely seeking the ability to manipulate control systems.

^{at} The minister’s specific intended meaning of the phrase “cyberattack” could not be discerned from context and may not meet the strict, narrow definition of “cyberattack” used by this report.

^{au} Joint Operations Command Centers have been credibly assessed to be one of two possible organizations likely responsible for the operational command of the PLA SSF’s cyber units. (Source: https://ndupress.ndu.edu/Portals/68/Documents/stratperspective/china-china-perspectives_13.pdf).



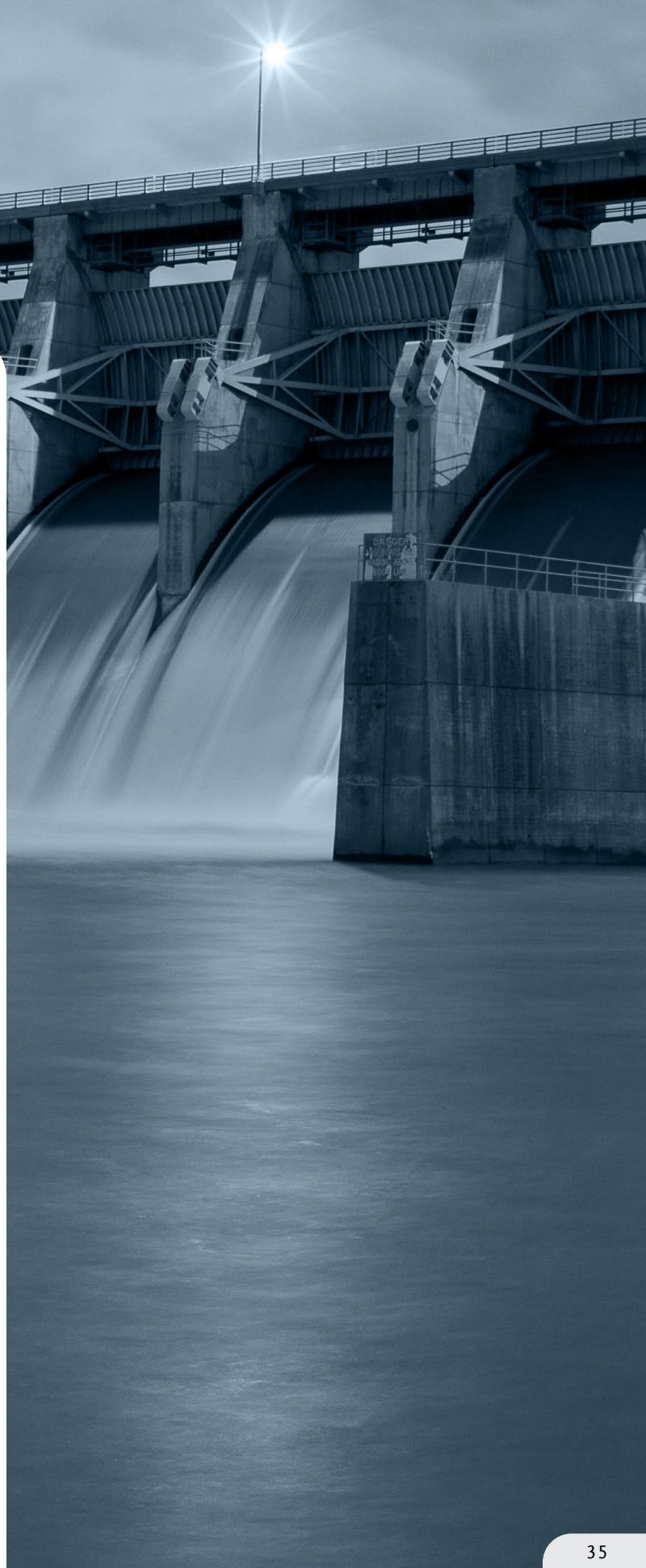
CONCLUSION

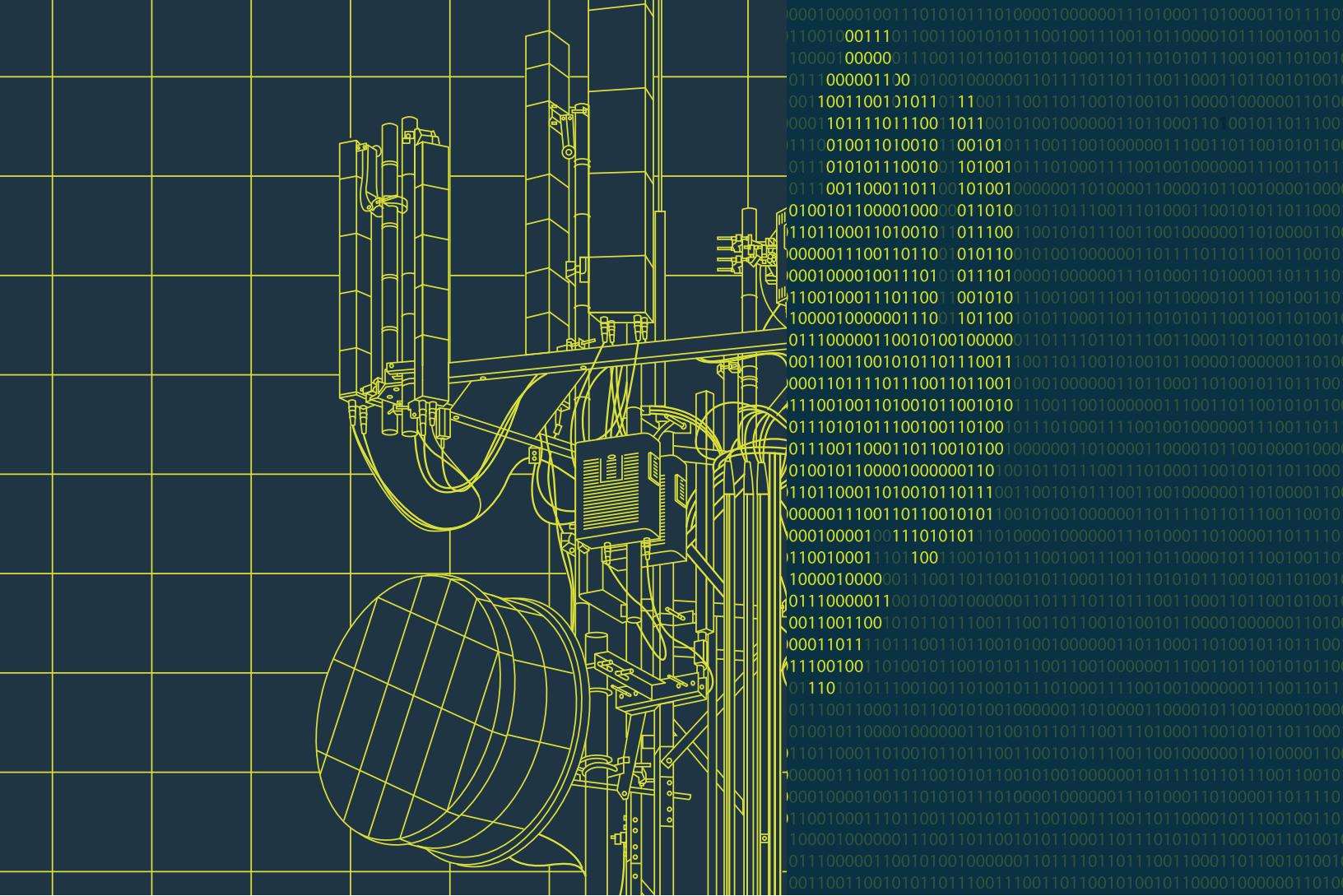
Discussions of the cyber threats posed by China must include espionage, influence, and attack operations. Case studies show that China is developing and deploying cyberattack capabilities to advance its national “core interests.” These cyberattacks complement China’s better known, increasingly assertive, and diverse attempts to advance its interests online through legal, financial, cultural, political, and technical means.

Beijing’s increasing confidence in its cyberattack capabilities shows in its national military documents. China’s 2015 military strategy framed the country as a “major victim of cyberattacks,” necessitating the rapid “development of a [military] cyber force.”⁴⁶⁸ An updated version of this paragraph appeared in China’s 2019 national defense paper; this time, China more boldly described itself as a “major cyber country” and stated that the PLA was developing cyberspace capabilities in ways “consistent with ... [this] ‘status.’”⁴⁶⁹ China states that it seeks to become the leading global cyber power by 2035.⁴⁷⁰

Beijing’s assuredness is likely well founded. In the past decade, China has better defined the missions of its cyber-capable agencies and more efficiently reorganized operational units. China now includes both offensive and defensive operators in joint military exercises.⁴⁷¹ The case studies in this report show a shift from crude shows of force—barely distinguishable from common hacktivism—to carefully timed operations exploiting persistent access to cause precise effects timed to support messaging and useful narratives. The true measure of China’s cyberattack capabilities, however, likely cannot be fully discerned in open sources. It is possible China has chosen to not deploy its full capabilities or it has done so without public attribution.

China’s growing cyberattack capabilities and global assertiveness create a potent threat to the United States and other countries and organizations whose own priorities, goals, and actions conflict with China’s expanding core interests. The time to prepare for this threat is now.





APPENDIX A: THREAT ACTORS AND ACTIVITY CLUSTERS

This appendix details the threat actors and activity clusters mentioned in this report. Each sub-section first describes the adversary or operation linked to a mentioned attack (attribution may be from a government or private-sector research organization). The tables then expand to capture the assessments of different threat research organizations that connect their own interchangeable and affiliated groups. This appendix generally does not attempt to significantly deconflict or exclude stated threat actor aliases, except when asserted clustering was very likely erroneous.

HURRICANE PANDA

Hurricane Panda is a PRC-aligned threat actor that conducted the mid-to-late 2014 DDoS attacks against Hong Kong pro-democracy entities, as well as espionage and intellectual property theft in East Asia and the U.S. circa 2013–2015. A notable feature of this threat actor was its use of legitimate code-signing certificates, likely stolen from South Korean companies. Threat research groups disagree about whether this actor can be directly linked to additional activity outside the 2013–2015 period. The following table captures the narrowest public tracking of its activity.

ACTIVITY GROUPS OR CLUSTERS ASSOCIATED WITH HURRICANE PANDA		
ACTIVITY GROUP OR CLUSTER	CITED ALIGNMENT	DESCRIPTION
Operation Poisoned Hurricane	FireEye ⁴⁷²	FireEye tracked Operation Poisoned Hurricane as activity by a suspected China-based threat actor supporting PRC government objectives. Overlaps in tools and infrastructure led FireEye to connect the mid-to-late 2014 distributed denial of service (DDoS) attacks against Hong Kong entities to earlier 2014 espionage and intellectual property theft. ⁴⁷³ The name likely refers to the threat actor's abuse of internet service provider Hurricane Electric's public domain name system (DNS) resolution service to route command-and-control traffic. ⁴⁷⁴ This adversary used legitimate code-signing certificates likely stolen from South Korean technology companies.
Hurricane Panda	CrowdStrike	CrowdStrike tracked a suspected China-based adversary primarily conducting targeted intrusions at telecommunications, technology, and infrastructure ⁴⁷⁵ companies since mid-2013 ⁴⁷⁶ as Hurricane Panda . ⁴⁷⁷ CrowdStrike noted the adversary's abuse of Hurricane Electric's DNS resolution service and use of PlugX malware and the ChinaChopper webshell. ^{478 479} The firm observed that its known targets were in the U.S. and Japan and it engaged in intellectual property theft. ⁴⁸⁰ The group was active until at least January 2015. ⁴⁸¹
Unnamed Hong Kong and Japan activity cluster	Volexity ⁴⁸²	Volexity identified a cluster of websites belonging to Hong Kong pro-democracy groups, as well as major Japanese newspaper Nikkei, similarly compromised with JavaScript to deliver unknown payloads hosted on the same domain. ⁴⁸³ This domain was also used for the command-and-control of DDoS against Hong Kong news sites in October 2014. ⁴⁸⁴ The malware used a legitimate code-signing certificate from a South Korean gaming company. Many portions of this activity were explicitly reported by FireEye as being part of Operation Poisoned Handover (a.k.a. Operation Poisoned Hurricane).
Unnamed activity cluster	Palo Alto Networks ⁴⁸⁵	Palo Alto Networks identified targeted summer 2014 intrusions against the regional office of an unspecified international law firm and a major university, both in East Asia. ⁴⁸⁶ The adversary used legitimate code-signing certificates stolen from several South Korean firms in software development, semiconductor, and automotive manufacturing; at least one of these certificates was used in Operation Poisoned Hurricane . Hence, Palo Alto Networks assessed this activity was closely related to Operation Poisoned Hurricane.
Operation Poisoned Helmand	ThreatConnect ⁴⁸⁷	ThreatConnect saw overlaps between suspected PRC political espionage activity in Afghanistan and the Operation Poisoned Hurricane -related activity reported by FireEye and Palo Alto Networks, all in the second half of 2014. The Afghanistan activity clusters had overlapping malware code and similar naming conventions and URL structures for command-and-control domains. ⁴⁸⁸ ThreatConnect did not publicly assess that these two campaigns were conducted by the same operators.

Some threat researchers connect Hurricane Panda to the actor responsible for the historic breach of Anthem Insurance, very likely part of a major counterintelligence campaign. We assess that this adversary connection is plausible. The two threat actors very likely share common tooling sources and both may have targeted the Hong Kong democracy movement in 2014. However, there is not sufficient information available to assess with high confidence whether Hurricane Panda and the Anthem actor are collaborators, parallel entities, or the same. Hence, the table below provides information about the Anthem actor for reference but does not attempt to capture all alternative aliases for the Anthem actor.

The U.S. government publicly attributed the Anthem operation to an unspecified threat group based in China and indicted two members (one of whom resides in Shenzhen).⁴⁸⁹ Based mainly on DNS-record pivoting, several security researchers have credibly assessed a connection between the Anthem actor, Beijing TopSec (a cybersecurity company and cleared PLA vendor), and an academic at Nanjing's Southeast University who has received MSS funding.^{490 491} In the early 2000s, Beijing TopSec reportedly employed the founder of the Honker Union of China, a hacktivist group referenced in this report.⁴⁹²

ACTIVITY GROUPS OR CLUSTERS ASSOCIATED WITH THE ANTHEM BREACH		
ACTIVITY GROUP OR CLUSTER	CITED ALIGNMENT	DESCRIPTION
Ironman campaign	CrowdStrike ⁴⁹³	<p>CrowdStrike initially assessed that the actor responsible for the Anthem breach was Deep Panda,⁴⁹⁴ but later revised this assessment to track the activity as a separate Ironman campaign. This campaign name refers to a command-and-control domain, xha-mster[.]com, which was registered with the alias “tony starke,” an apparent misspelling of “Tony Stark” (a.k.a. Ironman), a superhero from the Avengers franchise.⁴⁹⁵ A similar naming scheme reappeared in the China-attributed breach of the U.S. Office of Personnel Management (OPM). Despite CrowdStrike’s reassessment, many other threat research organizations track the actor responsible for Anthem as Deep Panda.</p> <p>Of relevance to Hurricane Panda’s DDoS activity in Hong Kong, CrowdStrike attributed targeted surveillance of prominent pro-democracy activists and supporters of the 2014 protests to Deep Panda.⁴⁹⁶ Also similar to the Hurricane Panda activity, the Ironman campaign used code-signing certificates from South Korean companies.</p>
Black Vine	Symantec ⁴⁹⁷	<p>Symantec identifies the threat actor behind the Anthem breach as a PRC-aligned espionage group tracked as Black Vine and assesses that some relevant individuals are affiliated with the Beijing TopSec security company.⁴⁹⁸ Symantec noted in 2015 that the group had targeted energy, aerospace, healthcare, military, and other sectors since 2012, overwhelmingly in the U.S. Symantec assessed that Black Vine likely has access to a shared tooling source used by multiple PRC-aligned threat groups.⁴⁹⁹</p>
Temp. Avengers	iSight Partners ⁵⁰⁰	<p>iSight Partners (now part of Mandiant) tracked the Anthem threat actor as Temp.Avengers, presumably a reference to its fraudulent domain registrations listing Avenger characters like Tony Stark. iSight also attributed this group to breaches at United Airlines and OPM. It is unknown whether iSight recognized any other industry names for the threat actor.</p>
Beijing TopSec and Southeast University affiliated actors	ThreatConnect ⁵⁰¹	<p>ThreatConnect assesses that the threat actors responsible for the Anthem breach are likely affiliated with a closely connected group of academics at Southeast University and private-sector technologists at Beijing TopSec, a cleared PLA contractor. ThreatConnect noted that, in the early 2000s, Beijing TopSec reportedly employed the founder of pro-PRC hacktivist group Honker Union of China (HUC), which is referenced in this report. Around 2011, HUC reemerged again under this individual’s leadership.^{502 503}</p>
APT31	Mandiant ⁵⁰⁴ IronNet ⁵⁰⁵ Positive Technologies ⁵⁰⁶ Rapid7 ⁵⁰⁷	<p>Mandiant tracks APT31 as a PRC-aligned espionage actor that collects data of political, economic, and military value to the PRC government and state-owned enterprises. It targets numerous sectors including government, international finance, aerospace, defense, high-tech, construction, engineering, telecommunications, media, and insurance.⁵⁰⁸ Mandiant does not publicly recognize any equivalent aliases.</p> <p>IronNet tracks APT31 as a PRC state-sponsored espionage actor supporting government and state-owned enterprises since 2013. IronNet assesses that APT31 is interchangeable with Hurricane Panda, Judgment Panda, Bronze Vinewood, Red Bravo, and Zirconium.⁵⁰⁹</p> <p>Positive Technologies tracks APT31 as an espionage actor that targets military, political, and commercial entities in diverse fields and has been active since at least 2016. Positive Technologies considers APT31 to be interchangeable with Hurricane Panda and Zirconium. It is unclear why Positive Technologies clusters APT31 and Hurricane Panda but is not confident that this activity began before 2016.</p> <p>Rapid7 tracks APT31 as a PRC state-sponsored group that conducts intellectual property theft. It recognizes common APT31 aliases as Bronze Vinewood, Hurricane Panda, Judgment Panda, TEMP.Avengers, and Zirconium.⁵¹⁰</p>

1937CN TEAM/GOBLIN PANDA

1937CN Team was a group of self-proclaimed pro-PRC hacktivists active from 2012 to 2016. The group primarily conducted defacement attacks against countries whose maritime territorial claims competed with China's own. According to government and private-sector research, 1937CN is effectively synonymous with an espionage-focused group often called **Goblin Panda** that mainly targets China's South China Sea competitors and has been active since 2012. It is plausible these two are closely linked subgroups under unified command (e.g., a militia unit and a uniformed unit).

In addition, several threat research groups credibly assess a relationship between Goblin Panda and APT40 via joint activity tracked as Hellsing. This relationship would be consistent with the overlaps in Goblin Panda and APT40's targeting profiles. The U.S. government has stated that APT40 is affiliated with the Hainan State Security Department of the MSS,⁵¹¹ which similarly focuses on Southeast Asia and Australia. Goblin Panda might then be a parallel military entity. A plausible candidate with this profile is whatever PLA entity succeeded Unit 75770 (75770部队), the signals intelligence unit for the now-defunct Guangzhou Military Region.⁵¹² After 2015 PLA reforms, that region has been reorganized as part of the Southeast Asia-focused Southern Theater Command.

ACTIVITY GROUPS OR CLUSTERS ASSOCIATED WITH 1937CN TEAM / GOBLIN PANDA		
ACTIVITY GROUP OR CLUSTER	CITED ALIGNMENT	DESCRIPTION
1937CN Team (a.k.a. 中国网军公盟, 1937cN TeAm, 1937CNTEAM, 1937CN)	Self-`proclaimed	<p>1937CN Team was a self-described pro-PRC hacktivist group. Though its leaders claimed that the group was founded in 2008,⁵¹³ its publicly observable activity spanned only 2012–2016. The 2008 start date likely refers to an earlier iteration, because the group's wiki notes that it was founded in June 2012 as a follow-up to the defunct group "Northwest Hacker Base" (西北黑客基地).⁵¹⁴ 1937CN's name refers to the 1937 massacre of Chinese civilians by imperial Japanese soldiers in Nanking (modern day Nanjing) during the Second Sino-Japanese War.⁵¹⁵ The group claimed to have disbanded in August 2016 because of an internal power struggle and differing opinions over the group's direction.^{516 517} During its existence, the group's primary activity was defacement attacks.</p> <p>In public interviews, 1937CN Team leaders claimed to have had no role in the Vietnamese aviation sector operation.⁵¹⁸</p> <p>Bkav considers 1937CN Team to be a PRC-based group responsible for the Vietnamese aviation sector operations.⁵¹⁹</p>
Unnamed activity cluster in Vietnam	Bkav ⁵²⁰ VNCERT ⁵²¹	<p>In August 2016, Vietnamese cybersecurity company Bkav identified a long- running spyware campaign targeting Vietnamese entities since mid-2012, including government agencies, corporations, banks, research institutes, and universities, all linked to a C2 server (dcsvn[.]org) that imitates the Vietnamese military.⁵²² Bkav observed that the same malware used in the Vietnamese aviation sector operation matched the malware used in this activity cluster.</p> <p>VNCERT did not comment on the attribution of this activity or its connection to the Vietnamese aviation sector operation but warned that the malware could steal information or destroy systems.⁵²³</p>
Unnamed activity cluster in Laos	RiskIQ	<p>In November 2016, RiskIQ identified spear-phishing in Laos by a "known Chinese adversary ... most likely affiliated with the Chinese government." The campaign's C2 server (dubkill[.]com) had been in the actor's control since 2014 and used in activity targeting Vietnam, reported in June 2015 by Bkav.⁵²⁴</p> <p>RiskIQ found a loose connection between its Vietnam and Laos activity cluster and Bkav's 2012–2016 activity cluster, based on program database (PDB) strings, C2 domains, and historical DNS data overlaps and connections.⁵²⁵</p>

Unnamed activity cluster	Votiro Labs ⁵²⁶ ClearSky Fortinet	In August 2017, Votiro Labs and ClearSky attributed a possible espionage campaign targeting a large Vietnamese organization to the Vietnamese aviation sector activity group, possibly 1937CN. ⁵²⁷ Fortinet conducted further research into this activity cluster but did not attribute it or assess the validity of Votiro and ClearSky's attribution. ⁵²⁸
Goblin Panda	CrowdStrike Fortinet ⁵²⁹ Viettel ⁵³⁰ Anomali ⁵³¹	CrowdStrike tracks Goblin Panda as a PRC state-aligned threat actor focused on Southeast Asia, especially Vietnam, and principally targeting defense, energy, and government sectors. ^{532 533} CrowdStrike considers Goblin Panda to be interchangeable with APT27 . ⁵³⁴ Fortinet describes Goblin Panda as a threat actor focused on Southeast Asia, mainly targeting Cambodia, Indonesia, the Philippines, Myanmar, Malaysia, Thailand, and Vietnam, as well as India to a lesser extent. ⁵³⁵ Fortinet recognized Goblin Panda as being the same as Cycldek , Hellsing , APT27 , and <i>possibly 1937CN</i> . Vietnamese Ministry of Defense owned-and-operated cybersecurity firm Viettel ⁵³⁶ considers Goblin Panda to be the same as Hellsing , 1937CN , and unspecified other groups. It identifies Goblin Panda as a group targeting government, defense, and energy companies in South Asia and often in Vietnam. ⁵³⁷ Anomali considers Goblin Panda to be a PRC-aligned group principally targeting entities in Vietnam and elsewhere in Southeast Asia. Anomali assesses that its potential motivation is "espionage aligned with commercial and South China Sea issues." ⁵³⁸ Anomali treats Goblin Panda as synonymous with Conimes . Anomali assesses that Goblin Panda may receive tools, exploits, and infrastructure from the same shared source as Temp.Periscope (a.k.a. APT40, Leviathan) and Nomad/Dagger Panda (a.k.a. Temp. Trident, Icefog, RedFoxrot ⁵³⁹). The U.S. attributes APT40 to the Hainan State Security Department of the MSS ⁵⁴⁰ (a group focused on commercial espionage and research data theft, often in the South China Sea), and Recorded Future attributes RedFoxrot to PLA Strategic Support Force (SSF) Unit 69010 ^{av} (a group targeting commercial, research, and government organizations in Central Asia). ⁵⁴¹
Cycldek	Kaspersky Lab ⁵⁴²	Kaspersky Lab tracks Cycldek as a Chinese-speaking ⁵⁴³ threat group active since at least 2013, targeting large, high-profile organizations and government entities in Southeast Asia, especially Vietnam, Thailand, and Laos. ⁵⁴⁴ Kaspersky considers Cycldek to be interchangeable with Goblin Panda , Conimes , and APT27 . ⁵⁴⁵ Although some media outlets and threat encyclopedias identify Cycldek as interchangeable with the Southeast Asia-focused Hellsing espionage group, Kaspersky assessed that the Hellsing was a "stand-alone operation" that shared developer resources with Cycldek. ⁵⁴⁶
Conimes (a.k.a. Conimes Team, TEMP. Conimes)	iSight Partners ⁵⁴⁷ FireEye ⁵⁴⁸	iSight Partners and later FireEye, its first successor parent organization (now Mandiant), tracked a suspected PRC-aligned threat actor it called Conimes . ⁵⁴⁹ The actor targeted entities in Southeast Asia, mainly Vietnam, and especially so during periods of tension over the South China Sea. The name refers to the group's use of the "conimes.com" domain for C2. Kaspersky had associated this domain with the original Winnti threat actor. ⁵⁵⁰ TrendMicro observed that the same email address had been used to register the conimes[.]com C2 domain and scvhosts[.]com, ⁵⁵¹ both of which CrowdStrike had associated with Goblin Panda. ⁵⁵² Neither FireEye nor Mandiant have acknowledged in any reviewed public sources the analysis that tracks Goblin Panda as interchangeable with APT27.
Hive0045	IBM ⁵⁵³	IBM tracks Hive0045 , a suspected PRC-aligned state-sponsored threat group that primarily targets Southeast Asian countries in defense, energy, and government sectors with a primary interest in territorial conflicts. IBM assesses that the group "significantly overlaps" with Goblin Panda , Cycldek , and Hellsing .

^{av} **Unit 69010** (69010部队) is the military unit cover designator for a PLA cyber espionage, attack, and defense organization in Urumqi. This unit is presently affiliated with the Western Theater Command and the PLA SSF, following the past decade's military reorganizations. This command's area of responsibility encompasses Central Asia, the Indian subcontinent, and Afghanistan.

CHENGDU-BASED INDIVIDUALS

The **Chengdu-based individuals** activity cluster is a group of operators who conduct for-profit cybercrime and state-sponsored cyber activities. When treated as a whole, the cluster is often tracked as **APT41** or Winnti. However, public tracking of the cluster often divides it into two halves: the criminal enterprise behind the company named Sea Gamer (a.k.a. Wicked Spider, BlackFly, **Barium**) and the government contractors behind a company named Chengdu 404 (a.k.a. Wicked Panda, Grayfly, Lead).

The U.S. alleges that Chengdu 404 supported the MSS, and that this company's website stated that it also supported "public security, military, and military enterprises."⁵⁵⁴ Its criminal activities sometimes blended with its contracting, most prominently by targeting video game companies, stealing digital items of value for resale while concurrently collecting code-signing certificates later reused in espionage and surveillance operations.

Substantial deconfliction issues have persisted around this threat group. Very likely several PRC-aligned threat groups have access to common tooling, including the Winnti malware, which has led to nebulous clustering under the name "Winnti." This sourcing arrangement has been referred to as a "digital quartermaster" and the group-of-groups as the "Winnti Umbrella." Because deconfliction is largely outside the scope of this report, we note again that the following tables capture various government and industry attribution names "as is" for informational purposes.

Activity Groups or Clusters Associated with Chengdu-based Individuals		
ACTIVITY GROUP OR CLUSTER	CITED ALIGNMENT	DESCRIPTION
Chengdu-based individuals, operating behind commercial fronts	United States ⁵⁵⁵	In September 2020, the U.S. Department of Justice (DOJ) unsealed indictments charging five PRC nationals with intrusions at global commercial entities; governments in Vietnam, India, and Hong Kong; and nonprofit entities, as well as pro-democracy activists and politicians in Hong Kong. ⁵⁵⁶ The U.S. further alleged that the operators had engaged in various for-profit criminal activity like ransomware and crypto-jacking. The U.S. notes that one alleged co-conspirator has boasted of his relationship with the MSS and that Chengdu 404's website stated that its customers were "public security, military, and military enterprises." ⁵⁵⁷ This statement suggests that Chengdu 404 was a contractor for the Ministry of Public Security (MPS), PLA, and PRC defense companies. According to DOJ, the alleged activity had been tracked by the private sector as APT41 , Barium , Winnti , Wicked Panda , and Wicked Spider .
Chengdu 404 Network Technology (a.k.a. Chengdu 404) and Sea Gamer Mall SDN BHD (a.k.a. Sea Gamer)		

APT41	FireEye ⁵⁵⁸ SentinelOne ⁵⁵⁹ Group-IB ⁵⁶⁰ Venafi ⁵⁶¹	<p>FireEye assesses that APT41 is likely a PRC-aligned group that conducts for-hire state-sponsored espionage, intellectual property theft, and tracking and surveillance, while also conducting for-profit cybercrime, including ransomware operations.⁵⁶² While its for-profit activity has been consistent, it has not conducted intellectual property theft since 2015, shifting toward strategic intelligence collection.⁵⁶³ Also during the 2015-onwards era, the group has repeatedly surveilled Hong Kong pro-democracy groups.⁵⁶⁴ The firm assesses that APT41 "partially overlaps"⁵⁶⁵ with Barium and Winnti activity, as tracked by Kaspersky Lab,⁵⁶⁶ ESET,⁵⁶⁷ and ClearSky.⁵⁶⁸</p> <p>SentinelOne recognizes APT41 as a group of Chengdu-based individuals comprising two sub-groups, Lead and Barium, formerly collectively tracked as "Winnti." SentinelOne considers Barium to be two named PRC nationals and Lead to be Chengdu 404.⁵⁶⁹ SentinelOne assesses that these individuals and their close associates developed high-profile tools used by multiple China-affiliated threat groups, most importantly PlugX and ShadowPad. Suspected major clients using ShadowPad are APT41 and an amalgamation of Tonto Team and Tick, as well as other activity clusters Operation Redbonus (targeting India), Fishmonger (targeting universities, government, media, technology, and COVID-19 research organizations in Hong Kong, Taiwan, India, and the U.S.) and Operation Redkanku.⁵⁷⁰</p> <p>Group-IB assesses that APT41 is a PRC state-linked actor conducting both espionage and cybercrime. Group-IB considers APT41 interchangeable with Wicked Spider, Wicked Panda, and Barium.⁵⁷¹</p> <p>Venafi considers APT41 to be synonymous with the Chengdu-based individuals, Winnti, Wicked Panda, Wicked Spider, Barium, Blackfly, and Suckfly.⁵⁷²</p> <p>Note: FireEye previously, but no longer associates the "GREF" threat group it identified in 2014 with APT41,⁵⁷³ but rather now as a group with which APT41 shares tools and digital certificates.⁵⁷⁴ Some publications refer to APT41 as "Double Dragon," which is very likely a misunderstanding of a FireEye report's title.⁵⁷⁵</p>
Wicked Spider Wicked Panda	CrowdStrike	<p>CrowdStrike uses the Wicked Spider and Wicked Panda names, per the company's adversary nomenclature, to indicate the group's dual identity as a PRC state-linked actor and a cybercriminal actor.⁵⁷⁶</p> <p>Wicked Spider has extensively targeted global technology companies and repeatedly stolen code-signing certificates from video game companies, often used by Wicked Panda.</p> <p>CrowdStrike associated Wicked Panda with contractors who have PRC government clients, including MPS,⁵⁷⁷ likely serving as an "exploitation group for hire" (a.k.a. access-as-a-service).⁵⁷⁸ Wicked Panda's targeting has focused on "high-value" engineering, manufacturing, and technology sector entities, as well as chemical companies and think tanks globally. CrowdStrike considers Wicked Panda to be synonymous with Winnti, Group 72, Barium, Lead, GREF, APT41, TG-2633, Bronze Atlas.⁵⁷⁹</p>
Barium Lead	Microsoft ⁵⁸⁰	<p>Microsoft identifies many threat groups or activity clusters with the Winnti malware, but most strongly associates with it two distinct clusters tracked as Barium and Lead.⁵⁸¹</p> <p>Barium primary targets electronic gaming, multimedia, and internet content industries, as well as other technology companies. In 2017, Microsoft successfully sought a court order to seize domains used by Barium.⁵⁸²</p> <p>Lead focuses on industrial espionage with targeting of manufacturers in diverse industries, university-based research and development, and ICS security.</p>
Blackfly Gadfly	Symantec ⁵⁸³	<p>Symantec states that it tracks the broader APT41 activity as two distinct groups, Blackfly (financially motivated crime) and Gadfly (intellectual property theft), and associates them with the Chengdu-based cluster named by the U.S.⁵⁸⁴</p>

Winnti (a.k.a. Winnti Group)	Kaspersky Lab ⁵⁸⁵ ESET ⁵⁸⁶ ClearSky ⁵⁸⁷ TrendMicro ⁵⁸⁸	In 2013, Kaspersky Lab first used the name Winnti as a threat actor to describe activity involving the Winnti malware (coined by Symantec). The group had been active since at least 2009, primarily targeting video gaming companies globally with a focus on East and Southeast Asia. ⁵⁸⁹ Kaspersky observed that digital certificates stolen from these organizations were being used to sign malware targeting Uyghurs and Tibetan activists and in large-scale data-theft activities in South Korea. ESET also tracks Winnti , attributing in early 2019 a series of recent supply chain attacks, using backdoored video game products to infect victims almost exclusively in Southeast Asia, overwhelmingly in Thailand, the Philippines, Taiwan, Hong Kong, Indonesia, and Vietnam. ⁵⁹⁰
Winnti Umbrella	Protectwise ⁵⁹¹	Protectwise clusters numerous clusters of espionage and financial crime activity under a single overarching entity, thus tracked by the name " Winnti Umbrella ". ⁵⁹² Protectwise attributes this activity to China's intelligence apparatus. This umbrella encompasses Winnti, PassCV, APT17, Axiom, Lead, Barium, Wicked Panda, and GREF .
TG-2633 (a.k.a. Threat Group – 2633)	SecureWorks ⁵⁹³	SecureWorks tracks Kaspersky's Winnti Group as TG-2633 . SecureWorks also assessed that TG-2633 may be related to TG-3279 , another suspected PRC-aligned threat group, active since 2009, that breached video game companies to steal source code. ⁵⁹⁴
Red Kelpie	PwC	PwC associates Red Kelpie with the Chengdu 404 attribution, as well as APT41 and Barium . ⁵⁹⁵ PwC considers Red Kelpie to be the primary developer and user of ShadowPad malware and one of the primary Winnti malware users. ⁵⁹⁶ PwC assesses that Red Kelpie engages in financially motivated and espionage operations worldwide and in diverse sectors, including continued targeting of the video game industry from 2012 to at least 2019.
Bronze Atlas	SecureWorks ⁵⁹⁷	SecureWorks associates Bronze Atlas with activity since 2007 primarily focused on intellectual property theft from developed economies and possibly economic intelligence collection supporting the PRC government. The group has allegedly targeted pharmaceuticals, media, fossil fuel, and agricultural sectors. ⁵⁹⁸ The firm considers Bronze Atlas to be synonymous with APT41, Axiom, Barium, Blackfly, GREF, Group 72, Red Kelpie, TG-2633, Wicked Panda, and Winnti .
Group 72	Cisco ⁵⁹⁹	In 2014, Cisco assessed that Group 72 was a threat actor collecting high-value intellectual property from the manufacturing, industrial, aerospace, defense, and media sectors, with an almost exclusive focus on the U.S., Japan, Taiwan, and South Korea. Cisco considered Group 72 to be synonymous with Axiom . ⁶⁰⁰
Earth Baku	TrendMicro ⁶⁰¹	TrendMicro tracks Earth Baku as a threat group active in espionage and for-profit crime and considers it to be interchangeable with APT41 and the named Chengdu-based cluster . ⁶⁰²
Axiom	Novetta ⁶⁰³	In 2015, Novetta assessed that Axiom was an espionage group likely affiliated with China's intelligence community. Novetta assesses that Axom was a subgroup of a larger espionage group active since at least 2009. Axiom reportedly primarily targets entities of strategic economic interest to China and pro-democracy groups and individuals. Targets include "Fortune 500 companies, journalists, environmental groups, pro-democracy groups, software companies, academic institutions, and government agencies worldwide." ⁶⁰⁴ Novetta found possible associations between Axiom and numerous other groups but did not assess any one-to-one interchangeability.
PassCV	Blue Coat Systems Cylance	Blue Coat Systems, a firm later acquired by Symantec and then Broadcom, originated the name PassCV in 2014, referring to a malware strain using code-signing certificates from gaming companies, mainly in South Korea, and linked it to Winnti Group and Chinese-speaking individuals with activity going back to at least 2007. ⁶⁰⁵ In 2016, Cylance, now part of BlackBerry, assessed that PassCV was stealing code-signing certificates from gaming companies and had expanded its operations to target entities in the U.S., Russia, China, and Taiwan. ⁶⁰⁶

TONTO TEAM

Tonto Team is a PRC-aligned threat group that principally conducts espionage in South Korea, Russia, Mongolia, and Japan. This group is sometimes assessed to have been affiliated with PLA Unit 65016, formerly the Technical Reconnaissance Bureau (TRB) of the Shenyang Military Region headquartered in Shenyang and focused on Russia, the Koreas, and Japan.⁶⁰⁷ After PLA reforms, this unit likely fell under the control of the Shenyang-headquartered Northern Theater Command. According to the U.S. Department of Defense, this command is responsible for the Koreas, Russia, and Mongolia,⁶⁰⁸ which aligns with Tonto's targeting in these areas.

ACTIVITY GROUPS OR CLUSTERS ASSOCIATED WITH TONTO TEAM		
ACTIVITY GROUP OR CLUSTER	CITED ALIGNMENT	DESCRIPTION
Tonto Team	FireEye ⁶⁰⁹ Cisco ⁶¹⁰	<p>FireEye attributes Tonto Team to the PLA⁶¹¹ and suspects it may have been affiliated with the now reorganized Shenyang Military Region Technical Reconnaissance Bureau (Unit 65016).⁶¹² This group is associated with targeting of South Korea, Russia, and Japan.⁶¹³ The Shenyang Military Region has been subsumed by the Shenyang-headquartered Northern Theater Command due to the country's 2015 military reforms.</p> <p>Cisco also tracks Tonto Team, noting its use of the Bisonal malware for more than a decade and its consistent focus on Japanese, South Korean, and Russian organizations.⁶¹⁴ Cisco believes that Tonto Team created Bisonal and appears to track Bisonal activity as Tonto Team activity, assessing that it encompasses Operation Bitter Biscuit and HeartBeat APT,⁶¹⁵ and targeted activity in Russia and South Korea reported by Palo Alto Networks.⁶¹⁶</p>
Bronze Huntley	SecureWorks ⁶¹⁷	SecureWorks tracks Bronze Huntley as an espionage actor targeting economically and militarily important entities along China's periphery. The group has targeted political, media, research, military, government, mining, manufacturing, and engineering organizations in South Korea, Mongolia, Japan, India, and Russia. SecureWorks considers Bronze Huntley to be synonymous with Karma Panda and Tonto Team . ⁶¹⁸
Red Beifang	PwC	PwC tracks Red Beifang as one of five distinct China-based groups using ShadowPad malware and the malware's second primary user after Red Kelpie (a.k.a. APT41 , Barium). ⁶¹⁹ PwC considers Red Beifang to be synonymous with Tonto Team and Karma Panda . “Bēifāng” means “north” in Mandarin, possibly chosen as a reference to the Northern Theater Command of the PLA.
CactusPete	Kaspersky Lab ⁶²⁰	Kaspersky Lab tracks CactusPete as a threat group that has consistently targeted military, diplomacy, and infrastructure entities in Asia and Eastern Europe since at least 2013 ⁶²¹ and possibly as early as 2009. Kaspersky considers CactusPete to be synonymous with Tonto Team and Karma Panda . ⁶²²
Karma Panda	CrowdStrike	CrowdStrike tracks Karma Panda as a suspected China-linked adversary targeting dissident groups, ⁶²³ which the firm has tracked since at least 2014. ⁶²⁴ CrowdStrike considers Karma Panda to be synonymous with MysticChess , an alias of unknown origin. ^{625 626}
Operation Bitter Biscuit	AhnLab ⁶²⁷	AhnLab has tracked Bisonal malware activity since 2010 against South Korea, Japan, Russia, and India, especially the military and defense sector, as Operation Bitter Biscuit . ⁶²⁸ AhnLab associates this activity with HeartBeat APT and Bioazih RAT activity in India , ⁶²⁹ as well as other unspecified activity reported by FireEye, TrendMicro, and Coseinc.

TICK

Tick is a PRC-aligned threat group that primarily conducts espionage in Japan and against overseas Japanese entities. According to the Japanese government, Tick is associated with PLA Unit 61419, formerly the Fourth Operational Bureau (OB) of the PLA General Staff Department (GSD) in Qingdao, which focused on Korea and Japan.⁶³⁰ After 2015 reforms, Tick and this unit may have realigned to the Eastern Theater Command, which is responsible for Japan and Taiwan, consistent with Tick's observed Japan focus.⁶³¹

ACTIVITY GROUPS OR CLUSTERS ASSOCIATED WITH TICK		
ACTIVITY GROUP OR CLUSTER	CITED ALIGNMENT	DESCRIPTION
Tick	Symantec ⁶³² Cyfirma ⁶³³ LAC ⁶³⁴ TrendMicro ⁶³⁵ Japan ⁶³⁶	In 2016, Symantec identified Tick as an espionage group likely active since 2005, primarily targeting Japan, especially large firms involved in Japanese technology, engineering, and media firms. ⁶³⁷ Cyfirma considers Tick to be a PRC state-linked espionage group active since 2012 that primarily targets Japan and sometimes South Korea. Cyfirma assesses that the group's primary goal is to cause financial and reputational damage and that it engages in industrial espionage. The firm considers Tick to be interchangeable with Bronze Butler and Redbaldknight . ⁶³⁸ TrendMicro considers Tick to be an espionage group active since 2008 that is synonymous with Bronze Butler and Redbaldknight . ⁶³⁹ Redbaldknight appears to be TrendMicro's historical term for the same group. ⁶⁴⁰
PLA Unit 61419	Japan ⁶⁴¹	Japan assesses that Tick is associated with PLA Unit 61419 . At least until the 2015 military reforms, this unit was the Fourth Operational Bureau of the PLA General Staff Department in Qingdao. ⁶⁴² In 2021, Japan alleged that Tick had targeted about 200 companies and research institutions, successfully breaching the Japan Aerospace Exploration Agency (JAXA) in 2016. ⁶⁴³
Bronze Butler/ CTG-2006	SecureWorks ⁶⁴⁴	SecureWorks tracks Bronze Butler as an espionage actor, possibly operating on the behalf of China, that primarily targets entities in Japan in the manufacturing, engineering, and media industries. ⁶⁴⁵ SecureWorks considers Bronze Butler to be interchangeable with CTG-2006 , Stalker Panda , and Tick . SecureWorks's research team Counter Threat Unit (CTU) in its discussion interchangeably uses the alias CTG-2006 for Bronze Butler.
Nian	TeamT5 ⁶⁴⁶ Macnica Networks ⁶⁴⁷	TeamT5 and Macnica Networks tracks Nian as a PRC-aligned espionage group that focuses on Northeast Asian countries, especially Japan and South Korea, collecting military, government, and commercial intelligence, such as from electronics and chemical industries. TeamT5 and Macnica Networks consider Nian to be interchangeable with Redbaldknight , Bronze Butler , and Tick . In Chinese mythology, Nian is a creature often associated with New Year's celebrations.
Stalker Panda	CrowdStrike	CrowdStrike tracks Stalker Panda as a PRC-aligned adversary that has targeted petrochemical and industrial manufacturing entities in East Asia, ⁶⁴⁸ as well as entities in unspecified sectors in Japan. ⁶⁴⁹ CrowdStrike has not publicly acknowledged any other firms' aliases for Stalker Panda.

REDECHO

RedEcho is a PRC-aligned threat actor that targeted Indian critical infrastructure sectors in 2020. Information about this group is very limited, and no threat research group has publicly connected RedEcho to other tracked adversaries, as can be determined in reviewed public sources. It is plausible that RedEcho is linked to the Chengdu-based APT41 or the Western Theater Command of the PLA, which is responsible for executing the kinetic aspects of the stand-off with India and has a joint operations command center^{aw} in Chengdu.⁶⁵⁰ During the stand-off, Indian law enforcement noted that much offensive cyber activity against India, including targeting of its critical infrastructure, was originating in Chengdu.⁶⁵¹

^{aw} **Joint Operations Command Centers** have been credibly assessed to be one of two possible organizations likely responsible for the operational command of the PLA SSF's cyber units. (Source: https://ndupress.ndu.edu/Portals/68/Documents/stratperspective/china/china-perspectives_13.pdf)

ACTIVITY GROUPS OR CLUSTERS ASSOCIATED WITH REDECHO

ACTIVITY GROUP OR CLUSTER	CITED ALIGNMENT	DESCRIPTION
RedEcho	Recorded Future ⁶⁵²	In 2020, Recorded Future identified RedEcho as a PRC-aligned threat activity group. Recorded Future attributes a series of 2020 intrusions at Indian critical infrastructure sectors (oil and gas, electricity and power, marine, and rail) to this group. ⁶⁵³ Recorded Future could not firmly attribute this activity to an existing threat group, but noted that it had strong infrastructure and targeting overlaps with Tonto Team and APT41 , and one of its recurring tools (ShadowPad) is also used by at least five other distinct PRC-linked activity groups . ⁶⁵⁴ The name RedEcho reflects Recorded Future's nomenclature of beginning threat groups with colors associated with different countries and ending with a NATO phonetic alphabet code word.

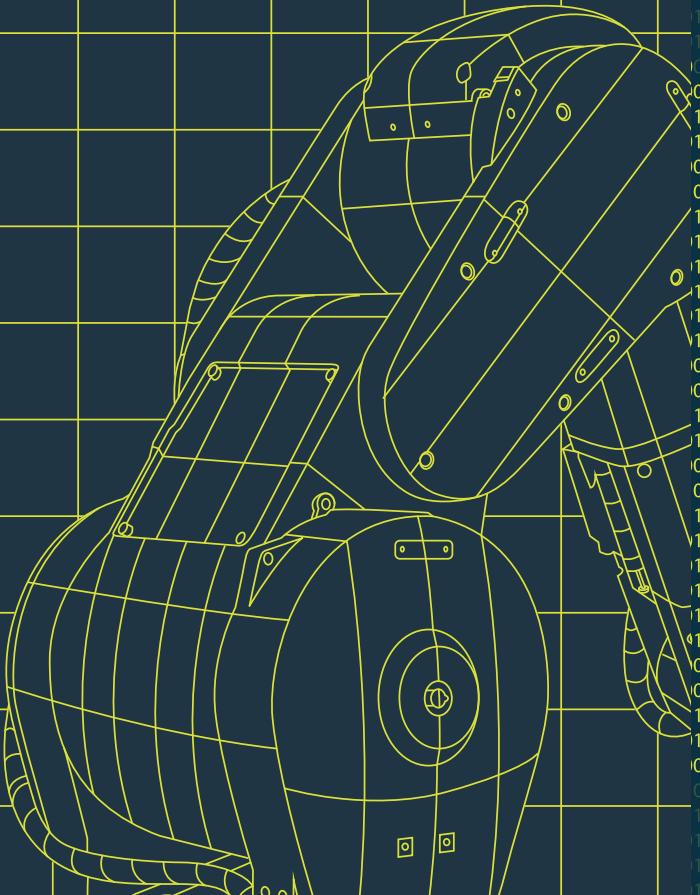
APT1

APT1 is a threat group that primarily conducted intellectual property theft in sectors related to the PRC's strategic development goals. The U.S. government publicly attributed APT1 to Unit 61398 of the PLA General Staff Department's (GSD) Third Department (3PLA), Second Bureau.⁶⁵⁵ Following the PLA reforms, the Third Department became the central component around which the Network System Department of the PLA SSF's cyber mission organized.⁶⁵⁶

ACTIVITY GROUPS OR CLUSTERS ASSOCIATED WITH APT1

ACTIVITY GROUP OR CLUSTER	CITED ALIGNMENT	DESCRIPTION
Unit 61368, PLA Third Department ^{ax}	U.S. ⁶⁵⁷	In 2014, the U.S. charged five officers with Unit 61398, PLA Third Department , for their roles in targeted intrusions between 2006 and 2014 at U.S. companies involved in nuclear power, metals, and solar products. ⁶⁵⁸ They conspired to steal intellectual property, trade secrets, and other beneficial non-public information to aid PRC state-owned enterprises.
APT1	Mandiant/FireEye	In 2013, Mandiant, later part of FireEye, attributed its APT1 threat group to Unit 61398, PLA Third Department, Second Bureau . ⁶⁵⁹ Mandiant assessed that the group principally conducted intellectual property theft from companies in strategically important industries for China and overwhelmingly in English-speaking countries. Mandiant assessed that APT1 was the same as Comment Crew and Comment Group . ⁶⁶⁰
Comment Crew	Symantec	Symantec considered its Comment Crew to be synonymous with APT1 . ⁶⁶¹
Comment Panda	CrowdStrike	CrowdStrike assessed that Comment Panda was the same as Unit 61398 . ⁶⁶² In 2014, CrowdStrike assessed that Comment Panda is organizationally related to Putter Panda , a group the firm attributed to Unit 61486, PLA Third Department, 12th Bureau . ⁶⁶³ The two shared infrastructure, and an identified member of Putter Panda was observed speaking online with a member of Unit 61398.
Shanghai Group	SecureWorks	SecureWorks tracked Comment Crew activity as the Shanghai Group , a reference to their assessed location. ⁶⁶⁴
Operation Oceansalt	McAfee	In 2018, McAfee reported activity targeting diverse entities primarily in South Korea, as well as the U.S. and Canada, which it dubbed Operation Oceansalt . ⁶⁶⁵ The activity used portions of code found in Comment Crew's Oceansalt malware, a non-public tool whose code McAfee believed had never been leaked. Analysis of the operation's attribution was inconclusive. McAfee has recognized APT1 and Comment Crew as interchangeable.

^{ax} Media and threat encyclopedias reference several other threat group names as industry aliases for Unit 61398. Reports by the originating companies using or explaining these names could not be found in reviewed sources.



ENDNOTES

- 1 “湘声：打好网上舆论斗争主动仗（“Xiangsheng: Fighting the online public opinion battle well”）,” People’s Government of Hunan Provence, June 9, 2020, accessed March 15, 2022, http://www.hunan.gov.cn/topic/fkxxgzbdfkxxbdpljd/202006/t20200609_12272872.html.
- 2 2021 Annual Threat Assessment of the U.S. Intelligence Community, Office of the Director of National Intelligence, April 9, 2021, accessed May 17, 2022, <https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf>. (p. 8)
- 3 Military and Security Developments Involving the People’s Republic of China 2021: Annual Report to Congress, Office of the Secretary of Defense, 2021, accessed March 28, 2022, <https://media.defense.gov/2021/Nov/03/2002885874/-1/1/0/2021-CMPR-FINAL.PDF>. (p. 88)
- 4 Chris Inglis, “Keynote Session: A Conversation With Chris Inglis,” The Geopolitics of Cybersecurity, April 20, 2022, accessed May 30, 2022, <https://www.cfr.org/event/geopolitics-cybersecurity>.
- 5 Edmund J. Burke., Kristen Gunness, Cortez A. Cooper III, and Mark Cozad, People’s Liberation Army Operational Concepts, RAND Corporation, 2020, https://www.rand.org/content/dam/rand/pubs/research_reports/RRA300/RRA394-1/RAND_RRA394-1.pdf. (p. 4)
- 6 “1994 China access to the Internet,” CCTV, September 7, 2009, accessed September 27, 2022, <http://www.cctv.com/english/special/60anni/20090907/110334.shtml>.
- 7 Desmond Ball, “China’s Cyber Warfare Capabilities,” Security Challenges, Vol. 7, No. 2 (Winter 2011) <https://www.jstor.org/stable/26461991>. (p. 81)
- 8 Qiao Liang and Wang Xiangsui, Unrestricted Warfare, PLA Literature and Arts Publishing House, February 1999, http://cdn.preterhuman.net/texts/underground/Information_Warfare/uw.pdf. (p. 118).
- 9 Ellen Messmer, “Kosovo cyber-war intensifies: Chinese hackers targeting U.S. sites, government says,” CNN, May 12, 1999, accessed September 27, 2022, <http://www.cnn.com/TECH/computing/9905/12/cyberwar.idg>.
- 10 “关于南昌、长沙、郑州宣传文化工作的考察报告 [Inspection report on propaganda and cultural work in Nanchang, Changsha and Zhengzhou],” 中共合肥市委宣传部 [Propaganda Department of the CCP, Heifei City], May 24, 2006, (Archived July 17, 2011), <https://web.archive.org/web/20110717061944/http://i46.tinypic.com/243qfti.jpg>.
- 11 Dawn S. Onley and Patience Wait, “Red Storm Rising,” GCN, August 17, 2006, [archived on January 19, 2022], <https://web.archive.org/web/20220119202126/https://gcn.com/cybersecurity/2006/08/red-storm-rising/285059/>
- 12 “Suspected Chinese hacker attacks target AIT, MND,” *Taipei Times*, June 19, 2006, accessed September 27, 2022, <https://www.taipei-times.com/News/taiwan/archives/2006/06/19/2003314414>.
- 13 Ankit Panda, “Xi Jinping: China Should Become a ‘Cyber Power,’” The Diplomat, March 4, 2014, accessed September 27, 2022, <https://thediplomat.com/2014/03/xi-jinping-china-should-become-a-cyber-power/>
- 14 Indo-Pacific Strategy of the United States, The White House, February 2022, accessed June 16, 2022, <https://www.whitehouse.gov/wp-content/uploads/2022/02/U.S.-Indo-Pacific-Strategy.pdf>. (p. 8)
- 15 “Xinhua Commentary-Explainer: How China has achieved long-term social stability,” Xinhua, June 28, 2021, accessed March 15, 2022, http://www.xinhuanet.com/english/special/2021-06/28/c_1310032526.htm.

- 16 Michael D. Swaine, "China's Assertive Behavior. Part One: On 'Core Interests,'" *China Leadership Monitor*, no. 34, 2011, accessed March 15, 2022, https://carnegieendowment.org/files/CLM34MS_FINAL.pdf.
- 17 Caitlin Campbell, Ethan Meick, Kimberly Hsu, and Craig Murray, "China's 'Core Interests' and the East China Sea," US-China Economic and Security Review Commission, 2013. <https://www.uscc.gov/sites/default/files/Research/China%27s%20Core%20Interests%20and%20the%20East%20China%20Sea.pdf>.
- 18 "中国为什么要宣示核心利益? ("Why does China declare its core interests?)," *People's Daily Online*, July 27, 2010, accessed March 15, 2022, <https://business.sohu.com/20100727/n273795955.shtml>.
- 19 "China never allows sovereignty, security and development interests to be harmed: Xi," Xinhua, October 23, 2020, accessed March 15, 2022, http://www.xinhuanet.com/english/2020-10/23/c_139461177.htm.
- 20 "China's military to safeguard sovereignty, security, development interests," CGTN, last modified May 22, 2020, accessed March 15, 2022, <https://news.cgtn.com/news/2020-05-22/China-vows-to-safeguard-sovereignty-security-development-interests-QH1ePpFZTi/index.html>.
- 21 "Xi stresses adherence to socialist rule of law with Chinese characteristics," Ministry of Justice of the People's Republic of China, last modified December 8, 2021, accessed March 15, 2022, http://en.moj.gov.cn/2021-12/08/c_688750.htm.
- 22 "China faces multiple, complicated security threats," *China Daily*, last modified April 16, 2013, accessed March 15, 2022, http://www.chinadaily.com.cn/china/2013-04/16/content_16410493.htm.
- 23 "China's Defensive National Defense Policy in the New Era," Ministry of National Defense of the People's Republic of China, n.d., accessed March 15, 2022, <http://eng.mod.gov.cn/defense-policy/index.htm>.
- 24 Cui Jia, "Social stability remains 'key task,'" *China Daily*, last modified Nov. 1, 2017, accessed March 15, 2022 (republished by The State Council of the People Republic of China), http://english.www.gov.cn/state_council/state_councilors/2017/11/01/content_281475928076588.htm.
- 25 "Xinhua Commentary-Explainer: How China has achieved long-term social stability," Xinhua, June 28, 2021, accessed March 15, 2022, http://www.xinhuanet.com/english/special/2021-06/28/c_1310032526.htm.
- 26 "MEPs call for respecting China's territorial integrity (07/16/09)," Xinhua, July 17, 2009, accessed March 15, 2022, Embassy of the People's Republic of China in the United States of America, <https://www.mfa.gov.cn/ce/ceus//eng/zt/Xinjiang/t573634.htm>.
- 27 "Wang Yi: Underline Three Bottom Lines of China's Relations with the United States," Embassy of the People's Republic of China in the Republic of Liberia, n.d., accessed March 15, 2022, <https://www.mfa.gov.cn/ce/celr/eng/zgyw/t1895276.htm>.
- 28 "Foreign Ministry Spokesperson Geng Shuang's Regular Press Conference on June 19, 2018," Consulate General of the People's Republic of China in Mumbai, June 19, 2018, accessed March 15, 2022, <https://www.mfa.gov.cn/ce/cgmb/eng/fyrt/t1569968.htm>, <https://www.mfa.gov.cn/ce/cegr/eng/ztlm/lxjzzdh/t317420.htm>.
- 29 "Foreign Ministry Spokesperson Jiang Yu's Regular Press Conference on 8 May 2007," Embassy of the People's Republic of China in the Hellenic Republic, May 9, 2007, accessed March 15, 2022, <https://www.mfa.gov.cn/ce/cegr/eng/ztlm/lxjzzdh/t317420.htm>.
- 30 "Yang Jiechi States China's Solemn Position on Issues Related to Xinjiang and Hong Kong," Embassy of the People's Republic of China in the United States of America, June 12, 2021, accessed March 15, 2022, <https://www.fmprc.gov.cn/ce/ceus/eng/zmgxss/t1883498.htm>.
- 31 "PLA vows to defend sovereignty and territorial integrity ahead of 90th anniversary," The State Council Information Office of the People's Republic of China, July 24, 2017, accessed March 15, 2022, http://english.scio.gov.cn/2017-07/24/content_41273285.htm.
- 32 "Foreign Ministry Spokesperson Hua Chunying's Remarks on the Indian Government's Announcement of the Establishment of the Ladakh Union Territory Which Involves Chinese Territory," Embassy of the People's Republic of China in the United States of America, August 6, 2019, accessed March 15, 2022, <https://www.mfa.gov.cn/ce/ceus//eng/fyrt/t1686549.htm>.
- 33 "China's Sovereignty over the South China Sea Islands - Brooks No Denial," Office of the Commissioner of the Ministry of Foreign Affairs of the People's Republic of China in the Macao Special Administration Region, n.d., accessed March 15, 2022, <https://www.mfa.gov.cn/ce/como//eng/gsxwfb/t1328193.htm>.
- 34 "White Paper-The One-China Principle and the Taiwan Issue," The Office of the Chargé d'Affaires of the People's Republic of China in the Republic of Lithuania, n.d., accessed March 15, 2022, <https://www.mfa.gov.cn/ce/ceft//eng/zt/zgtw/t125229.htm>.
- 35 "China Takes Tough Line on Sovereignty Amid Territorial Spats With Neighbors," NBC News, last modified August 1, 2017, accessed March 15, 2022, <https://www.nbcnews.com/news/world/china-takes-tough-line-sovereignty-amid-territorial-spats-neigh>
- 36 "Wang Yi: Underline Three Bottom Lines of China's Relations with the United States," Embassy of the People's Republic of China in the Republic of Liberia, n.d., accessed March 15, 2022, <https://www.mfa.gov.cn/ce/celr/eng/zgyw/t1895276.htm>.
- 37 孙飞 ("Sun Fei"), "中国领导人频提“发展利益”背后的战略转变 ("The strategic shift behind Chinese leaders' frequent mention of 'development interests')," 联合早报 ("Lianhe Zaobao"), October 29, 2020, accessed March 15, 2022, <https://www.haozaobao.com/mon/keji/20201029/80076.html>.
- 38 Song Zhongping, "New national defense law to protect China's development interests," *Global Times*, December 28, 2020, accessed March 15, 2022, <https://www.globaltimes.cn/page/202012/1211278.shtml>.
- 39 "【海外利益安全】国家发展利益的延伸 ([Security of Overseas Interests] Extension of National Development Interests)," 兰州网信办 ("Lanzhou State Internet Information Office"), April 15, 2021, accessed March 15, 2021, http://www.lzwxb.gov.cn/hdmbi/bas/col_detail.php?id=1517.
- 40 "Military and Security Developments Involving the People's Republic of China 2020," Office of the Secretary of Defense, accessed March 16, 2020, <https://media.defense.gov/2020/Sep/01/2002488689/-1/-1/1/2020-DOD-CHINA-MILITARY-POWER-REPORT-FINAL.PDF> (p. 130).
- 41 "Xi stresses CPC's absolute leadership over army," *China Daily*, last modified November 2, 2014, accessed March 17, 2022, https://www.chinadaily.com.cn/china/2014-11/02/content_18843109.htm.
- 42 Lily Kuo, "Xi Jinping calls for 'absolute loyalty' from Chinese army," *The Guardian*, August 20, 2018, accessed March 17, 2022, <https://www.theguardian.com/world/2018/aug/20/xi-jinping-calls-for-absolute-loyalty-from-chinese-army>.
- 43 Wang Baocun and Li Fei, "INFORMATION WARFARE," *Liberation Army Daily*, June 13 and June 20, 1995, (translated by Institute for National Strategic Studies, 1996), https://irp.fas.org/world/china/docs/iw_wang.htm.
- 44 Adam Ni and Bates Gill, "The People's Liberation Army Strategic Support Force: Update 2019," *China Brief*. Volume: 19 Issue: 10. Jamestown Foundation, May 29, 2019, accessed March 17, 2022, <https://jamestown.org/program/the-peoples-liberation-army-strategic-support-force-update-2019/>.

- 45 “尹卓:战略支援部队负责太空网络电磁空间 贯穿整个作战 [“Yin Zhuo: The Strategic Support Force is responsible for the space, network, and electromagnetic space throughout the entire conflict”],” 大报版 [Guancha], January 5, 2016, (archived by Internet Archive on January 6, 2016), https://web.archive.org/web/20160106112825/http://www.guancha.cn/military-affairs/2016_01_05_346981.shtml.
- 46 Rachael Burton and Mark Stokes, The People’s Liberation Army Strategic Support Force Leadership and Structure, Project 2049 Institute, September 25, 2018, https://project2049.net/wp-content/uploads/2018/09/180925_PLA_SSF_Leadership-and-Structure_Stokes_Burton.pdf.
- 47 Adam Ni and Bates Gill, “The People’s Liberation Army Strategic Support Force: Update 2019,” China Brief. Volume: 19 Issue: 10. Jamestown Foundation, May 29, 2019, accessed March 17, 2022, <https://jamestown.org/program/the-peoples-liberation-army-strategic-support-force-update-2019/>.
- 48 Elsa B. Kania, “China’s Strategic Support Force At 3,” *The Diplomat*, December 29, 2018, accessed April 7, 2022, <https://thediplomat.com/2018/12/chinas-strategic-support-force-at-3/>.
- 49 Bryan Krekel, George Bakos, and Christopher Barnett, Capability of the People’s Republic of China to Conduct Cyber Warfare and Computer Network Exploitation, U.S. China Economic and Security Review Commission, <https://apps.dtic.mil/sti/pdfs/ADA509000.pdf> (p. 30-36).
- 50 Adam Kozy, “OPENING STATEMENT OF ADAM KOZY, INDEPENDENT ANALYST, CEO & FOUNDER, SINACYBER,” U.S.-China Economic and Security Review Commission, February 17, 2022, https://www.uscc.gov/sites/default/files/2022-02/February_17_2022_Hearing_Transcript.pdf. (p. 85)
- 51 Allan Paller, “Cyber Security: Developing a National Strategy,” U.S. Senate Committee on Homeland Security and Government Affairs, April 28, 2009, accessed March 17, 2022, <https://www.hsgac.senate.gov/imo/media/doc/042809Paller.pdf>. (p. 3)
- 52 Clive Akass, “Wicked Rose and China’s information war,” Personal Computer World, September 23, 2008, (archived by Internet Archive on September 30, 2011), <https://web.archive.org/web/20110930081404/http://labs.pcw.co.uk/2008/09/wicked-rose-and.html>.
- 53 Allan Paller, “Cyber Security: Developing a National Strategy,” U.S. Senate Committee on Homeland Security and Government Affairs, April 28, 2009, accessed March 17, 2022, <https://www.hsgac.senate.gov/imo/media/doc/042809Paller.pdf>. (p. 3)
- 54 “史上首次! 国家安全部官宣招募渠道, 揭秘国家安全部是怎么样一个部门。(“For the first time in history! The Ministry of National Security officially announced recruitment channels, revealing what kind of organization the Ministry of National Security is.”),” 法制日报 (“Legal Daily”), January 7, 2021, accessed March 17, 2021, (republished by Xishui People’s Government), http://www.xsx.gov.cn/xwzx/tt/202101/t20210107_66075553.html.
- 55 Bill Gertz, “Chinese spy who defected tells all,” *The Washington Times*, March 19, 2009, (archived by Internet Archive on January 13, 2010), <https://web.archive.org/web/20100113061119/http://www.washingtontimes.com/news/2009/mar/19/exclusive-chinese-spy-who-defected-tells-all/>.
- 56 Bill Gerz, “Chinese spy who defected tells all,” *The Washington Times*, March 19, 2009, (archived by Internet Archive on March 22, 2009), <https://web.archive.org/web/20100113061119/http://www.washingtontimes.com/news/2009/mar/19/exclusive-chinese-spy-who-defected-tells-all/?page=2>.
- 57 Paul Mozur and Chris Buckley, “Spies for Hire: China’s New Breed of Hackers Blends Espionage and Entrepreneurship,” *The New York Times*, August 26, 2021, accessed March 17, 2022, <https://www.nytimes.com/2021/08/26/technology/china-hackers.html>.
- 58 UNITED STATES OF AMERICA CRIMINAL v. JIANG LIZHI, QIAN CHUAN, and FU QIANG, United States District Court for The District of Columbia, August 11, 2020, accessed March 17, 2022, <https://www.justice.gov/opa/press-release/file/1317206/download>. (p. 3, 6)
- 59 “Winnti. More than just a game,” Securelist by Kaspersky, April 11, 2013, accessed March 17, 2022, <https://securelist.com/winnti-more-than-just-a-game/37029>.
- 60 “CHINA’S CENSORSHIP OF THE INTERNET AND SOCIAL MEDIA: THE HUMAN TOLL AND TRADE IMPACT,” Congressional-Executive Commission on China, November 17, 2011, accessed March 17, 2022, <https://www.govinfo.gov/content/pkg/CHRG-112hhrg72895/html/CHRG-112hhrg72895.htm>.
- 61 “Agencies Responsible for Censorship in China,” Congressional-Executive Commission on China, n.d., accessed March 17, 2022, <https://www.cecc.gov/agencies-responsible-for-censorship-in-china>.
- 62 Bryan Krekel, George Bakos, and Christopher Barnett, “Capability of the People’s Republic of China to Conduct Cyber Warfare and Computer Network Exploitation,” U.S. China Economic and Security Review Commission, <https://apps.dtic.mil/sti/pdfs/ADA509000.pdf>.
- 63 Nathan Attrill and Audrey Fritz, “China’s cyber vision How the Cyberspace Administration of China is building a new consensus on global internet governance,” Australian Strategic Policy Institute, November 2021, accessed March 17, 2022, <https://ad-aspi.s3.ap-southeast-2.amazonaws.com/2021-11/Chinas%20cyber%20vision.pdf?VersionId=M0ePH4lj3w7WRJrLlhvxVvt269MWSYOs>.
- 64 Jane Li, “How China’s top internet regulator became Chinese tech giants’ worst enemy,” Quartz, last modified January 7, 2022, accessed March 17, 2022, <https://qz.com/2039292/how-did-chinas-top-internet-regulator-become-so-powerful/>.
- 65 Zeyi Yang, “VPNs are out, more security reviews are in: What’s in China’s new cyber rules,” Protocol, November 18, 2021, accessed March 17, 2022, <https://www.protocol.com/china/vpns-out-new-cyber-regulation>.
- 66 Renée Diressta, Carly Miller, Vanessa Molter, John Pomfret, And Glenn Tiffert, “Telling China’s Story: The Chinese Communist Party’s Campaign to Shape Global Narratives,” Stanford Internet Observatory and the Hoover Institution, 2020, https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/sio-china_story_white_paper-final.pdf.
- 67 Chung Li-hua and Jake Chung, “China using local ‘agents’ to spread misinformation online: institute,” *Taipei Times*, August 4, 2019, accessed March 17, 2022, <http://www.taipeitimes.com/News/front/archives/2019/08/04/2003719873>.
- 68 “专设统战工作领导小组 中央“大统战”思维升级 (“Leading Group Dedicated to Improved United Front Work Core ‘Great United Front’ Thought”),” *The People’s Daily*, July 31, 2015, accessed March 17, 2022, <http://cpc.people.com.cn/xuexi/n/2015/0731/c385474-27391395.html>.
- 69 “习近平: 巩固发展最广泛的爱国统一战线 (“Xi Jinping: Consolidate and Develop the Broadest Possible Patriotic United Front”),” Xinhua, May 20, 2015, accessed March 17, 2022, http://www.xinhuanet.com/politics/2015-05/20/c_1115351358.htm.
- 70 Jeff Kao and Mia Shuang Li, “How China Built a Twitter Propaganda Machine Then Let It Loose on Coronavirus,” ProPublica, March 26, 2020, accessed March 17, 2022, <https://www.propublica.org/article/how-china-built-a-twitter-propaganda-machine-then-let-it-loose-on-coronavirus>.
- 71 “2017 Report to Congress,” U.S.-China Economic and Security Review Commission, November 2017, https://www.uscc.gov/sites/default/files/2019-10/Chapter%203,%20Section%2020-%20China's%20Domestic%20Information%20Controls,%20Global%20Media%20Influence,%20and%20Cyber%20Diplomacy_0_0.pdf. (Chapter 3, Section 5)

- 72 Doug Livermore, "China's 'Three Warfares' In Theory and Practice in the South China Sea," Georgetown Security Studies Review, March 25, 2018, accessed March 17, 2022, <https://georgetownsecurity-studiesreview.org/2018/03/25/chinas-three-warfares-in-theory-and-practice-in-the-south-china-sea>.
- 73 "Military and Security Developments Involving the People's Republic of China 2020," Office of the Secretary of Defense, accessed March 16, 2020, <https://media.defense.gov/2020/Sep/01/2002488689/1-1/2020-DOD-CHINA-MILITARY-POWER-REPORT-FINAL.PDF>. (p. 130)
- 74 "Science of Military Strategy," China's Academy of Military Sciences, 2013, (translated by the China Aerospace Studies Institute), https://www.airuniversity.af.edu/Portals/10/CASI/documents/Translations/2021-02-08%20Chinese%20Military%20Thoughts-%20In%20their%20own%20words%20Science%20of%20Military%20Strategy%202013.pdf?ver=NxAwg4BPw_NylEjxaha8Aw%3d%3d. (p.163)
- 75 Nathan Beauchamp-Mustafaga, "Cognitive Domain Operations: The PLA's New Holistic Concept for Influence Operations," China Brief Volume: 19 Issue: 16, September 6, 2019, Jamestown Foundation, accessed March 17, 2022, <https://jamestown.org/program/cognitive-domain-operations-the-plas-new-holistic-concept-for-influence-operations/>.
- 76 Nathan Beauchamp-Mustafaga, Derek Grossman, Kristen Gunness, Michael S. Chase, Marigold Black, and Natalia D. Simmons-Thomas, Deciphering Chinese Deterrence Signalling in the New Era: An Analytic Framework and Seven Case Studies. Santa Monica, CA: RAND Corporation, 2021. https://www.rand.org/pubs/research_reports/RRA1074-1.html. (p. 32–33)
- 77 Dean Chang, "An Overview of Chinese Thinking About Deterrence," NL ARMS Netherlands Annual Review of Military Studies 2020, NL ARMS. T.M.C. Asser Press, The Hague. https://doi.org/10.1007/978-94-6265-419-8_10.
- 78 Nathan Beauchamp-Mustafaga, Derek Grossman, Kristen Gunness, Michael S. Chase, Marigold Black, and Natalia D. Simmons-Thomas, Deciphering Chinese Deterrence Signalling in the New Era: An Analytic Framework and Seven Case Studies. Santa Monica, CA: RAND Corporation, 2021. https://www.rand.org/pubs/research_reports/RRA1074-1.html.
- 79 "Science of Military Strategy," China's Academy of Military Sciences, 2013, (translated by the China Aerospace Studies Institute), https://www.airuniversity.af.edu/Portals/10/CASI/documents/Translations/2021-02-08%20Chinese%20Military%20Thoughts-%20In%20their%20own%20words%20Science%20of%20Military%20Strategy%202013.pdf?ver=NxAwg4BPw_NylEjxaha8Aw%3d%3d (p.156).
- 80 "VOA Condemns Jamming in China," Voice of America, February 26, 2013, accessed March 17, 2022, <https://www.insidevoa.com/a/voa-condemns-jamming-in-china/1611410.html>.
- 81 "2017 Report to Congress," U.S.-China Economic and Security Review Commission, November 2017, https://www.uscc.gov/sites/default/files/2019-10/Chapter%203,%20Section%205%20-%20China's%20Domestic%20Information%20Controls,%20Global%20Media%20Influence,%20and%20Cyber%20Diplomacy_0_0.pdf (Chapter 3, Section 5, Page 482).
- 82 "The Internet in China," *People's Daily*, June 8, 2010, accessed March 18, 2022, <http://en.people.cn/90001/90776/90785/7017177.html>.
- 83 Charles Clover and Murad Ahmed, "Xi Jinping defends China's right to 'sovereign' internet," Financial Times, December 16, 2015, accessed March 18, 2022, <https://www.ft.com/content/858b4988-a3bf-11e5-873f-68411a84f346>.
- 84 "China web users call for 'Jasmine Revolution,'" The Sydney Morning Herald, last modified February 20, 2011, accessed March 18, 2022, <https://www.smh.com.au/technology/china-web-users-call-for-jasmine-revolution-20110220-1b0so.html>.
- 85 "China web users call for 'Jasmine Revolution,'" The Sydney Morning Herald, last modified February 20, 2011, accessed March 18, 2022, <https://www.smh.com.au/technology/china-web-users-call-for-jasmine-revolution-20110220-1b0so.html>.
- 86 Austin Ramzy, "State Stamps Out Small 'Jasmine' Protests in China," Time, February 21, 2011, accessed March 18, 2022, <http://content.time.com/time/world/article/0,8599,2052860,00.html>.
- 87 "Chinese president urges improved social management for greater harmony, stability," Embassy of the People's Republic of China in the United States of America, February 19, 2011, accessed March 18, 2022, <https://www.mfa.gov.cn/ce/ceus//eng/gdxw/t801742.htm>.
- 88 Michael Wines, "China Creates New Agency for Patrolling the Internet," *The New York Times*, May 4, 2011, accessed March 18, 2022, <https://www.nytimes.com/2011/05/05/world/asia/05china.html>.
- 89 Nathan Attrill and Audrey Fritz, "China's cyber vision How the Cyberspace Administration of China is building a new consensus on global internet governance," Australian Strategic Policy Institute, November 2021, accessed March 17, 2022, <https://ad-aspi.s3.ap-southeast-2.amazonaws.com/2021-11/Chinas%20cyber%20vision.pdf?VersionId=M0ePH4lj3w7WRjrLlhxyVvt269MWSYOs> (p. 4).
- 90 Michael Wines, "China Creates New Agency for Patrolling the Internet," *The New York Times*, May 4, 2011, accessed March 18, 2022, <https://www.nytimes.com/2011/05/05/world/asia/05china.html>.
- 91 Edward Wong, "China: 54 Detained in Crackdown," *The New York Times*, April 11, 2011, accessed March 18, 2022, <https://www.nytimes.com/2011/04/16/world/asia/16briefs-ART-china.html>.
- 92 Keith B. Richburg, "Chinese artist Ai Weiwei arrested in ongoing government crackdown," *The Washington Post*, April 3, 2011, accessed March 18, 2022, https://www.washingtonpost.com/world/chinese-artist-ai-wei-wei-arrested-in-latest-government-crack-down/2011/04/03/AFHB5PVC_story.html.
- 93 Damain Grammaticas, "Details emerge of Chinese artist Ai Weiwei's detention," BBC, August 11, 2011, accessed March 18, 2022, <https://www.bbc.com/news/world-asia-pacific-14487328>.
- 94 "Chinese artist Ai Weiwei held for 'economic crimes'," BBC, April 7, 2011, accessed March 18, 2022, <https://www.bbc.com/news/world-asia-pacific-12994785>.
- 95 I love Weiwei, "又一网站Twitition.com因为“释放艾未未”签名遭到DDoS攻击 ("Another website, Twitition.com, experienced a DDoS attack due to its 'Release Ai Weiwei' petition"), " Blogspot, April 23, 2011, accessed March 18, 2011, <http://loveaiww.blogspot.com/2011/04/twititioncomddos.html#more>.
- 96 "Call for the Release of Ai Weiwei," Change.org, last modified June 22, 2011, accessed March 18, 2011, https://www.change.org/p/call-for-the-release-of-ai-weiwei?share_id=sLnYJwFWme&share_source=share-petition_tw.
- 97 Abby d'Arcy Hughes, "Ai Weiwei arrest protests at Chinese embassies worldwide," *The Guardian*, April 17, 2011, accessed March 18, 2011, <https://www.theguardian.com/artanddesign/2011/apr/17/ai-weiwei-protests-1001-chairs>.
- 98 Tania Branigan, "Ai Weiwei campaign website 'victim of Chinese hackers'," *The Guardian*, April 20, 2011, accessed March 18, 2022, <https://www.theguardian.com/artanddesign/2011/apr/20/ai-weiwei-campaign-website-chinese-hackers>.

- 99 "The arrest of a Chinese artist affects our digital agency in Leeds," B3Labs, April 21, 2011, (archived by Internet Archive on July 2, 2011), <https://web.archive.org/web/20110702122859/http://www.branded3.com/b3labs/how-jailing-a-prominent-chinese-artist-affected-our-leeds-based-agency>.
- 100 Twitter search results for "Twitition" and "down" between April 1 and April 25, 2011, Twitter, accessed March 18, 2022, https://twitter.com/search?q=Twitition%20down%20since%3A2011-04-01%20until%3A2011-04-25&src=typed_query&f=live.
- 101 Patrick Altoft (@patrickaltoft), "@rackspace tells us that our twitition.com site...", Twitter, April 7, 2011 4:38 am, <https://twitter.com/patrickaltoft/status/55912307062083584>.
- 102 Luisetta Mudie, "Petition Site Hit by Hackers," Radio Free Asia, April 20, 2011, accessed March 18, 2022, <https://www.rfa.org/english/news/china/petition-04202011152208.html>.
- 103 Fahmida Y. Rashid, "FBI to Investigate China-Based DDoS Attacks Against Change.org," EWeek, April 29, 2011, accessed March 18, 2022, <https://www.eweek.com/cloud/fbi-to-investigate-china-based-ddos-attacks-against-change.org>.
- 104 Tania Branigan, "Ai Weiwei campaign website 'victim of Chinese hackers,'" The Guardian, April 20, 2011, accessed March 18, 2022, <https://www.theguardian.com/artanddesign/2011/apr/20/ai-wei-wei-campaign-website-chinese-hackers>.
- 105 Fahmida Y. Rashid, "FBI to Investigate China-Based DDoS Attacks Against Change.org," EWeek, April 29, 2011, accessed March 18, 2022, <https://www.eweek.com/cloud/fbi-to-investigate-china-based-ddos-attacks-against-change.org>.
- 106 Joseph E. Macmanus to Rosa DeLauro, May 18, 2011, <https://change.app.box.com/s/f030mfnr2lfvsttbyz/file/779019852>.
- 107 Lorand Laskai, "When China's White-Hat Hackers Go Patriotic," Council on Foreign Relations, March 13, 2017, accessed March 18, 2022, <https://www.cfr.org/blog/when-chinas-white-hat-hackers-go-patriotic>.
- 108 Paul McNamara, "Chinese hackers plotting DDoS against CNN?," Network World, April 18, 2008, accessed March 18, 2022, <https://www.networkworld.com/article/2343859/chinese-hackers-plotting-ddos-against-cnn-.html>.
- 109 Mo Nong, "Ideological bias clouds Western views," China Daily, April 14, 2011, accessed March 18, 2022, https://www.chinadaily.com.cn/opinion/2011-04/14/content_12323209.htm.
- 110 Michael Kan, "Change.org victim of DDoS attack from China," CSO, April 19, 2011, accessed March 18, 2022, <https://www.csoonline.com/article/2128124/change-org-victim-of-ddos-attack-from-china.html>.
- 111 "The arrest of a Chinese artist affects our digital agency in Leeds," B3Labs, April 21, 2011, (archived by Internet Archive on July 2, 2011), <https://web.archive.org/web/20110702122859/http://www.branded3.com/b3labs/how-jailing-a-prominent-chinese-artist-affected-our-leeds-based-agency>.
- 112 Jaime A. FlorCruz and Lucrezia Seu, "From snail mail to 4G, China celebrates 20 years of Internet connectivity," CNN, April 23, 2014, accessed March 18, 2022, <https://www.cnn.com/2014/04/23/world/asia/china-internet-20th-anniversary/index.html>.
- 113 Greg Walton, "China's Golden Shield," Rights and Democracy, 2011, accessed August 30, 2019, (archived by Internet Archive on August 27, 2011), https://web.archive.org/web/20110827000522/http://www.ichrdd.ca/site/_PDF/publications/globalization/CGS_ENG.PDF.
- 114 自曲主编 ("Editor in Chief"), "阅后即焚: 'GFW' ('Burn after reading: 'GFW'') Free More News, August 30, 2009, (archived by Internet Archive on January 4, 2010), <https://web.archive.org/web/20100104124506/http://freemorenews.com/2009/08/30/burn-after-reading-gfw>.
- 115 Daniel Anderson, "Splinternet Behind the Great Firewall of China," ACM Queue, November 30, 2012, accessed March 22, 2022, [hxxp://queue.acm.org/detail.cfm?id=2405036](https://queue.acm.org/detail.cfm?id=2405036).
- 116 pingp, "The Great Firewall of China: Background," Torfox, Stanford, June 1, 2011, accessed March 22, 2022, [hxxps://cs.stanford.edu/people/eroberts/cs181/projects/2010-11/FreedomOfInformationChina/author/pingp/index.html](https://cs.stanford.edu/people/eroberts/cs181/projects/2010-11/FreedomOfInformationChina/author/pingp/index.html).
- 117 "The Great Firewall of China," Bloomberg, November 5, 2018, accessed March 22, 2022, [hxxps://www.bloomberg.com/quicktake/great-firewall-of-china](https://www.bloomberg.com/quicktake/great-firewall-of-china).
- 118 Bill Marczak et al., "China's Great Cannon," The Citizen Lab, April 10, 2015, accessed March 22, 2022, [hxxps://citizenlab.ca/2015/04/chinas-great-cannon](https://citizenlab.ca/2015/04/chinas-great-cannon).
- 119 Charlie, "Collateral Freedom and the not-so-Great Firewall," Greatfire.org, March 12, 2015, accessed March 18, 2022, <https://en.greatfire.org/blog/2015/mar/collateral-freedom-and-not-so-great-firewall>.
- 120 Jeff South, "Punching a Hole in the Great Firewall," ChinaFile, March 21, 2014, accessed March 18, 2022, <https://www.chinafile.com/Punching-Hole-Great-Firewall>.
- 121 Jeff South, "Punching a Hole in the Great Firewall," ChinaFile, March 21, 2014, accessed March 18, 2022, <https://www.chinafile.com/Punching-Hole-Great-Firewall>.
- 122 Michael Kan, "GitHub unblocked in China after former Google head slams its censorship," IT World, January 23, 2013, (archived by Internet Archive on March 8, 2013), <https://web.archive.org/web/20130308120547/http://www.itworld.com/software/337835/github-unblocked-china-after-former-google-head-slams-its-censorship>.
- 123 "Outlook在中国遭中间人攻击 ("Outlook hit by man-in-the-middle attack from China")," GreatFire.org, January 19, 2015, March 18, 2022, <https://web.archive.org/web/20150412080258/https://zh.greatfire.org/blog/2015/jan/outlook-grim-chinese-authorities-attack-microsoft>.
- 124 "国家网信办发言人: "Outlook受中国攻击"的说法纯属污蔑 ("Cyberspace Administration of China spokesman: 'Outlook under attack by China' is pure slander")," Cyberspace Administration of China, January 22, 2015, (archived by Internet Archive on January 23, 2015), http://www.cac.gov.cn/2015-01/22/c_1114097853.htm.
- 125 Berthold Stevens, "DW defies tighter Internet censorship in China," DW, January 29, 2015, accessed March 18, 2022, <https://www.dw.com/en/dw-defies-tighter-internet-censorship-in-china/a-18222615>.
- 126 David Dawson, "Chinese Authorities Snuff out Last Online Remnants of the New York Times," The Diplomat, February 11, 2015, accessed March 18, 2022, <https://thediplomat.com/2015/02/chinese-authorities-snuff-out-last-online-remnants-of-the-new-york-times>.
- 127 "China's 'Great Cannon' programme has been in development for about a year, sources say," South China Morning Post, last modified April 15, 2015, (archived by Internet Archive on April 25, 2015), <https://web.archive.org/web/20150425175122/http://www.scmp.com/news/china/article/1764378/chinas-great-cannon-programme-has-been-development-about-year-sources-say>.
- 128 Robert Graham, "Pin-pointing China's attack against GitHub," Errata Security, April 1, 2015, accessed March 18, 2022, <https://blog.erratasec.com/2015/04/pin-pointing-chinas-attack-against.html#.YYsQhWDML-g>.
- 129 Bill Marczak et al., "China's Great Cannon," Citizen Lab, April 10, 2015, accessed March 18, 2022, [hxxps://citizenlab.ca/2015/04/chinas-great-cannon](https://citizenlab.ca/2015/04/chinas-great-cannon).
- 130 Charlie, "We are under attack," Greatfire.org, March 19, 2015, accessed March 18, 2022, <https://en.greatfire.org/blog/2015/mar/we-are-under-attack>.

- 131 Niels Provos, "A Javascript-based DDoS Attack as seen by Safe Browsing," Google Security Blog, April 24, 2015, accessed March 18, 2022, <https://security.googleblog.com/2015/04/a-javascript-based-ddos-attack-as-seen.html>.
- 132 "IP Lookup for 114.113.156.119," Geoplookup, n.d., accessed March 18, 2022, <http://geoplookup.net/ip/114.113.156.119>.
- 133 "IP Lookup for 203.90.242.126," Geoplookup, n.d., accessed March 18, 2022, <http://geoplookup.net/ip/203.90.242.126>.
- 134 "Using Baidu 百度 to steer millions of computers to launch denial of service attacks," March 25, 2015, accessed March 18, 2022, https://drive.google.com/file/d/0ByrxblDXR_yqeUNZYU5WcjFCbXM/view?resourcekey=0-08k-QXs9Vv5fqoJmTvzTTw.
- 135 GreatFire.org (@GreatFireChina), "Pls note: greatfire.org is not being DDoSed..." Twitter, March 19, 2015 2:57 PM, accessed March 18, 2022, <https://twitter.com/GreatFireChina/status/578631443309572096>.
- 136 Charlie, "We are under attack," Greatfire.org, March 19, 2015, accessed March 18, 2022, <https://en.greatfire.org/blog/2015/mar/we-are-under-attack>.
- 137 "Using Baidu 百度 to steer millions of computers to launch denial of service attacks," March 25, 2015, accessed March 18, 2022, https://drive.google.com/file/d/0ByrxblDXR_yqeUNZYU5WcjFCbXM/view?resourcekey=0-08k-QXs9Vv5fqoJmTvzTTw.
- 138 Erik Hjelmvik, "China's Man-on-the-Side Attack on GitHub," Netresec, March 31, 2015, accessed March 18, 2022, <https://www.netresec.com/index.ashx?page=Blog&month=2015-03&post=China%27s-Man-on-the-Side-Attack-on-GitHub>.
- 139 Robert Hackett, "GitHub triumphant over its 'largest ever' cyber pummeling," Fortune, April 3, 2015, accessed March 18, 2022, <https://fortune.com/2015/04/03/github-ddos-china>.
- 140 Anthr@x, "Baidu's traffic hijacked to DDoS GitHub.com [Updated]," Insight-labs, March 27, 2015, (archived by Internet Archive on June 5, 2015), <https://web.archive.org/web/20150605092047/http://insight-labs.org/?p=1682>.
- 141 Niels Provos, "A Javascript-based DDoS Attack as seen by Safe Browsing," Google Security Blog, April 24, 2015, accessed March 18, 2022, <https://security.googleblog.com/2015/04/a-javascript-based-ddos-attack-as-seen.html>.
- 142 "GitHub Blog Search: Search Results for: ddos," GitHub Blog, n.d., accessed March 18, 2022, <https://github.blog/?s=ddos>.
- 143 Jesse Newland, "Large Scale DDoS Attack on github.com," Github Blog, March 27, 2015, accessed March 21, 2022, <https://github.blog/2015-03-27-large-scale-ddos-attack-on-github-com>.
- 144 Russell Brandom, "Last night, GitHub was hit with massive denial-of-service attack from China," *The Verge*, March 27, 2015, accessed March 21, 2022, <https://www.theverge.com/2015/3/27/8299555/github-china-ddos-censorship-great-firewall>.
- 145 Bill Marczak et al., "China's Great Cannon," Citizen Lab, April 10, 2015, accessed March 18, 2022, <https://citizenlab.ca/2015/04/chinas-great-cannon>.
- 146 "China's 'Great Cannon' programme has been in development for about a year, sources say," *South China Morning Post*, last modified April 15, 2015, (archived by Internet Archive on April 25, 2015), <https://web.archive.org/web/20150425175122/http://www.scmp.com/news/china/article/1764378/chinas-great-cannon-programme-has-been-development-about-year-sources-say>.
- 147 "China's 'Great Cannon' programme has been in development for about a year, sources say," *South China Morning Post*, last modified April 15, 2015, (archived by Internet Archive on April 25, 2015), <https://web.archive.org/web/20150425175122/http://www.scmp.com/news/china/article/1764378/chinas-great-cannon-programme-has-been-development-about-year-sources-say>.
- 148 Jonathan Woetzel et al., "China's Digital Economy: a Leading Global Force," McKinsey & Company, August 2017, accessed March 21, 2022, <https://www.mckinsey.com/-/media/mckinsey/featured%20insights/China/Chinas%20digital%20economy%20leading%20global%20force/MGI-Chinas-digital-economy-A-leading-global-force.ashx>.
- 149 Meaghan Tobin, "GitHub is China's last land of free speech - but for how long?," Rest of World, November 1, 2021, accessed March 21, 2022, <https://restofworld.org/2021/github-microsoft-in-china-how-long>.
- 150 Rita Liao, "China is building a GitHub alternative called Gitee," TechCrunch, August 21, 2020, accessed March 21, 2022, <https://techcrunch.com/2020/08/21/china-is-building-its-github-alternative-gitee>.
- 151 "Unblocked Website: Mingjing News," Reports Without Borders, n.d., accessed March 21, 2022, <https://rsf.org/en/mingjing-news>.
- 152 飞鸽传书 ("The Pigeon Post"), "郭文贵将曝中共贪官恶吏内幕 | 明镜邮报 ("Guo Wengui will expose the inside story of the CCP's corrupt and evil officials | *Mingjing News*)," 环球实报 ("Global Report"), January 26, 2017, accessed March 21, 2022, <https://hqsb.wordpress.com/2017/01/26/%E9%83%AD%E6%96%87%E8%B4%8B%5E5%86%86%E6%9B%9D%E4%B8%AD%E5%85%81%8B%4AA%E5%AE%98%E6%81%86%E5%90%8F%E5%86%85%85%85%95%95%98%8E%99%95%9C%E9%82%AE%E6%8A%A5>.
- 153 Miles Kwok, "Guo Wengui - Mingjing Interview - 1/26/2017," YouTube, October 25, 2017, accessed March 21, 2022, <https://www.youtube.com/watch?v=jYQkCseeisE>.
- 154 Kate O'Keeffe, Aruna Viswanatha and Cezary Podkul, "China's Pursuit of Fugitive Businessman Guo Wengui Kicks Off Manhattan Caper Worthy of Spy Thriller," *The Wall Street Journal*, last modified October 22, 2017, accessed March 21, 2022, <https://www.wsj.com/articles/chinas-hunt-for-guo-wengui-a-fugitive-businessman-kicks-off-manhattan-caper-worthy-of-spy-thriller-1508717977>.
- 155 Kate O'Keeffe, Aruna Viswanatha and Cezary Podkul, "China's Pursuit of Fugitive Businessman Guo Wengui Kicks Off Manhattan Caper Worthy of Spy Thriller," *The Wall Street Journal*, last modified October 22, 2017, accessed March 21, 2022, <https://www.wsj.com/articles/chinas-hunt-for-guo-wengui-a-fugitive-businessman-kicks-off-manhattan-caper-worthy-of-spy-thriller-1508717977>.
- 156 "China accuses mogul of rape in quest to get him out of U.S.," CBS News, August 31, 2017, March 21, 2022, <https://www.cbsnews.com/news/china-guo-wengui-rape-new-york-based-chinese-billionaire-corruption>.
- 157 Charles Lau, "Hong Kong police investigating fugitive Chinese tycoon Guo Wengui over alleged HK\$32 billion money laundering conspiracy, court papers reveal," *South China Morning Post*, last modified August 15, 2018, accessed March 21, 2022, <https://web.archive.org/web/20180821031711/https://www.scmp.com/news/hong-kong/hong-kong-law-and-crime/article/2159724/hong-kong-police-investigating-fugitive>.
- 158 Gerry Shih, "AP Exclusive: China accuses outspoken tycoon in US of rape," AP News, August 31, 2017, accessed March 21, 2022, <https://apnews.com/article/ap-top-news-sexual-assault-international-news-arrests-politics-9a4b4be3f0fb4e7191a53b9368318513>.
- 159 "Chinese-American journalist says wife kidnapped by China," CBS News, January 17, 2018, accessed March 21, 2022, <https://www.cbsnews.com/news/china-wife-chinese-american-journalist-chen-xiaoping>.

- 160 “明镜电视直播郭文贵，拉开中国政治大戏 (“Mingjing News livestreams Guo Wengui, kicking off major Chinese political drama”),” RFI, February 12, 2017, accessed March 21, 2022, <https://www.rfi.fr/cn/%e4%b8%ad%e5%9b%bd/20170212-%e6%98%8e%e9%95%9c%e7%94%b5%e8%a7%86%e7%9b%b-4%e6%92%ad%e9%83%ad%e6%96%87%e8%b4%b5%ef%b-c%8c%e6%8b%89%e5%bc%80%e4%b8%ad%e5%9b%b-d%e6%94%bf%e6%b2%bb%e5%a4%a7%e6%88%8f>.
- 161 Jakub Dalek et al., “Insider Information: An intrusion campaign targeting Chinese language news sites,” The Citizen Lab, July 5, 2017, accessed March 21, 2022, <https://citizenlab.ca/2017/07/insider-information-an-intrusion-campaign-targeting-chinese-language-news-sites/>.
- 162 Williamli (edited by Cody Gray), “What is randomly replacing Baidu Tongji (Analytics)’s Javascript code to make DDOS attack on websites on browser?,” StackOverflow, last modified August 25, 2017, accessed March 21, 2022, <https://stackoverflow.com/questions/45874555/what-is-randomly-replacing-baidu-tongji-analyticss-javascript-code-to-make-dd>.
- 163 Williamli (edited by Cody Gray), “What is randomly replacing Baidu Tongji (Analytics)’s Javascript code to make DDOS attack on websites on browser?,” StackOverflow, last modified August 25, 2017, accessed March 21, 2022, <https://stackoverflow.com/questions/45874555/what-is-randomly-replacing-baidu-tongji-analyticss-javascript-code-to-make-dd>.
- 164 “shanxidianyuan.net,” URLscan.io, November 20, 2018, accessed March 21, 2022, <https://urlscan.io/result/3fd5a719-24d9-42cd-ae10-87129ad87fd1/#transactions>.
- 165 Nectar Gan, “Fugitive Chinese tycoon Guo Wengui ‘has US\$1.1 billion of assets frozen by Hong Kong court’,” South China Morning Post November 20, 2018, accessed March 21, 2022, (reposted by Yahoo!news), <https://sg.news.yahoo.com/fugitive-chinese-tycoon-guo-wengui-143352034.html>.
- 166 “Steve Bannon, exiled Chinese billionaire Guo Wengui unite against China ‘assassinations’,” The Straits Times, November 21, 2018, accessed March 21, 2022, <https://www.straitstimes.com/asia/east-asia/steve-bannon-exiled-chinese-billionaire-guo-wengui-unite-behind-china-crimes>.
- 167 “Tweeting through the Great Firewall,” Australian Strategic Policy Institute, September 3, 2019, accessed March 21, 2022, <https://www.aspi.org.au/report/tweeting-through-great-firewall>.
- 168 “Tweeting through the Great Firewall,” Australian Strategic Policy Institute, September 3, 2019, accessed March 21, 2022, <https://www.aspi.org.au/report/tweeting-through-great-firewall>.
- 169 Jakub Dalek et al., “Insider Information: An intrusion campaign targeting Chinese language news sites,” The Citizen Lab, July 5, 2017, accessed March 21, 2022, <https://citizenlab.ca/2017/07/insider-information-an-intrusion-campaign-targeting-chinese-language-news-sites/>.
- 170 Jakub Dalek et al., “Insider Information: An intrusion campaign targeting Chinese language news sites,” The Citizen Lab, July 5, 2017, accessed March 21, 2022, <https://citizenlab.ca/2017/07/insider-information-an-intrusion-campaign-targeting-chinese-language-news-sites/>.
- 171 Gwynn Guilford, “The Secret History of Hong Kong’s Democratic Stalemate,” The Atlantic, October 14, 2014, accessed March 21, 2022, <https://www.theatlantic.com/international/archive/2014/10/the-secret-history-of-hong-kongs-democratic-stalemate/381424>.
- 172 Matt Schiavenza, “Why Didn’t Britain Democratize Hong Kong?,” Asia Society, February 8, 2018, accessed March 21, 2022, <https://asiasociety.org/new-york/why-didnt-britain-democratize-hong-kong>.
- 173 Natalie Lung and Iain Marlow, “Hong Kong’s Autonomy,” Bloomberg, October 24, 2019, accessed March 21, 2022, <https://www.bloomberg.com/quicktake/hong-kongs-autonomy>.
- 174 “DECISION OF THE STANDING COMMITTEE OF THE NATIONAL PEOPLE’S CONGRESS ON ISSUES RELATING TO THE METHODS FOR SELECTING THE CHIEF EXECUTIVE OF THE HONG KONG SPECIAL ADMINISTRATIVE REGION AND FOR FORMING THE LEGISLATIVE COUNCIL OF THE HONG KONG SPECIAL ADMINISTRATIVE REGION IN THE YEAR 2012 AND ON ISSUES RELATED TO UNIVERSAL SUFFRAGE (ADOPTED BY THE STANDING COMMITTEE OF THE TENTH NATIONAL PEOPLE’S CONGRESS AT ITS THIRTY-FIRST SESSION ON 29 DECEMBER 2007),” Hong Kong Legal Information Institute, n.d., accessed March 21, 2022, <https://web.archive.org/web/2008122314014/http://www.hklii.org/hk/legis/en/ord/2211/longtitle.html>.
- 175 “Yang Jiechi States China’s Solemn Position on Issues Related to Xinjiang and Hong Kong,” Embassy of the People’s Republic of China in the United States of America, June 12, 2021, accessed March 21, 2022, <https://www.fmprc.gov.cn/ce/ceus/eng/zmgxs/t1883498.htm>.
- 176 “Hong Kong votes on electoral reform despite Chinese opposition,” The Guardian, June 20, 2014, accessed March 21, 2022, <https://www.theguardian.com/world/2014/jun/20/hong-kong-votes-electoral-reform-despite-chinese-opposition>.
- 177 “Hong Kong democracy ‘referendum’ draws nearly 800,000,” BBC, June 30, 2014, accessed March 21, 2022, <https://www.bbc.com/news/world-asia-china-28076566>.
- 178 “V. Fully and Accurately Understanding and Implementing the Policy of ‘One Country, Two Systems,’ in The Practice of the ‘One Country, Two Systems’ Policy in the Hong Kong Special Administrative Region, June 2014, http://www.china.org.cn/government/whitepaper/2014-06/10/content_32623618.htm.
- 179 “国务院港澳办:香港进行所谓公投均非法无效 (“Hong Kong and Macao Affairs Office of the State Council: Hong Kong’s so-called referendum is illegal and invalid)” Xinhua, June 20, 2014, accessed March 21, 2022, (republished by Sina), <http://news.sina.com.cn/c/2014-06-20/233030399920.shtml>.
- 180 “IFJ condemns cyber attack on site reporting Hong Kong ‘referendum’,” International Federal of Journalists, n.d., accessed March 21, 2022, <https://www.ifj.org/es/centro-de-medios/noticias/detalle/category/press-releases/article/ifj-condemns-cyber-attack-on-site-reporting-hong-kong-referendum.html>.
- 181 “「6.22 民間全民投票」活動報告 (“6.22 Civil Referendum’ activity report”),” 香港大學民意研究計劃 (“Public Opinion Research Project of the University of Hong Kong”), February 15, 2015, accessed March 21, 2015, https://popvote.hk/doc/popvote622_activity_report_tc.pdf?v=20150216. (p. 38).
- 182 “香港全民投票日未到 网站遭骇客攻击(图) (“Hong Kong’s website hit by hackers before referendum day (Photos)”),” Vision Times, June 16, 2014, accessed March 21, 2022, <https://www.secretchina.com/news/gb/2014/06/16/544047.html>.
- 183 “佔中網被駭 恐影響投票數 (“Occupy Central Online Hacked. Impact on Vote Count Feared.”),” Apple Daily, June 16, 2014, accessed March 21, 2022, (archived by Internet Archive on September 18, 2019), <https://web.archive.org/web/20190918212222/https://tw.appledaily.com/headline/daily/20140616/35896723/>.
- 184 “「6.22民間全民投票」模擬投票系統受到龐大攻擊 (“6.22 Civil Referendum’ mock voting system under massive attack”),” HKU POP SITE, June 16, 2014, accessed March 22, 2022, <https://www.hkupop.hku.hk/chinese/release/release1149.html>.
- 185 “「6.22民間全民投票」模擬投票系統受到龐大攻擊 (“6.22 Civil Referendum’ mock voting system under massive attack”),” HKU POP SITE, June 16, 2014, accessed March 22, 2022, <https://www.hkupop.hku.hk/chinese/release/release1149.html>.

- 186 Mr Jazz MA, "POPVote Technical Sharing Seminar," POPVOTE, September 2014, accessed March 22, 2022, https://www.hkupop.hku.hk/english/resources/workshops/20140925/PopVote_Seminar_22sept2014_Jazz.pdf.
- 187 Matthew Prince (@eastdakota), "Battling 300Gbps+ attack right now...," Twitter, June 19, 2014 7:28 PM, (archived by Internet Archive on November 11, 2014), <https://web.archive.org/web/20141111142339/https://twitter.com/eastdakota/statuses/479812898315706368>.
- 188 Peter Apps, "DDoS cyber attacks get bigger, smarter, more damaging," Reuters, March 5, 2014, accessed March 22, 2022, <https://www.reuters.com/article/us-cyber-ddos/ddos-cyber-attacks-get-bigger-smarter-more-damaging-idUSBREA240XZ20140305>.
- 189 Jazz Ma, "POPVote Technical Sharing Seminar," POPVOTE, September 2014, accessed March 22, 2022, https://www.hkupop.hku.hk/english/resources/workshops/20140925/PopVote_Seminar_22sept2014_Jazz.pdf. (p. 47–49)
- 190 Jeffie Lam, "More than 400,000 vote in Occupy Central's electoral reform poll," International Viewpoint, June 24, 2014, accessed March 22, 2022, <https://internationalviewpoint.org/spip.php?article3426>.
- 191 Jazz Ma, "POPVote Technical Sharing Seminar," POPVOTE, September 2014, accessed March 22, 2022, https://www.hkupop.hku.hk/english/resources/workshops/20140925/PopVote_Seminar_22sept2014_Jazz.pdf. (p. 47–49)
- 192 Thomas Fox-Brewster, "Did China Order Hackers to Cripple the Hong Kong Protest?," Vice, November 5, 2014, accessed March 22, 2022, <https://www.vice.com/en/article/539wnz/inside-the-unending-cyber-siege-of-hong-kong>.
- 193 Thomas Fox-Brewster, "Did China Order Hackers to Cripple the Hong Kong Protest?," Vice, November 5, 2014, accessed March 22, 2022, <https://www.vice.com/en/article/539wnz/inside-the-unending-cyber-siege-of-hong-kong>.
- 194 IFJ condemns cyber attack on site reporting Hong Kong 'referendum,' International Federal of Journalists, n.d., accessed March 21, 2022, <https://www.ifj.org/es/centro-de-medios/noticias/detalle/category/press-releases/article/ifj-condemns-cyber-attack-on-site-reporting-hong-kong-referendum.html>.
- 195 Lai Ying-kit, "Cyberattackers brought down Apple Daily website with 40 million hits every second," South China Morning Post, last modified June 20, 2014, accessed March 22, 2022, <https://www.scmp.com/news/hong-kong/article/1535484/apple-daily-website-taken-offline-cyberattack-ahead-occupy-vote>.
- 196 IFJ condemns cyber attack on site reporting Hong Kong 'referendum,' International Federal of Journalists, n.d., accessed March 21, 2022, <https://www.ifj.org/es/centro-de-medios/noticias/detalle/category/press-releases/article/ifj-condemns-cyber-attack-on-site-reporting-hong-kong-referendum.html>.
- 197 Lai Ying-kit, "Cyberattackers brought down Apple Daily website with 40 million hits every second," South China Morning Post, last modified June 20, 2014, accessed March 22, 2022, <https://www.scmp.com/news/hong-kong/article/1535484/apple-daily-website-taken-offline-cyberattack-ahead-occupy-vote>.
- 198 Michele Fan (@wingp), "@appledaily_hk not only its website was attacked by DDoS, hacker(s) had deleted part of the papers' archive #HK," Twitter, June 20, 2014 8:55 AM, accessed March 22, 2022, <https://twitter.com/wingp/status/48001605410166145/photo/1>.
- 199 IFJ condemns cyber attack on site reporting Hong Kong 'referendum,' International Federal of Journalists, n.d., accessed March 21, 2022, <https://www.ifj.org/es/centro-de-medios/noticias/detalle/category/press-releases/article/ifj-condemns-cyber-attack-on-site-reporting-hong-kong-referendum.html>.
- 200 Joyce Ng, "Occupy Central co-founder Benny Tai urges Hong Kong's democracy fighters to 'first protect themselves,'" South China Morning Post, last modified September 14, 2015, accessed March 22, 2022, <https://www.scmp.com/news/hong-kong/politics/article/1857813/occupy-central-co-founder-benny-tai-urges-hong-kongs>.
- 201 Wing-Wah Law, Politics, Managerialism, and University Governance: Lessons from Hong Kong Under China's Rule Since 1997, Springer Singapore, March 20, 2019, https://www.google.com/books/edition/Politics_Managerialism_and_University_Go/nbSPDwAAQBA-J?hl=en&gbpv=1&dq=Benny+Tai+email+hacked+2014&pg=PA97&printsec=frontcover. (p. 97)
- 202 Bryan Harris, "Hackers target email account of University of Hong Kong vice chancellor," South China Morning Post, last modified April 26, 2015, accessed March 22, 2022, <https://www.scmp.com/news/hong-kong/politics/article/1776567/hackers-target-email-account-university-hong-kong-vice>.
- 203 Adam Kozy, "Occupy Central: The Umbrella Revolution and Chinese Intelligence," CrowdStrike, October 2, 2014, accessed May 26, 2022, <https://www.crowdstrike.com/blog/occupy-central-the-umbrella-revolution-and-chinese-intelligence/>.
- 204 "Hong Kong Media Tycoon Blames China For Attack on Website," Radio Free Asia, June 18, 2014, accessed March 22, 2022, <https://www.rfa.org/english/news/china/attack-06182014182526.html>.
- 205 "China Link Alleged to Cyberattack as Hong Kong Tensions Grow," Radio Free Asia, June 25, 2014, accessed March 22, 2022, <https://www.rfa.org/english/news/china/link-06252014150922.html>.
- 206 "揪出公投黑客 中移动中科院 發動四成攻擊, ("Referendum Hackers Uncovered, China Mobile and Chinese Academy of Sciences Launch 40% of the Attack")," 壹週刊 ("Next Magazine") issue 1268, accessed March 22, 2022, (reposted by 热爆娱乐 ("Hot Explosive Entertainment") on June 26, 2014) (archived by Internet Archive on November 13, 2020), https://web.archive.org/web/20201113200911/https://hittt.blogspot.com/2014/06/1268-m1_4237.html.
- 207 "中国移动驳斥香港《壹周刊》所谓‘公投黑客’报道 ("China Mobile refutes Hong Kong's Next Magazine's so-called 'referendum hack' report)," China News, June 27, 2014, accessed March 22, 2022, <https://web.archive.org/web/20140629235556/http://www.chinanews.com/ga/2014/06-27/6329026.shtml>.
- 208 Peter Apps, "DDoS cyber attacks get bigger, smarter, more damaging," Reuters, March 5, 2014, accessed March 22, 2022, <https://www.reuters.com/article/us-cyber-ddos/ddos-cyber-attacks-get-bigger-smarter-more-damaging-idUSBREA240XZ20140305>.
- 209 Terence Yun, "假佔中投票網站露出馬腳 ("Fake Occupy Central voting website exposed")," 鹿米館 ("Lumiguan"), June 27, 2014, accessed March 22, 2022, https://lunkayun.blogspot.com/2014/06/blog-post_27.html.
- 210 Terence Yun, "假民間公投網站 檔案名稱露出馬腳 ("Fake civil referendum website, file name exposed")," VJ Media, June 27, 2014, accessed March 22, 2022, <https://www.vjmedia.com.hk/articles/2014/06/27/76525/%E5%81%87%E6%B0%91%E9%96%93%E5%85%AC%E6%8A%95%E7%B6%B2%E7%AB%99%E3%80%80%E6%AA%94%E6%A1%88%E5%90%8D%E7%A8%B1%E9%9C%B2%E5%87%BA%E9%A6%AC%E8%85%83>.
- 211 Tripti Lahiri, "Refresher Course on Hong Kong's 2014 Umbrella Movement," Quartz, September 27, 2019, accessed March 22, 2022, <https://qz.com/1714897/what-was-hong-kongs-umbrella-movement-about>.
- 212 "Hong Kong protests: Timeline of the occupation," BBC, December 11, 2014, accessed March 22, 2022, <https://www.bbc.com/news/world-asia-china-30390820>.

- 213 Ohad Bobrov, "Lacoon Discovers Xsser mRAT, the First Advanced iOS Trojan," Lacoon Mobile Security, September 30, 2014, (archived by Internet Archive on October 1, 2014), <https://web.archive.org/web/20141001000258/https://www.lacoon.com/lacoon-discovers-xsser-mrat-first-advanced-ios-trojan/>.
- 214 "DTL-12012015-01: Hong Kong SWC attack," Dragon Threat Labs, January 11, 2015, accessed March 22, 2022, <http://blog.dragonthreat-labs.com/2015/01/dtl-12012015-01-hong-kong-swc-attack.html>.
- 215 "Democracy in Hong Kong Under Attack," Volexity, October 9, 2014, (archived by Internet Archive on July 30, 2017), <https://web.archive.org/web/20170730230501/https://www.volexity.com/blog/2014/10/09/democracy-in-hong-kong-under-attack>.
- 216 Carol Ko and Sheila Lam, "Next Media: under cyberattack and operations disruption," Computer World Hong Kong, October 14, 2014, (archived by Internet Archive on November 3, 2014), "<https://web.archive.org/web/20141103120055/http://cw.com.hk/news/next-media-under-cyberattack-and-operations-disruption>.
- 217 Christopher Beam, "Hong Kong's Own Reddit Is Doing the Protesters' Dirty Work—Sometimes too Dirty," *The New Republic*, October 15, 2014, accessed March 22, 2022, <https://newrepublic.com/article/119835/hong-kong-golden-website-doing-occupy-protesters-dirty-work>.
- 218 Jeff Chu and Helsa Chan, "5 Ways Protesters Organized #OccupyCentral," *Fast Company*, September 29, 2014, accessed March 22, 2022, <https://www.fastcompany.com/3036374/5-ways-protesters-organized-occupycentral>.
- 219 Parmy Olson, "The Largest Cyber Attack In History Has Been Hitting Hong Kong Sites," *Forbes*, November 20, 2014, accessed March 22, 2022, <https://www.forbes.com/sites/parmyolson/2014/11/20/the-largest-cyber-attack-in-history-has-been-hitting-hong-kong-sites>.
- 220 Kirk Soluk, "DDoS Activity in the Context of Hong Kong's Pro-democracy Movement," Arbor Networks, November 11, 2014, (archived by Internet Archive on January 1, 2015), <https://web.archive.org/web/20150101180554/http://www.arbornetworks.com/asert/2014/11/ddos-activity-in-the-context-of-hong-kongs-pro-democracy-movement>.
- 221 Ned Moran, Mike Oppenheim, and Mike Scott, "Operation Poisoned Handover: Unveiling Ties Between APT Activity in Hong Kong's Pro-Democracy Movement," FireEye, November 3, 2014, (archived by Internet Archive on March 31, 2015), <https://www.fireeye.com/blog/threat-research/2014/11/operation-poisoned-handover-unveiling-ties-between-apt-activity-in-hong-kongs-pro-democracy-movement.html>.
- 222 Kirk Soluk, "DDoS Activity in the Context of Hong Kong's Pro-democracy Movement," Arbor Networks, November 11, 2014, (archived by Internet Archive on January 1, 2015), <https://web.archive.org/web/20150101180554/http://www.arbornetworks.com/asert/2014/11/ddos-activity-in-the-context-of-hong-kongs-pro-democracy-movement>.
- 223 Ned Moran, Mike Oppenheim, and Mike Scott, "Operation Poisoned Handover: Unveiling Ties Between APT Activity in Hong Kong's Pro-Democracy Movement," FireEye, November 3, 2014, (archived by Internet Archive on March 31, 2015), <https://www.fireeye.com/blog/threat-research/2014/11/operation-poisoned-handover-unveiling-ties-between-apt-activity-in-hong-kongs-pro-democracy-movement.html>.
- 224 "When Pandas Attack: Defending A Technology Company," CrowdStrike, n.d., (archived by Internet Archive on April 1, 2015), https://web.archive.org/web/20150401010832/https://www.CrowdStrike.com/wp-content/uploads/2015/03/CrowdStrike-Case-Study_When-Pandas-Attack.pdf.
- 225 "Democracy in Hong Kong Under Attack," Volexity, October 9, 2014, (archived by Internet Archive on July 30, 2017), <https://web.archive.org/web/20170730230501/https://www.volexity.com/blog/2014/10/09/democracy-in-hong-kong-under-attack>.
- 226 Michael Forsythe, "U.N. Human Rights Panel Urges China to Allow Free Elections in Hong Kong," *The New York Times*, October 23, 2014, accessed March 22, 2022, <https://www.nytimes.com/2014/10/24/world/asia/un-urges-china-to-allow-free-elections-in-hong-kong.html>.
- 227 "China says U.N. rights covenant no measure for Hong Kong reform," Reuters, n.d., accessed March 22, 2022, <https://www.reuters.com/article/us-china-hongkong-un/china-says-u-n-rights-covenant-no-measure-for-hong-kong-reform-idUSKCN0ID14U20141024>.
- 228 "Facts about Hong Kong's extradition bill," Reuters, n.d., accessed March 22, 2022, <https://www.reuters.com/article/us-hongkong-protests-extradition-law-fac/facts-about-hong-kongs-extradition-bill-idUSKCN1VP0OF>.
- 229 James Pomfret and Anne Marie Roantree, "Protesters arrested in Hong Kong over proposed China extradition law," Reuters, n.d., accessed March 22, 2022, <https://www.reuters.com/article/us-hongkong-politics-extradition/protesters-arrested-in-hong-kong-over-proposed-china-extradition-law-idUSKCN1QW1AC>.
- 230 Jeff Li, "China's history of extraordinary rendition," BBC, June 16, 2019, accessed March 22, 2022, <https://www.bbc.com/news/world-asia-china-48634136>.
- 231 Katie Tam, "Over concerns, Hong Kong introduces revised extradition laws," AP, April 3, 2019, accessed March 22, 2022, <https://apnews.com/article/f330237ed2a341e2919f16c5a8bbe9ca>.
- 232 Helen Davidson and Lily Kuo, "Hong Kong protests: government vows to push ahead with extradition bill," *The Guardian*, June 10, 2019, (archived by Internet Archive on October 8, 2019), <https://web.archive.org/web/20191008152047/https://www.theguardian.com/world/2019/jun/10/hong-kong-protests-china-state-media-foreign-forces-extradition-bill>.
- 233 "Hong Kong formally scraps extradition bill that sparked protests," BBC, October 23, 2019, accessed March 22, 2022, <https://www.bbc.com/news/world-asia-china-50150853>.
- 234 Emma Graham-Harrison, "Hong Kong voters deliver landslide victory for pro-democracy campaigners," *The Guardian*, November 25, 2019, accessed March 22, 2022, <https://www.theguardian.com/world/2019/nov/24/hong-kong-residents-turn-up-for-local-elections-in-record-numbers>.
- 235 Jeffie Lam, Sum Lok-kei, and Ng Kang-chung, "Hong Kong elections: pro-democracy camp wins 17 out of 18 districts while city leader says she will reflect on the result," *South China Morning Post*, last modified November 25, 2019, accessed March 22, 2022, <https://www.scmp.com/news/hong-kong/politics/article/3039151/hong-kong-elections-tsunami-disaffection-washes-over-city>.
- 236 Telegram Messenger (@telegram), "We're currently experiencing a powerful DDoS attack, Telegram users in the Americas and some users from other countries may experience connection issues," Twitter, June 12, 2019 4:20 AM, accessed March 22, 2022, <https://twitter.com/telegram/status/1138768124914929664>.
- 237 Danny Vincent, "How apps power Hong Kong's 'leaderless' protests," BBC, June 30, 2019, accessed March 22, 2022, <https://www.bbc.com/news/technology-48802125>.

- 238 Pavel Durov (@durov), "IP addresses coming mostly from China. Historically, all state actor-sized DDoS (200-400 Gb/s of junk) we experienced coincided in time with protests in Hong Kong (coordinated on @telegram). This case was not an exception." Twitter, June 12, 2019 3:53 PM, accessed March 22, 2022, <https://twitter.com/durov/status/1138942773430804480>.
- 239 "Hong Kong faces shut down over extradition bill," *Asia Times*, June 11, 2019, accessed March 22, 2022, <https://asiatimes.com/2019/06/push-to-shut-down-hong-kong-as-extradition-bill-debated>.
- 240 LIHKG, "LIHKG has been under unprecedeted DDoS attacks in the past 24 hours...", LIHKG, August 31, 2019 6:15:21 PM, (archived by Internet Archive on September 2, 2019), <https://web.archive.org/web/20190901083158/https://lihkg.com/thread/1525319/page/1>.
- 241 Mike Ives and Austin Ramzy, "Hong Kong Protesters Clash With Police After Defying Ban," *The New York Times*, last modified September 1, 2022, accessed March 31, 2022, <http://nytimes.com/2019/08/31/world/asia/hong-kong-protest.html>.
- 242 STAYC YOUNG LUV (@0w0ing), "#HongKongToday A forum where protesters are active is down again. the forum has been being ddos in large scale, especially from china. today is the #ChinaNatioanalDay , protests are all over Hong Kong, and lihkg is down again. #NotMyNationalDay #GoodMourningChina," Twitter, October 1, 2019 3:29 AM, accessed March 22, 2022, <https://twitter.com/0w0ing/status/1178934918681808896>.
- 243 LIHKG Forum (@lihkg_forum), Telegram, accessed October 4, 2021, https://t.me/s/lihkg_forum?before=11.
- 244 Jessie Yeung, James Griffiths and Steve George, "Hong Kong protesters hit the streets as China marks 70 years of Communist rule," CNN, last modified October 1, 2019, accessed March 23, 2022, <https://www.cnn.com/asia/live-news/china-hong-kong-oct-1-live-intl-hnk/index.html>.
- 245 Chris Doman, "The 'Great Cannon' has been deployed again," ATT – Alien Labs, December 4, 2019, (archived by Internet Archive on December 6, 2019), <https://web.archive.org/web/20191206074255/https://cybersecurity.att.com/blogs/labs-research/the-great-cannon-has-been-deployed-again>.
- 246 @fast13711, "準時 6 點 ddos ("The 6 o'clock ddos is on time")," Twitter, November 23, 2019 2:28 PM, <https://twitter.com/fast13711/status/1198367737791205376>.
- 247 "Election to last 15 hours," news.gov.hk, November 22, 2019, accessed March 23, 2022, https://www.news.gov.hk/eng/2019/11/20191122_161534_480.html.
- 248 Catie Keck, "Facebook and Twitter: It Sure Looks Like China's Spreading Bullshit About Hong Kong Protesters," *Gizmodo*, August 19, 2019, accessed March 23, 2022, <https://gizmodo.com/facebook-and-twitter-it-sure-looks-like-chinas-spreadi-1837383015>.
- 249 Dell Cameron, "YouTube Dismantles 'Influence Operation' Targeting Hong Kong Protests, Avoids Discussing Its Reach," *Gizmodo*, August 22, 2019, accessed March 23, 2022, <https://gizmodo.com/youtube-dismantles-influence-operation-targeting-hong-k-1837490031>.
- 250 "State-sponsored hackers target Amnesty International Hong Kong with sophisticated cyber-attack," Amnesty International, April 25, 2019, accessed March 23, 2022, <https://www.amnesty.org/en/latest/press-release/2019/04/state-sponsored-cyber-attack-hong-kong>.
- 251 "THREAT ACTOR TARGETING HONG KONG PRO-DEMOCRACY FIGURES," Red Alert, December 3, 2019, accessed March 23, 2022, <https://threatrecon.nshc.net/2019/12/03/threat-actor-targeting-hong-kong-activists>.
- 252 Michael D. Swaine, "Xi Jinping's Address to the Central Conference on Work Relating to Foreign Affairs: Assessing and Advancing Major-Power Diplomacy with Chinese Characteristics," *China Leadership Monitor*, no. 46, accessed April 15, 2022, https://carnegieendowment.org/files/Michael_Swaine_CLM_46.pdf.
- 253 John Ruwitch, "Satellites and seafood: China keeps fishing fleet connected in disputed waters," Reuters, July 27, 2014, (archived by Internet Archive on November 22, 2015), <https://web.archive.org/web/20151122233548/http://www.reuters.com:80/article/2014/07/28/us-southchinasea-china-fishing-insight-idUSKBNOF-WOQP20140728>.
- 254 Jeff Himmelman, "A Game of Shark and Minnow," *The New York Times*, October 27, 2013, <https://www.nytimes.com/newsgraph/2013/10/27/south-china-sea/index.html>.
- 255 M. Taylor Fravel, "China's Strategy in the South China Sea," *Contemporary Southeast Asia* Vol. 33, No. 3 (2011), <https://taylorfravel.com/documents/research/fravel.2011.CSA.china.strategy.scs.pdf>.
- 256 "Science of Military Strategy," China's Academy of Military Sciences, 2013, (translated by the China Aerospace Studies Institute), <https://www.airuniversity.af.edu/Portals/10/CASI/documents/Translations/2021-02-08%20Chinese%20Military%20Thoughts-%20In%20their%20own%20words%20Science%20of%20Military%20Strategy%202013.pdf?ver=NxAWg4BPw-NylEjxaha8Aw%3d%3d>. (p. 134)
- 257 Derek Grossman, "Vietnam Is the Chinese Military's Preferred Warm-Up Fight," RAND, May 15, 2019, accessed March 23, 2022, <https://www.rand.org/blog/2019/05/vietnam-is-the-chinese-militarys-preferred-warm-up.html>.
- 258 Mark Payumo, "How the Philippine Army Can Find Its Place in the South China Sea," *The Diplomat*, September 30, 2020, accessed March 23, 2022, <https://thediplomat.com/2020/09/how-the-philippine-army-can-find-its-place-in-the-south-china-sea>.
- 259 David Pilling, "China's spreading 'core interests,'" *Financial Times*, September 13, 2011, accessed March 23, 2022, <https://www.ft.com/content/7aadb3f3-bdd2-373e-98f6-3d9e46547e7c>.
- 260 Catherine Wong, "China blasts Nato with British aircraft carrier 'heading to South China Sea,'" *South China Morning Post*, last modified January 2, 2021, accessed March 23, 2022, <https://www.scmp.com/news/china/military/article/3116146/china-blasts-nato-british-aircraft-carrier-heading-south-china>.
- 261 "The South China Sea Case and China's New Nationalism," *The Diplomat*, July 19, 2016, accessed March 23, 2022, <https://thediplomat.com/2016/07/the-south-china-sea-case-and-chinas-new-nationalism>.
- 262 MANKA Channel, "Chinese ships destroy Vietnam sea cable," YouTube, June 2, 2011, accessed March 23, 2022, <https://www.youtube.com/watch?v=w1H6zcuXj8>.
- 263 "CHINESE MARINE SURVEILLANCE SHIPS VIOLATE VN'S SOVEREIGNTY," Embassy of the Socialist Republic of Vietnam in the United States of America, May 27, 2011, accessed March 22, 2022, <https://vietnamembassy-usa.org/news/2011/05/chinese-marine-surveillance-ships-violate-vns-sovereignty>.
- 264 Qin Jize and Zhou Wa, "FM: Vietnam's oil exploration 'violates consensus,'" *China Daily*, May 30, 2011, accessed March 23, 2022, http://www.chinadaily.com.cn/china/2011-05/30/content_12600945.htm.
- 265 Steven Groves and Dean Cheng, "A National Strategy for the South China Sea," The Heritage Foundation, April 24, 2014, accessed March 23, 2022, <https://www.heritage.org/asia/report/national-strategy-the-south-china-sea>.
- 266 Kevin Lim, "China says will not threaten anyone with modern military," Reuters, June 5, 2011, accessed March 23, 2022, <https://www.reuters.com/article/us-singapore-defence-idUSTRE753O920110605>.

- 267 “国内多家政府网站被黑 疑似越南黑客故意挑衅 (“Many domestic government websites hacked, suspected Vietnamese hackers intentionally provocative”),” e-gov.org.cn, April 14, 2012, accessed March 23, 2022, (archived by Internet Archive on August 31, 2019), https://web.archive.org/web/20190831191547/http://www.e-gov.org.cn/egov/web/article_detail.php?id=119305.
- 268 “Website chính phủ Trung Quốc bị hacker Việt Nam tấn công (“Chinese government website hacked by Vietnamese hackers”),” Tin Đa Chiều (“Multidimensional News”), June 2, 2011, accessed March 23, 2022, <https://www.tindachieu.com/news/2011/06/website-chinh-phu-trung-quoc-bi-hacker-viet-nam-tan-cong.html>.
- 269 “中越黑客大战 (“Sino-Vietnamese Hacker War”),” Baidu Baike, n.d., accessed March 23, 2022, <https://baike.baidu.com/item/%E4%B8%AD%E8%B6%8A%E9%BB%91%E5%AE%A2%E5%A4%A7%E6%88%98/5683627>.
- 270 “[RAT] Tống hợp 2011 - Hacker Việt Nam vs Hacker Trung Quốc (7/6/2011) (“[RAT] Summary 2011 - Vietnamese Hackers vs Chinese Hackers (June 7, 2011)”),” Tội phạm máy tính (“Computer crime”), June 4, 2011, accessed March 23, 2022, <http://www.toiphammaytinh.com/2011/06/tong-hop-2011-hacker-viet-nam-vs-hacker.html>.
- 271 “Tin tức đột nhập nhiều trang web TQ khẳng định chủ quyền của VN tại Biển Đông, (“Hackers break into multiple TQ websites, assert Vietnam sovereignty in South China Sea”),” VIETINFO, June 2, 2011, accessed March 23, 2022, <http://m.vietinfo.eu/chuyen-muc-bien-dong/tin-tac-dot-nhap-nhieu-trang-web-tq-khang-dinh-chu-quyen-cua-vn-tai-bien-dong.html>.
- 272 “中国红客联盟 (“Honker Union of China”),” Baidu Baike, n.d., accessed March 23, 2022, <https://baike.baidu.com/item/%E4%B8%AD%E5%9B%BD%E7%BA%A2%E5%AE%A2%E8%81%94%E7%9B%9F/837764>.
- 273 Michael Yip and Craig Webber, “Hacktivism: a theoretical and empirical exploration of China's cyber warriors,” Proceedings of the 3rd International Web Science Conference, June 2011, accessed March 23, 2022, https://www.researchgate.net/publication/262346542_Hacktivism_a_theoretical_and_empirical_exploration_of_China's_cyber_warriors.
- 274 Owen Fletcher, “Patriotic Chinese Hacking Group Reboots,” *The Wall Street Journal*, October 5, 2011, accessed March 23, 2022, <https://www.wsj.com/articles/BL-CJB-14435>.
- 275 Mihoko Matsubara, “Boosting Japan's Cybersecurity,” *The Japan Times*, October 26, 2012, (archived by Internet Archive on November 2, 2012), <https://web.archive.org/web/20121102103913/http://www.japantimes.co.jp:80/text/eo20121026a1.html>
- 276 Jojo Malig, “Chinese hackers target more PH websites,” ABS-CBN News, April 28, 2012, accessed March 23, 2022, <https://news.abs-cbn.com/-depth/04/25/12/chinese-hackers-target-more-ph-websites>.
- 277 Joe Stewart, “HTran and the Advanced Persistent Threat,” Secure-Works, August 3, 2011, accessed March 23, 2022, <https://www.secureworks.com/research/htran>.
- 278 Greg Walton, “Year of the Gh0st RAT,” Beijing Olympics 2008: Winning Press Conference, April 18-19, 2008, (archived by Internet Archive on August 11, 2009), <https://web.archive.org/web/20090811031100/http://www.beijing2008conference.com/articles.php?id=101>.
- 279 Bryan Krekel, George Bakos, and Christopher Barnett, “Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation,” U.S. China Economic and Security Review Commission, <https://apps.dtic.mil/sti/pdfs/ADA509000.pdf>.
- 280 Jeff Himmelman, “A Game of Shark and Minnow,” *The New York Times*, October 27, 2013, accessed March 23, 2022, <https://www.nytimes.com/newsgraphics/2013/10/27/south-china-sea/index.html>.
- 281 Brian Spegele and Wayne Ma, “For China Boss, Deep-Water Rigs Are a ‘Strategic Weapon,’ ” *The Wall Street Journal*, last modified August 29, 2012, accessed March 23, 2022, <https://www.wsj.com/articles/SB1000087239639044233104577592890738740290>.
- 282 Martin N. Murphy, “Deep-Water Oil Rigs as Strategic Weapons,” *The Atlantic Council*, September 19, 2012, accessed March 23, 2022, <https://www.atlanticcouncil.org/blogs/new-atlanticist/deepwater-oil-rigs-as-strategic-weapons>.
- 283 “Viet Nam's International Press Conference on 7th May 2014,” Die Botschaft der Sozialistischen Republik Vietnam in der Bundesrepublik Deutschland (“The embassy of the Socialist Republic of Vietnam in the Federal Republic of Germany”), <http://www.vietnamambotschaft.org/viet-nams-international-press-conference-on-7th-may-2014/>.
- 284 ejang, Thread: “饮水思源 (When you drink water, consider the source),” May 8, 2014 at 13:44:21, (archived by Internet Archive on June 26, 2017), <https://web.archive.org/web/20170626011749/http://bbs.sjtu.edu.cn/bbswaptcon/board,Military,reid,1399475438,-file,M.1399516847.A.html>.
- 285 Michael Green et al., “COUNTER-COERCION SERIES: CHINA-VIETNAM OIL RIG STANDOFF,” Asia Maritime Transparency Initiative, June 12, 2017, accessed March 23, 2022, <https://amtis.csis.org/counter-co-oil-rig-standoff>.
- 286 “Nguy cơ bùng phát chiến tranh mạng Việt – Trung? (Risk of Outbreak of Vietnam-China cyberwar?),” ICTNews, May 11, 2014, accessed March 23, 2022, <https://ictnews.vietnamnet.vn/cuoc-song-so/nguy-co-bung-phat-chien-tranh-mang-viet-trung-385334.html>.
- 287 Hạnh Thảo, “Hàng trăm Website của Việt Nam bị hacker tấn công (“Hundreds of Vietnamese Websites Hacked by Hackers”),” *Security Daily*, May 10, 2014, accessed March 23, 2022, <https://securitydaily.net/hang-tram-website-vietnam-bi-hacker-tan-cong>.
- 288 “Lộ diện nhóm hacker Trung Quốc (“Revealing the Chinese hacker group”),” Báo Người Lao Động (“The Labor Newspaper”) May 13, 2014, accessed March 23, 2022, <https://nld.com.vn/khoa-hoc/lo-dien-nhom-hacker-trung-quoc-20140513224345766.htm>.
- 289 “Lộ diện nhóm hacker Trung Quốc (“Revealing the Chinese hacker group”),” Báo Người Lao Động (“The Labor Newspaper”) May 13, 2014, accessed March 23, 2022, <https://nld.com.vn/khoa-hoc/lo-dien-nhom-hacker-trung-quoc-20140513224345766.htm>.
- 290 “Chinese hack some 750 Vietnamese websites in a week,” *Thanh Niên* (“Youth Newspaper”), September 5, 2014, accessed March 23, 2022, <http://www.thanhniennews.com/tech/chinese-hack-some-750-vietnamese-websites-in-a-week-30791.html>.
- 291 “GOVERNMENT OFFICERS TAKE FOUR DAYS OFF ON INDEPENDENCE DAY VACATION 2014,” Vietnam Visa Immigration, n.d., accessed March 23, 2022, <https://www.vietnam-immigration.org.vn/news/view/government-officers-take-four-days-off-on-independence-day-vacation-2014.html>.
- 292 越南邻国宰相 (“Prime Ministers of Vietnam's Neighboring Countries”), Archive of a defacement of Biex Bitexco Financial Tower website, Zone-h, August 28, 2014, accessed March 23, 2022, <http://zone-h.com/mirror/id/22831164>.
- 293 “Hơn 700 website Việt Nam bị tin tặc Trung Quốc tấn công (“More than 700 Vietnamese websites were attacked by Chinese hackers”),” *Thanh Niên* (“Youth Newspaper”), September 7, 2014, accessed March 23, 2022, <https://thanhnien.vn/hon-700-website-viet-nam-bi-tin-tac-trung-quoc-tan-cong-post380465.html>.
- 294 “Global Hacked Site Statistics,” Global Hacked Site Statistics, accessed September 12, 2016, <http://hack-cn.com/search.php?sel-type=team&var=1937cN>.
- 295 “Global Hacked Site Statistics,” Global Hacked Site Statistics, accessed September 12, 2016, <http://hack-cn.com/search.php?sel-type=team&var=1937cN>.

- 296 越南邻国宰相 ("Prime Minister of Vietnam"), archived defacement of higoozukankou.jp, Zone-H, October 20, 2015, accessed October 3, 2016, [hxxp://www.zone-h.org/mirror/id/24984926](https://www.zone-h.org/mirror/id/24984926).
- 297 Leng Shumei and Bai Yunyi, "Alleged hackers deny Vietnam job," *Global Times*, August 1, 2016, (archived by Internet Archive on January 14, 2017), [hxxps://web.archive.org/web/20170114021007/globaltimes.cn/content/99758.shtml](https://web.archive.org/web/20170114021007/globaltimes.cn/content/99758.shtml).
- 298 Profile page for "中国网军公盟 ("Chinese Hacker Alliance," a.k.a. 1937CNTeam"), QQ, archived August 12, 2015, (archived by Internet Archive on January 14, 2017), [hxxps://t.qq.com/WWW_1937CN_COM](https://web.archive.org/web/20150812210745/hxxps://t.qq.com/WWW_1937CN_COM).
- 299 Matthew Tostevin, "Chinese cyber spies broaden attacks in Vietnam, security firm says," Reuters, August 31, 2017, accessed March 23, 2022, <https://www.reuters.com/article/us-vietnam-china-cyber-chinese-cyber-spies-broaden-attacks-in-vietnam-security-firm-says-idUSKCN1BB0I5>.
- 300 "Viettel on the way to becoming a world leading defense industry group," *People's Army Newspaper*, February 28, 2021, accessed March 23, 2022, <https://en.qdnd.vn/economy/military-businesses/viettel-on-the-way-to-becoming-a-world-leading-defense-industry-group-527325>.
- 301 "Chiến dịch của nhóm APT Trung Quốc Goblin Panda tấn công vào Việt Nam lợi dụng đại dịch Covid-19, ("China's APT Goblin Panda campaign attacks on Vietnam take advantage of Covid-19 pandemic")," Viettel Security, May 1, 2020, accessed March 23, 2022, <https://blog.viettelcybersecurity.com/p/1-chien-dich-cua-nhom-apt-trung-quoc-goblin-panda-tan-cong-vao-viet-nam-loi-dung-dai-dich-COVID-19>.
- 302 "Mã độc tấn công VNA xuất hiện tại nhiều cơ quan, doanh nghiệp ("Malware that attacks VNA appears in many agencies and businesses)," BKav, August 8, 2016, accessed March 23, 2022, <https://www.bkav.com.vn/tin-tuc-noi-bat/-/view-content/139443/ma-o-c-tan-cong-vna-xuat-hien-tai-nhieu-co-quan-doanh-nghiep>.
- 303 Thành Luân, "Nhóm tin tặc 1937CN tấn công Vietnam Airlines là ai? ("Who are the 1937CN hackers who attacked Vietnam Airlines?")," *Thanh Niên* ("Youth Newspaper"), <https://thanhnien.vn/cong-nghe/nhom-tin-tac-1937cn-tan-cong-vietnam-airlines-la-ai-728392.html>.
- 304 CrowdStrike, "CrowdCasts Monthly: You Have an Adversary Problem," Slideshare, October 16, 2013, accessed March 23, 2022, [https://www.slideshare.net/CrowdStrike/crowd-casts-monthly-you-have-an-adversary-problem. \(slide 17\)](https://www.slideshare.net/CrowdStrike/crowd-casts-monthly-you-have-an-adversary-problem. (slide 17))
- 305 "The South China Sea Arbitration (The Republic of Philippines v. The People's Republic of China)," Permanent Court of Arbitration, n.d., accessed March 23, 2022, <https://pca-cpa.org/en/cases/7>.
- 306 "China says U.S. trying to influence Philippines' sea case," Reuters, July 24, 2015, accessed March 23, 2022, <https://www.reuters.com/article/southchinasea-china-usa-idUSL3N1043AM20150724>.
- 307 "Hague Court Agrees to Hear South China Sea Dispute," *Voice of America*, last modified October 20, 2015, accessed March 25, 2022, <https://www.voanews.com/a/hague-court-agrees-to-hear-south-china-sea-dispute/3029324.html. a>.
- 308 "Press Release: The Tribunal Renders Its Award," Permanent Court of Arbitration, July 12, 2016, (archived by Internet Archive on February 22, 2020), <https://web.archive.org/web/20200222004350/https://pca-cpa.org/wp-content/uploads/sites/6/2016/07/PH-CN-20160712-Press-Release-No-11-English.pdf>.
- 309 "Press Release: The Tribunal Renders Its Award," Permanent Court of Arbitration, July 12, 2016, (archived by Internet Archive on February 22, 2020), <https://web.archive.org/web/20200222004350/https://pca-cpa.org/wp-content/uploads/sites/6/2016/07/PH-CN-20160712-Press-Release-No-11-English.pdf>.
- 310 "外交部: 仲裁庭南海裁决无效 中国不接受、不承认 ("Ministry of Foreign Affairs: The South China Sea ruling of the arbitral tribunal is invalid, and China does not accept or recognize it)," 凤凰新媒体 ("Phoenix New Media"), July 12, 2016, (archived by Internet Archive on July 16, 2016), https://web.archive.org/web/20160715034754/https://news.ifeng.com/a/20160712/49340813_0.shtml.
- 311 DK Sta. Ana, "At least 68 govt web sites attacked following UN Arbitral court ruling," InterAksyon, July 15, 2016, (archived by Internet Archive on July 17, 2016), <https://web.archive.org/web/20160717180646/http://interaksyon.com:80/article/130387/at-least-68-govt-web-sites-attacked-following-un-arbitral-court-ruling>.
- 312 DK Sta. Ana, "At least 68 govt web sites attacked following UN Arbitral court ruling," InterAksyon, July 15, 2016, (archived by Internet Archive on July 17, 2016), <https://web.archive.org/web/20160717180646/http://interaksyon.com:80/article/130387/at-least-68-govt-web-sites-attacked-following-un-arbitral-court-ruling>.
- 313 Catalin Ciampu, "Philippines Government Websites Hit by Massive DDoS Attacks, China Suspected," *Softpedia*, July 18, 2016, accessed March 25, 2022, <https://news.softpedia.com/news/philippines-government-websites-hit-by-massive-ddos-attacks-china-suspected-506412.shtml>.
- 314 Ankit Panda (@nktpnd), "PCA website still down after the release of the award..." Twitter, July 12, 2016 10:51 AM, accessed March 25, 2022, <https://twitter.com/nktpnd/status/752878172539121664>.
- 315 "Hague court's website down ahead of arbitration ruling," Inquirer.net, July 12, 2016, accessed March 25, 2022, <https://technology.inquirer.net/49350/hague-courts-website-down-ahead-of-arbitration-ruling>.
- 316 "Website PCA bị sập sau phán quyết Biển Đông ("PCA website crashed after South China Sea ruling)," *Báo Giao Thông* ("Traffic Newspaper"), July 13, 2016, (archived by Internet Archive on July 14, 2016), <https://web.archive.org/web/20160714160205/http://www.baogiaothong.vn/website-pca-bi-sap-sau-phan-quyet-bien-dong-d158534.html>.
- 317 Erlend Leonhardsen (@erlendml), "The websites of the PCA and the ICJ seem to be down..." Twitter, July 12, 2016 10:43 AM, accessed March 25, 2022, <https://twitter.com/erlendml/status/752876003500756993>.
- 318 Laura Zhou, "United Nations stresses separation from Hague tribunal," *South China Morning Post*, last modified July 20, 2016, accessed March 25, 2022, <https://www.scmp.com/news/china/diplomacy-defence/article/1989486/united-nations-stresses-separation-hague-tribunal>.
- 319 Global Times (@globaltimesnews), "Int'l Court of Justice (#ICJ) had "no involvement" in #SouthChinaSea Arbitration..." Twitter, accessed March 25, 2022, <https://twitter.com/globaltimesnews/status/753464128329682944>.
- 320 Catalin Ciampu, "Chinese Hackers Deface Two Philippines Government Websites," *Softpedia*, July 18, 2016 (archived by Internet Archive on July 18, 2016), <https://web.archive.org/web/20160718140211/http://news.softpedia.com/news/chinese-hackers-deface-two-philippines-government-websites-506385.shtml>.
- 321 The Good Geek, "Threat Actor Hunting: Investigation Into The Vietnam Airport Hack," Security G33k, December 4, 2018, accessed March 25, 2022, <http://securityg33k.blogspot.com/2018/12/threat-actor-hunting-investigation-into.html>.
- 322 "Hacker 'AlfabetoVirtual' Sentenced To Prison For Hacking Websites Of The Combating Terrorism Center At West Point And The New York City Comptroller," United States Department of Justice, February 26, 2019, accessed March 25, 2022, <https://www.justice.gov/usao-sdn/pr/hacker-alfabetovirtual-sentenced-prison-hacking-websites-combating-terrorism-center>.

- 323 Anonymous Keygen (@AnonKeyGen), Twitter, last modified March 17, 2014, (archived by Internet Archive on March 25, 2022), <https://web.archive.org/web/20140327220847/https://twitter.com/AnonKeyGen>.
- 324 "Top 7 Deface Pages For Websites," Hacking Zone, April 18, 2015, accessed March 25, 2022, <http://h4ckingzone.blogspot.com/2015/04/top-7-deface-pages-for-websites.html>.
- 325 "China Hacks the Peace Palace: All Your EEZ's Are Belong to Us," ThreatConnect, July 20, 2015, accessed March 25, 2022, <https://threatconnect.com/blog/china-hacks-the-peace-palace-all-your-eezs-are-belong-to-us>.
- 326 "Thêm một chủ khách sạn từ chối khách vì dùng hộ chiếu in 'đường lưỡi bò'" ("Another hotel owner refuses guests for using passports printed with 'cow's tongue line'"), Công an Nhân dân ("The People's Public Security"), July 20, 2016, accessed March 25, 2022, <https://cand.com.vn/doi-song/Khong-cho-thue-tro-vi-dung-ho-chieu-in-duong-luo-bo-i397875>.
- 327 "女子入境越南 护照南海地图处被越南边检写脏话 ("Swear words written by Vietnamese border inspection on South China Sea map in passport of woman entering Vietnam")", 搜狐 ("Sohu"), July 27, 2016, (archived by Internet Archive on August 2, 2016), <https://web.archive.org/web/20160802032422/http://cul.sohu.com/20160727/n461199803.shtml>.
- 328 "Vietnamese customs officer writes 'Fuck You' on Chinese passport, covering up nine-dash line," Shanghaiist, July 27, 2016, (archived by Internet Archive on July 31, 2016), https://web.archive.org/web/20160731184745/shanghaiist.com/2016/07/27/vietnam-customs-fuck_you.php.
- 329 "Chinese Passport Is Scribbled With "F*ck you" by Vietnamese Border Staff," People's Daily, (archived by Internet Archive on July 27, 2015), <https://web.archive.org/web/20160731190044/http://en.people.cn/n3/2016/0727/c90000-9091309.html>.
- 330 "Chinese Passport Is Scribbled With "F*ck you" by Vietnamese Border Staff," People's Daily, (archived by Internet Archive on July 27, 2015), <https://web.archive.org/web/20160731190044/http://en.people.cn/n3/2016/0727/c90000-9091309.html>.
- 331 "Không chứng thực 6.703 hộ chiếu in hình 'đường lưỡi bò' ("6,703 passports printed with 'cow's tongue line' not authenticated")," Phòng Tài chính ("Department of Finance"), July 25, 2016, accessed March 25, 2022, <https://taichinhcuojut.daknong.gov.vn/Cac-linh-vuc-khac/Khong-chung-thuc-6703-ho-chieu-in-hinh-duong-luo-bo-11555.html>.
- 332 Tạ Ban, "Nhiều sao Trung Quốc bị tẩy chay vì phớt lờ phán quyết về 'đường lưỡi bò'" ("Many Chinese stars were boycotted for ignoring the ruling on the 'cow's tongue line'"), Thanh Niên ("Youth Newspaper"), July 13, 2016, accessed March 25, 2022, <https://thanhnien.vn/nhieu-sao-trung-quoc-bi-tay-chay-vi-phot-lo-phan-quyet-ve-duong-luo-bo-post576620.html>.
- 333 VTC TIN MỚI, "Nhận diện nhóm tin tặc tấn công Vietnam Airlines | VTC ("Identify the hacker group that attacked Vietnam Airlines | VTC"), YouTube, July 31, 2016, accessed March 25, 2022, <https://youtu.be/F-nA0gZffaE?t=215>. (timestamp: 3:35).
- 334 Michael Tatarski, "China 1937CN team infiltrate Vietnam Airlines, airports (video)," Asean News Today, August 9, 2016, accessed March 25, 2022, <https://aseannewstoday.com/2016/hack-vietnam-airports-highlights-weaknesses>.
- 335 "Cyber-terrorists attack flight info screens at Vietnam's 2 major airports," VnExpress, July 29, 2016, accessed March 25, 2022, <https://e.vnexpress.net/news/news/cyber-terrorists-attack-flight-info-screens-at-vietnam-s-2-major-airports-3444504.html>.
- 336 The Good Geek, "Threat Actor Hunting: Investigation Into The Vietnam Airport Hack," Security G33k, December 4, 2018, accessed March 25, 2022, <http://securityg33k.blogspot.com/2018/12/threat-actor-hunting-investigation-into.html>.
- 337 Andrew Blake, "Cyberattack claims multiple airports in Vietnam," The Washington Times, July 29, 2016, accessed July 11, 2022, <https://www.washingtontimes.com/news/2016/jul/29/cyberattack-claims-multiple-airports-vietnam-airli/>.
- 338 VTC TIN MỚI, "Nhận diện nhóm tin tặc tấn công Vietnam Airlines | VTC ("Identify the hacker group that attacked Vietnam Airlines | VTC"), YouTube, July 31, 2016, accessed March 25, 2022, <https://www.youtube.com/watch?v=F-nA0gZffaE&t=183s>. (timestamp: 3:03).
- 339 E安全 ("ESecurity"), "中国鹰派黑客组织1937CN Team攻击21座越南机场 ("Hawkish Chinese hacking group 1937CN Team attacked 21 Vietnamese airports"), 77169.com July 30, 2016, accessed September 12, 2016, 77169.com/news/HTML/20160730133423.shtml.
- 340 Michael Tatarski, "China 1937CN team infiltrate Vietnam Airlines, airports (video)," Asean News Today, August 9, 2016, accessed March 25, 2022, <https://aseannewstoday.com/2016/hack-vietnam-airports-highlights-weaknesses>.
- 341 Thanh Thanh Lan, "Vietnamese banks freeze online payments after cyber attacks at 2 major airports," VnExpress, July 31, 2016, accessed March 25, 2022, <https://e.vnexpress.net/news/business/vietnamese-banks-freeze-online-payments-after-cyber-attacks-at-2-major-airports-3445619.html>.
- 342 Pierluigi Paganini, "China 1937CN Team hackers attack airports in Vietnam," Security Affairs, July 31, 2016, accessed September 14, 2016, <https://securityaffairs.co/wordpress/49876/hacking/china-1937cn-team-vietnam.html>.
- 343 Hữu Tình, "Hacker chiếm quyền điều khiển hệ thống thông tin tại sân bay Nội Bài ("Hackers took control of the information system at Noi Bai airport"), Thế Giới Di Động ("Mobile World"), <https://www.thegoididong.com/tin-tuc/hacker-chiem-quyen-dieu-khien-he-thong-thong-tin-tai-noi-bai-866320.html>.
- 344 Juno_okyo, "1937cn tấn công Vietnam Airlines - Nhận định từ các chuyên gia bảo mật ("1937cn attacked Vietnam Airlines - Comments from security experts")," Juno_okyo's Blog, August 2016, accessed March 25, 2022, <https://www.junookyo.com/2016/08/1937cn-hack-vietnam-airlines.html>.
- 345 Thanh Thanh Lan, "Vietnamese banks freeze online payments after cyber attacks at 2 major airports," VnExpress, July 31, 2016, accessed March 25, 2022, <https://e.vnexpress.net/news/business/vietnamese-banks-freeze-online-payments-after-cyber-attacks-at-2-major-airports-3445619.html>.
- 346 "Chinese hacker group denies involvement in Vietnam airport cyber-attack," VnExpress, July 30, 2016, accessed March 25, 2022, <https://e.vnexpress.net/news/news/chinese-hacker-group-denies-involvement-in-vietnam-airport-cyber-attack-3445010.html>.
- 347 Juno_okyo, "1937cn tấn công Vietnam Airlines - Nhận định từ các chuyên gia bảo mật ("1937cn attacked Vietnam Airlines - Comments from security experts")," Juno_okyo's Blog, August 2016, accessed March 25, 2022, <https://www.junookyo.com/2016/08/1937cn-hack-vietnam-airlines.html>.
- 348 Thanh Thanh Lan, "Vietnamese banks freeze online payments after cyber attacks at 2 major airports," VnExpress, July 31, 2016, accessed March 25, 2022, <https://e.vnexpress.net/news/business/vietnamese-banks-freeze-online-payments-after-cyber-attacks-at-2-major-airports-3445619.html>.
- 349 "Cảnh giác với các thủ đoạn của tin tặc tấn công mạng có chủ đích ("Beware of the tricks of hackers intentionally attacking public networks"), Sở Thông Tin và Truyền Thông ("Department of Information and Communication"), October 19, 2017, accessed December 13, 2021, <https://sttt.quangbinh.gov.vn/ca-ES/chi-tiet-tin/-/view-article/1/1457686409799/1505453021018>.

- 350 "Mã độc tấn công có chủ đích APT ("Target APT Attack with Malware")," Cục Công Nghệ Thông Tin Và Dữ Liệu Tài Nguyên Môi Trường ("Department of Information Technology at the Ministry of Natural Resources and Environment") , September 7, 2017, accessed March 25, 2025, <http://dinte.gov.vn/SitePages/BanTin.aspx/2112>.
- 351 "Mã độc tấn công VNA xuất hiện tại nhiều cơ quan, doanh nghiệp (Malware that attacks VNA appears in many agencies and businesses)," *Bkav*, August 8, 2016, accessed March 25, 2022, <https://www.bkav.com.vn/tin-tuc-noi-bat/-/view-content/400028/trang-tin-tuc>.
- 352 Mã độc tin tặc tấn công Vietnam Airlines có tại nhiều cơ quan ("The malicious code that attacked Vietnam Airlines is present in many agencies"), *Báo Người Lao Động* ("The Labor Newspaper"), August 8, 2016, accessed March 25, 2022, <https://nld.com.vn/thoi-su-trong-nuoc/ma-doc-tin-tac-tan-cong-vietnam-airlines-co-tai-nhieu-co-quan-20160808161659607.htm>.
- 353 "Cảnh giác với các thủ đoạn của tin tặc tấn công mạng có chủ đích ("Beware of the tricks of hackers intentionally attacking public networks"), *Sở Thông Tin và Truyền Thông* ("Department of Information and Communication"), October 19, 2017, accessed December 13, 2021, <https://sttt.quangbinh.gov.vn/ca-ES/chi-tiet-tin/-/view-article/1/1457686409799/1505453021018>.
- 354 "Mã độc tấn công VNA xuất hiện tại nhiều cơ quan, doanh nghiệp (Malware that attacks VNA appears in many agencies and businesses)," *Bkav*, August 8, 2016, accessed March 25, 2022, <https://www.bkav.com.vn/tin-tuc-noi-bat/-/view-content/400028/trang-tin-tuc>.
- 355 "Mã độc tin tặc tấn công Vietnam Airlines có tại nhiều cơ quan ("The malicious code that attacked Vietnam Airlines is present in many agencies"), *Báo Người Lao Động* ("The Labor Newspaper"), August 8, 2016, accessed March 25, 2022, <https://nld.com.vn/thoi-su-trong-nuoc/ma-doc-tin-tac-tan-cong-vietnam-airlines-co-tai-nhieu-co-quan-20160808161659607.htm>.
- 356 "CrowdStrike Global Threat Intel Report," CrowdStrike, 2014, accessed March 25, 2022, https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2015/GlobalThreatIntelReport.pdf.
- 357 "Alleged hackers deny Vietnam job," *Global Times*, August 1, 2016, (archived by Internet Archive on August 2, 2016), <https://web.archive.org/web/20160802182930/http://english.sina.com/china/s/2016-08-01/detail-ifxunyya2915888.shtml>.
- 358 "Global Hacked Site Statistics," Global Hacked Site Statistics, accessed September 12, 2016, <http://hack-cn.com/search.php?sel-type=team&var=1937cN>.
- 359 越南邻国宰相defacement notifications, Zone-H, last modified December 28, 2015 accessed March 25, 2022, <https://zone-h.com/archive/notifier=%25E8%25B6%258A%25E5%258D%2597%25E9%2582%25BB%25E5%259B%25BD%25E5%25AE%25B0%25E7%259B%25B8>. All of the defacements with listed dates on this page more recent than December 29, 2015 were initially saved by Zone-H on or before that date. The reason for the discrepancy is unclear.
- 360 "或许我们本就不该出现在虚拟又现实网络里 ("Maybe we shouldn't have been on real and virtual networks...")", 1937CN, n.d. (archived by Internet Archive on October 23, 2016), <https://web.archive.org/web/20161023225047/http://www.1937cn.com/>.
- 361 "Statement on Vietnam Airport Hacked by Chinese," 1937CN, July 41, 2016, (archived by Internet Archive on July 31, 2016), <https://web.archive.org/web/20160731222250/http://www.1937cn.net>.
- 362 Weixing Hu and Weizhan Meng. "The US Indo-Pacific Strategy and China's Response." *China Review* 20, no. 3 (2020): 143–76. <https://www.jstor.org/stable/26928115>. (p. 158–159)
- 363 "GDP Forecast by Country | Statistics from IMF | 2021-2025," Knoema, n.d., accessed March 25, 2022, <https://knoema.com/tbocwag/gdp-forecast-by-country-statistics-from-imf-2021-2025>.
- 364 "Indo-Pacific should shun new Cold War: *China Daily* editorial," *China Daily*, last modified March 13, 2021, accessed March 25, 2021, <http://global.chinadaily.com.cn/a/202103/14/WS604dedf7a31024ad-Obaaf092.html>.
- 365 "Quad mechanism turning into 'sinister gang of Indo-Pacific': *Global Times* editorial," *Global Times*, September 23, 2021, accessed March 25, 2022, <https://www.globaltimes.cn/page/202109/1234988.shtml>.
- 366 "Clinton Inks China Trade Bill," CBS News, September 19, 2000, accessed March 25, 2022, <https://www.cbsnews.com/news/clinton-inks-china-trade-bill>.
- 367 The National Security Strategy of the United States of America, The President of the United States, March 2006, (archived by Internet Archive on May 29, 2009), <https://web.archive.org/web/20090529235009/http://georgewbush-whitehouse.archives.gov:80/nsc/nss/2006/nss2006.pdf>.
- 368 Stephen Walt, "How 9/11 Will Be Remembered a Century Later," *Foreign Policy*, September 6, 2021, accessed March 25, 2022, <https://foreignpolicy.com/2021/09/06/how-9-11-will-be-remembered-a-century-later>.
- 369 Steward Patrick, "The U.S. Obsession With Failed States After 9/11 Was a Costly Distraction," *World Politics Review*, September 13, 2021, accessed March 23, 2022, <https://www.worldpoliticsreview.com/articles/29953/the-attacks-of-9-11-and-the-failed-state-distraction>.
- 370 Jaques deLisle, "9/11 and U.S.-China Relations," *Foreign Policy* Research Institute, September 3, 2011, accessed March 25, 2011, <https://www.fpri.org/article/2011/09/911-and-u-s-china-relations>.
- 371 Hillary Clinton, "America's Pacific Century," *Foreign Policy*, October 11, 2011, accessed March 25, 2022, <https://foreignpolicy.com/2011/10/11/americas-pacific-century>.
- 372 Barack Obama, "Remarks By President Obama to the Australian Parliament," The White House, November 17, 2011, accessed March 25, 2022, <https://obamawhitehouse.archives.gov/the-press-office/2011/11/17/remarks-president-obama-australian-parliament>.
- 373 Jackie Calms, "A U.S. Marine Base for Australia Irritates China," *The New York Times*, November 16, 2011, accessed March 25, 2022, <https://www.nytimes.com/2011/11/17/world/asia/obama-and-gillard-expand-us-australia-military-ties.html>.
- 374 "Tension grows as US 'Back in Asia,'" *Xinhua*, November 22, 2011, accessed March 25, 2022, (archived by Internet Archive on December 31, 2011), https://web.archive.org/web/20111231105241/http://news.xinhuanet.com/english2010/video/2011-11/22/c_131261603.htm.
- 375 Jackie Calms, "A U.S. Marine Base for Australia Irritates China," *The New York Times*, November 16, 2011, accessed March 25, 2022, <https://www.nytimes.com/2011/11/17/world/asia/obama-and-gillard-expand-us-australia-military-ties.html>.
- 376 "Alert (AA21-201A): Chinese Gas Pipeline Intrusion Campaign, 2011 to 2013," Cybersecurity and Infrastructure Security Agency, last modified July 21, 2021, accessed March 25, 2022, <https://us-cert.cisa.gov/ncas/alerts/aa21-201a>.
- 377 "Alert (AA21-201A): Chinese Gas Pipeline Intrusion Campaign, 2011 to 2013," Cybersecurity and Infrastructure Security Agency, last modified July 21, 2021, accessed March 25, 2022, <https://us-cert.cisa.gov/ncas/alerts/aa21-201a>.
- 378 "Alert (AA21-201A): Chinese Gas Pipeline Intrusion Campaign, 2011 to 2013," Cybersecurity and Infrastructure Security Agency, last modified July 21, 2021, accessed March 25, 2022, <https://us-cert.cisa.gov/ncas/alerts/aa21-201a>.
- 379 David E. Sanger, David Barboza and Nicole Perlroth, "Chinese Army Unit Is Seen as Tied to Hacking Against U.S.," *The New York Times*, February 18, 2013, accessed March 25, 2022, <https://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html>.

- 380 Brian Krebs, "Chinese Hackers Blamed for Intrusion at Energy Industry Giant Telvent," *Krebs on Security*, September 26, 2012, accessed March 25, 2022, <https://krebsonsecurity.com/2012/09/chinese-hackers-blamed-for-intrusion-at-energy-industry-giant-telvent>.
- 381 "OASyS SCADA," Telvent, n.d., accessed March 22, 2022, (archived by Internet Archive on October 7, 2012), https://web.archive.org/web/20121007114805/http://www.telvent.com/en/business_areas/smart_grid/solutions_overview/smart_grid/smart_operations/oasys-scada.cfm.
- 382 Jaikumar Vijayan, "Energy giant confirms breach of customer project files," *ComputerWorld*, September 26, 2012, accessed April 14, 2022, <https://www.computerworld.com/article/2491671/energy-giant-confirms-breach-of-customer-project-files.html>.
- 383 "Alert (AA21-201A): Chinese Gas Pipeline Intrusion Campaign, 2011 to 2013," Cybersecurity and Infrastructure Security Agency, last modified July 21, 2021, accessed March 25, 2022, <https://us-cert.cisa.gov/ncas/alerts/aa21-201a>.
- 384 "Alert (AA21-201A): Chinese Gas Pipeline Intrusion Campaign, 2011 to 2013," Cybersecurity and Infrastructure Security Agency, last modified July 21, 2021, accessed March 25, 2022, <https://us-cert.cisa.gov/ncas/alerts/aa21-201a>.
- 385 David E. Sanger, David Barboza and Nicole Perlroth, "Chinese Army Unit Is Seen as Tied to Hacking Against U.S.," *The New York Times*, February 18, 2013, accessed March 25, 2022, <https://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html>.
- 386 David E. Sanger, David Barboza and Nicole Perlroth, "Chinese Army Unit Is Seen as Tied to Hacking Against U.S.," *The New York Times*, February 18, 2013, accessed March 25, 2022, <https://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html>.
- 387 John Costello, "The Strategic Support Force: Update and Overview," China Brief Volume: 16 Issue: 19, The Jamestown Foundation, December 21, 2016, accessed March 25, 2022, <https://jamestown.org/program/strategic-support-force-update-overview>.
- 388 Jamie Keene, "NSA Director blames China for a 'great deal' of military-related data theft," *The Verge*, March 28, 2012, accessed March 25, 2022, <https://www.theverge.com/2012/3/28/2907930/nsa-keith-alexander-china-military-data-theft>.
- 389 Kevin Poulsen, "Second Defense Contractor L-3 'Actively Targeted' With RSA SecurID Hacks," *Wired*, May 31, 2011, accessed April 14, 2022, <https://www.wired.com/2011/05/l-3/>.
- 390 Mark Clayton, "Exclusive: potential China link to cyberattacks on gas pipeline companies," *Christian Science Monitor*, May 10, 2012, accessed March 25, 2022, <https://www.csmonitor.com/USA/2012/0510/Exclusive-potential-China-link-to-cyberattacks-on-gas-pipeline-companies>.
- 391 Tom Espiner, "RSA: Nation state double-teamed on SecurID attack," ZDNet, October 11, 2011, (archived by Internet Archive on November 13, 2011), <https://web.archive.org/web/20111113064824/http://www.zdnet.co.uk/news/security-threats/2011/10/11/rsa-nation-state-double-teamed-on-securid-attack-40094162>.
- 392 "APT17 is run by the Jinan bureau of the Chinese Ministry of State Security," *Intrusion Truth*, July 24, 2019, accessed March 25, 2022, <https://intrusiontruth.wordpress.com/2019/07/24/apt17-is-run-by-the-jinan-bureau-of-the-chinese-ministry-of-state-security>.
- 393 Based on statements by CrowdStrike and the FBI, APT17 is the probably same group as Sneaky Panda. In an interview, CrowdStrike co-founder Dmitri Alperovitch stated that his company tracked the group known elsewhere as "Beijing Group" or "Elderwood Gang" as "Sneaky Panda." [[Mark Clayton, "Stealing US business secrets: Experts ID two huge cyber 'gangs' in China" The Christian Science Monitor, September 14, 2012, accessed March 25, 2015, [https://www.csmonitor.com/USA/2012/0914/Stealing-US-business-secrets-Experts-ID-two-huge-cyber-gangs-in-China.\] The FBI reportedly determined that APT17 is another name for the group responsible for Operation Aurora, which has been previously attributed to Elderwood Gang and Beijing Group. \[\[Bell Gertz, "New Chinese Intelligence Unit Linked to Massive Cyber Spying Program," Washington Free Beacon, October 31, 2014, accessed March 25, 2022, \[https://freebeacon.com/national-security/new-chinese-intelligence-unit-linked-to-massive-cyber-spying-program.\\]\\]\]\(https://freebeacon.com/national-security/new-chinese-intelligence-unit-linked-to-massive-cyber-spying-program.\)](https://www.csmonitor.com/USA/2012/0914/Stealing-US-business-secrets-Experts-ID-two-huge-cyber-gangs-in-China.)
- 394 "Compromise of RSA SecurID tokens," Council on Foreign Relations, n.d., accessed March 25, 2022, <https://www.cfr.org/cyber-operations/compromise-rsa-secureid-tokens>.
- 395 Visi (@invisig0th), "Since everybody's talking about the RSA breach now..." Twitter, May 24, 2021 7:28 AM, accessed March 25, 2022, <https://twitter.com/invisig0th/status/1396835545465110534>.
- 396 Tom Espiner, "RSA: Nation state double-teamed on SecurID attack," ZDNet, October 11, 2011, accessed March 24, 2022, (archived by Internet Archive on November 13, 2011), <https://web.archive.org/web/20111113064824/http://www.zdnet.co.uk/news/security-threats/2011/10/11/rsa-nation-state-double-teamed-on-securid-attack-40094162>.
- 397 "Global Energy Cyberattacks: 'Night Dragon,'" McAfee, February 10, 2011, accessed March 25, 2022, (archived by Internet Archive on February 18, 2011), <https://web.archive.org/web/20110218091458/http://www.mcafee.com/us/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf>. (p. 7)
- 398 "APT1: Exposing One of China's Cyber Espionage Units," Mandiant, 2013, accessed March 25, 2022, <https://www.mandiant.com/sites/default/files/2021-09/mandiant-apt1-report.pdf>.
- 399 "An Interactive Look at the U.S.-China Military Scorecard," Rand: Project Air Force, n.d., accessed March 25, 2022, <https://www.rand.org/paf/projects/us-china-scorecard.html>.
- 400 "ANNUAL REPORT TO CONGRESS Military and Security Developments Involving the People's Republic of China 2013," Office of the Secretary of Defense, 2013, accessed March 25, 2022, https://dod.defense.gov/Portals/1/Documents/pubs/2013_China_Report_FINAL.pdf. (p. 38)
- 401 Evan Braden Montgomery, "Time to Worry about China's Military Rise," *International Security*, Belfer Center at the Harvard Kennedy School, June 2014, accessed March 28, 2022, <https://www.belfercenter.org/publication/time-worry-about-chinas-military-rise>.
- 402 Sydney J. Freedberg Jr., "Chinese Scarborough Shoal Base Would Threaten Manila," *Breaking Defense*, April 28, 2016, accessed March 28, 2022, <https://breakingdefense.com/2016/04/chinese-scarborough-shoal-base-would-threaten-manila>.
- 403 Javier C. Hernández, "China Suspends Diplomatic Contact With Taiwan," *The New York Times*, June 25, 2016, accessed March 28, 2022, <https://www.nytimes.com/2016/06/26/world/asia/china-suspends-diplomatic-contact-with-taiwan.html>.
- 404 Lily Kuo, "Taiwan election: Tsai Ing-Wen wins landslide in rebuke to China," *The Guardian*, January 11, 2020, accessed March 28, 2022, <https://www.theguardian.com/world/2020/jan/11/taiwan-re-elects-tsai-ing-wen-as-president-in-clear-message-to-china>.
- 405 "No shaking Taiwan from the motherland," *China Daily*, last modified January 16, 2020, accessed March 28, 2022, https://www.chinadaily.com.cn/newsrepublic/2020-01/16/content_37532559.htm.

- 406 "China firmly protects its territorial integrity, opposes Taiwan independence," *The Straits Times*, January 12, 2020, accessed March 28, 2022, <https://www.straitstimes.com/asia/east-asia/china-firmly-protects-its-territorial-integrity-opposes-taiwan-independence>.
- 407 Tsai Ing-wei, "Inaugural address of ROC 15th-term President Tsai Ing-wen," Office of the President of the Republic of China (Taiwan), May 20, 2020, accessed March 28, 2022, <https://english.president.gov.tw/News/6004>.
- 408 "駭客恐將再攻擊10企業 調查局：立即檢查防護機制 ("Hackers are about to attack 10 companies. Bureau of Investigation: Check your protection mechanisms now."), " *Epoch Times*, last modified May 15, 2020, accessed March 28, 2022, <https://www.epochtimes.com/b5/20/5/15/n12111916.htm>.
- 409 "國內重要企業遭勒索軟體攻擊事件調查說明 ("Description of the investigation into the ransomware attack on important domestic companies"), " Ministry of Justice, last modified May 15, 2020, accessed March 28, 2022, <https://www.mjib.gov.tw/news/Details/1/607>.
- 410 "駭進中油、台塑的海外華裔駭客，還鎖定台灣另十公司 ("Overseas Chinese hackers who hacked into CNPC and Formosa Plastics also targeted ten other companies in Taiwan"), " Inside, May 18, 2020, accessed March 28, 2022, <https://www.inside.com.tw/article/19816-chinese-hacker-Winnti-Group-hacked-CPC-FPC>.
- 411 "事件通告：加密勒索軟體猖獗，請加強系統/應用程式更新與資料備份作業 ("Event Notice: Encryption ransomware is rampant. Please strengthen systems, update applications, and conduct data backup operations")", HiNet, May 6, 2020, (archived by Internet Archive on November 18, 2021), https://web.archive.org/web/20211118103050/https://hisecure.hinet.net/secureinfo/popup.php?cert_id=HiNet-2020-0046.
- 412 "Bureau names ransomware culprits," *Taipei Times*, May 17, 2020, accessed March 28, 2020, <https://www.taipeitimes.com/News/taiwan/archives/2020/05/17/2003736564>.
- 413 "Targeted Ransomware Attacks in Taiwan," Cyberint, May 14, 2020, accessed March 28, 2022, <https://blog.cyberint.com/targeted-ransomware-attacks-in-taiwan>.
- 414 陳于晴 ("Chen Yuqing"), "調查局：中油、台塑化遭海外駭客集團勒索攻擊 另有10家遭鎖定, ("Investigation Bureau: CNPC and Formosa Plastics were blackmailed by overseas hacker groups, and 10 others were locked"), " *Anue*, May 15, 2020, accessed March 28, 2022, <https://news.cnyes.com/news/id/4478375>.
- 415 "China-Linked Threat Group Targets Taiwan Critical Infrastructure, Smokescreen Ransomware," Cycraft, 2021, accessed June 7, 2021, https://www.cycraft.com/resources/report/CyCraft_Technology_Critical_Infrastructure_Threat_Report.pdf.
- 416 "U.S. Justice Department Charges APT41 Hackers over Global Cyberattacks," Trend Micro, September 18, 2020, accessed March 28, 2022, https://www.trendmicro.com/en_us/research/20/i/u-s-justice-department-charges-apt41-hackers-over-global-cyberattacks.html.
- 417 "China-Linked Threat Group Targets Taiwan Critical Infrastructure, Smokescreen Ransomware," Cycraft, 2021, accessed June 7, 2021, https://www.cycraft.com/resources/report/CyCraft_Technology_Critical_Infrastructure_Threat_Report.pdf.
- 418 Matthew Strong, "Taiwan's Formosa Petrochemical gas stations hit by malware attack," *Taiwan News*, May 5, 2020, accessed March 28, 2022, <https://www.taiwannews.com.tw/en/news/3928508>.
- 419 "Taiwan's CPC suffers malware attack, experiences system outage," *Taiwan News*, May 4, 2020, accessed March 28, 2022, <https://www.taiwannews.com.tw/en/news/3927869>.
- 420 United States of America vs. Jiang Lizhi, Qian Chuan, and Fu Qiang, Case: 1:20-cr-00158, U.S. District Court for the District of Columbia, August 11, 2020, accessed March 28, 2022, <https://www.justice.gov/opa/press-release/file/1317206/download>. (p. 23)
- 421 "國內重要企業遭勒索軟體攻擊事件調查說明 ("Description of the investigation into the ransomware attack on important domestic companies"), " Ministry of Justice, last modified May 15, 2020, accessed March 28, 2022, <https://www.mjib.gov.tw/news/Details/1/607>.
- 422 United States of America vs. Jiang Lizhi, Qian Chuan, and Fu Qiang, Case: 1:20-cr-00158, U.S. District Court for the District of Columbia, August 11, 2020, accessed March 28, 2022, <https://www.justice.gov/opa/press-release/file/1317206/download>. (p. 23)
- 423 "The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China," The White House, July 19, 2021, accessed March 28, 2022, <https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/19/the-unit-ed-states-joined-by-allies-and-partners-attributes-malicious-cyber-activity-and-irresponsible-state-behavior-to-the-peoples-republic-of-china>.
- 424 United States of America vs. Jiang Lizhi, Qian Chuan, and Fu Qiang, Case: 1:20-cr-00158, U.S. District Court for the District of Columbia, August 11, 2020, accessed March 28, 2022, <https://www.justice.gov/opa/press-release/file/1317206/download>. (p. 3, 6)
- 425 United States of America vs. Jiang Lizhi, Qian Chuan, and Fu Qiang, Case: 1:20-cr-00158, U.S. District Court for the District of Columbia, August 11, 2020, accessed March 28, 2022, <https://www.justice.gov/opa/press-release/file/1317206/download>.
- 426 United States of America vs. Jiang Lizhi, Qian Chuan, and Fu Qiang, Case: 1:20-cr-00158, U.S. District Court for the District of Columbia, August 11, 2020, accessed March 28, 2022, <https://www.justice.gov/opa/press-release/file/1317206/download>.
- 427 Adam Meyers, "Meet CrowdStrike's Adversary of the Month for July: WICKED SPIDER," CrowdStrike, July 26, 2018, accessed March 28, 2022, <https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-july-wicked-spider>.
- 428 Marc-Etienne M. Léveillé, "Gaming industry still in the scope of attackers in Asia," WeLiveSecurity by ESET, March 11, 2019, accessed March 28, 2028, <https://www.welivesecurity.com/2019/03/11/gaming-industry-scope-attackers-asia>.
- 429 "Cyber Threats 2020: A Year in Retrospect," PwC, 2021., accessed March 28, 2022, <https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf>.
- 430 "Digitally Signed Malware Targeting Gaming Companies," BlackBerry, October 18, 2016, accessed March 28, 2022, <https://blogs.blackberry.com/en/2016/10/digitally-signed-malware-targeting-gaming-companies>.
- 431 "Winnti. More than just a game," Securelist by Kaspersky, April 11, 2013, accessed March 28, 2022, <https://securelist.com/winnti-more-than-just-a-game/37029>.
- 432 Austin Ramzy, "China Sends Warplanes to Taiwan Strait in a Show of Force to Biden," *The New York Times*, January 24, 2021, accessed March 28, 2022, <https://www.nytimes.com/2021/01/24/world/asia/china-taiwan-strait-exercise-biden.html>.
- 433 Pratik Jakhar, "India and China race to build along a disputed frontier," BBC, July 30, 2020, accessed March 28, 2022, <https://www.bbc.com/news/world-asia-53171124>.
- 434 Saif Khalid, "'All-out combat' feared as India, China engage in border standoff," Al Jazeera, May 28, 2020, accessed March 28, 2022, <https://www.aljazeera.com/news/2020/5/28/all-out-combat-feared-as-india-china-engage-in-border-standoff>.

- 435 Sushant Singh, "India-China conflict in Ladakh: What is the importance of Pangong Tso lake?" *The Indian Express*, May 20, 2020, accessed March 28, 2022, <https://indianexpress.com/article/explained/india-china-conflict-in-ladakh-the-importance-of-the-pangong-tso-lake-6419377>.
- 436 Soutik Biswas, "India-China clash: An extraordinary escalation 'with rocks and clubs,'" BBC, June 16, 2020, accessed March 28, 2022, <https://www.bbc.com/news/world-asia-india-53071913>.
- 437 "India-China dispute: The border row explained in 400 words," BBC, January 25, 2021, accessed March 28, 2022 <https://www.bbc.com/news/world-asia-53062484>.
- 438 Rahul Shrivastava, "Indian soldiers thrash, push back Chinese soldiers at Naku La in Sikkim; Army issues statement," *India Today*, last modified January 25, 2021, accessed March 28, 2022, <https://www.indiatoday.in/india/story/india-china-attempt-change-status-quo-lac-pla-soldiers-injured-nathu-la-indian-1762412-2021-01-25>.
- 439 Devyot Ghoshal and Gabriel Crossley, "India, China trade blame for break down in border talks," Reuters, October 11, 2021, accessed March 28, 2022, <https://www.reuters.com/world/india/india-china-trade-blame-break-down-border-talks-2021-10-11>.
- 440 Thomas Kika, "China Sends Bomber Planes to Indian Border in 'Warning' to Country," *Newsweek*, November 15, 2021, accessed March 28, 2022, <https://www.newsweek.com/china-sends-bomber-planes-indian-border-warning-country-1649746>.
- 441 "China-Linked Group RedEcho Targets the Indian Power Sector Amid Heightened Border Tensions," Recorded Future, 2021, accessed March 28, 2022, <https://go.recordedfuture.com/hubfs/reports/cta-2021-0228.pdf>.
- 442 Catalin Cimpanu, "RedEcho group parks domains after public exposure," The Record by Recorded Future, March 29, 2021, accessed March 28, 2022, <https://therecord.media/redecho-group-parks-domains-after-public-exposure>.
- 443 "China-Linked Group RedEcho Targets the Indian Power Sector Amid Heightened Border Tensions," Recorded Future, 2021, accessed March 28, 2022, <https://go.recordedfuture.com/hubfs/reports/cta-2021-0228.pdf>. (p. 6-7)
- 444 Sumit Kumar Singh, "India thwarted China's cyber attacks on power sector," *The Siasat Daily*, March 1, 2021, accessed March 28, 2022, <https://www.siasat.com/india-thwarted-chinas-cyber-attacks-on-power-sector-2100833>.
- 445 Abhinandan Mishra, "'Cyber incident' affected Mumbai power supply," *The Sunday Guardian Live*, last modified April 3, 2021, accessed March 28, 2022, <https://www.sundayguardianlive.com/news/cyber-incident-affected-mumbai-power-supply>.
- 446 "It was human error": Cyberattacks took place but didn't cause Mumbai power outage, says govt," *Times of India*, last modified March 2, 2021, accessed March 28, 2022, <https://timesofindia.indiatimes.com/india/2020-mumbai-power-outage-caused-by-human-error-not-cyber-attack-union-power-minister/article-show/81292545.cms>.
- 447 "Human error caused Mumbai power outage, not cyberattack: Union Power Minister RK Singh," *India Today*, last modified March 2, 2021, accessed March 28, 2022, <https://www.indiatoday.in/india/story/human-error-caused-mumbai-power-outage-not-cyberattack-union-power-minister-rk-singh-1774843-2021-03-02>.
- 448 "Mumbai blackout no cyber attack, but 'human error': Singh," *Indian Express*, last modified March 3, 2021, accessed March 28, 2022, <https://indianexpress.com/article/india/mumbai-blackout-no-cyber-attack-but-human-error-singh-7211789>.
- 449 "Cyberattacks took place, but human error caused Mumbai power outage: Centre," *Business Standard*, last modified March 2, 2021, accessed March 28, 2022, https://www.business-standard.com/article/current-affairs/cyberattacks-took-place-but-human-error-caused-mumbai-power-outage-centre-121030200955_1.html.
- 450 "Human error caused Mumbai power outage, not cyberattack: Union Power Minister RK Singh," *India Today*, last modified March 2, 2021, accessed March 28, 2022, <https://www.indiatoday.in/india/story/human-error-caused-mumbai-power-outage-not-cyberattack-union-power-minister-rk-singh-1774843-2021-03-02>.
- 451 "Mumbai blackout no cyber attack, but 'human error': Singh," *Indian Express*, last modified March 3, 2021, accessed March 28, 2022, <https://indianexpress.com/article/india/mumbai-blackout-no-cyber-attack-but-human-error-singh-7211789>.
- 452 "Cyberattacks took place, but human error caused Mumbai power outage: Centre," *Business Standard*, last modified March 2, 2021, accessed March 28, 2022, https://www.business-standard.com/article/current-affairs/cyberattacks-took-place-but-human-error-caused-mumbai-power-outage-centre-121030200955_1.html.
- 453 "Human error caused Mumbai power outage, not cyberattack: Union Power Minister RK Singh," *India Today*, last modified March 2, 2021, accessed March 28, 2022, <https://www.indiatoday.in/india/story/human-error-caused-mumbai-power-outage-not-cyberattack-union-power-minister-rk-singh-1774843-2021-03-02>.
- 454 "Continued Targeting of Indian Power Grid Assets by Chinese State-Sponsored Activity Group," Recorded Future, April 6, 2022, accessed April 15, 2022, <https://go.recordedfuture.com/hubfs/reports/ta-2022-0406.pdf>.
- 455 ICS/OT CYBERSECURITY YEAR IN REVIEW 2021, Dragos, 2022, accessed April 15, 2022, <https://hub.dragos.com/hubfs/333%20Year%20In%20Review/2021/2021%20ICS%20OT%20Cybersecurity%20Year%20In%20Review%20-%20Dragos%202021.pdf?hsLang=en>.
- 456 ICS/OT CYBERSECURITY YEAR IN REVIEW 2021, Dragos, 2022, accessed April 15, 2022, <https://hub.dragos.com/hubfs/333%20Year%20In%20Review/2021/2021%20ICS%20OT%20Cybersecurity%20Year%20In%20Review%20-%20Dragos%202021.pdf?hsLang=en>.
- 457 "Continued Targeting of Indian Power Grid Assets by Chinese State-Sponsored Activity Group," Recorded Future, April 6, 2022, accessed April 15, 2022, <https://go.recordedfuture.com/hubfs/reports/ta-2022-0406.pdf>.
- 458 Sahil Joshi and Divyesh Singh, "Mega Mumbai power outage may be result of cyber attack, final report awaited," *India Today*, November 20, 2020, accessed March 28, 2022, <https://www.indiatoday.in/india/story/mumbai-power-outage-malware-attack-1742538-2020-11-20>.
- 459 Kevin McCauley, "Snapshot: China's Western Theater Command," China Brief, Volume: 17 Issue: 1, The Jamestown Foundation, January 13, 2017, accessed March 28, 2022, <https://jamestown.org/program/snapshot-chinas-western-theater-command>.
- 460 UNITED STATES OF AMERICA CRIMINAL v. JIANG LIZHI, QIAN CHUAN, and FU QIANG, United States District Court for The District of Columbia, August 11, 2020, accessed March 17, 2022, <https://www.justice.gov/opa/press-release/file/1317206/download>. (p. 3, 6).
- 461 "China-Linked Group RedEcho Targets the Indian Power Sector Amid Heightened Border Tensions," Recorded Future, 2021, accessed March 28, 2022, <https://go.recordedfuture.com/hubfs/reports/cta-2021-0228.pdf>.
- 462 "China-Linked Group RedEcho Targets the Indian Power Sector Amid Heightened Border Tensions," Recorded Future, 2021, accessed March 28, 2022, <https://go.recordedfuture.com/hubfs/reports/cta-2021-0228.pdf>.

- 463 "Continued Targeting of Indian Power Grid Assets by Chinese State-Sponsored Activity Group," Recorded Future, April 6, 2022, accessed April 15, 2022, <https://go.recordedfuture.com/hubfs/reports/ta-2022-0406.pdf>.
- 464 Snigdha, "Chinese Hackers Made Two Attempts To Target Electricity Division Centres Near Ladakh But Not Successful: Govt," India.com, last modified April 7, 2022, accessed May 30, 2022, <https://www.india.com/news/india/chinese-hackers-target-electricity-division-centres-power-grid-ladakh-not-successful-govt-statement-centre-india-5325082/>.
- 465 Mark A. Stokes, "The Chinese People's Liberation Army Computer Network Operations Infrastructure" in China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain, Oxford University Press, 2015, https://www.google.com/books/edition/China_and_Cybersecurity/wQN1BgAAQBAJ?hl=en&gbpv=1&dq=%22neutralizing+single+points+of+failure+in+a+foreign+adversary%27s+critical+infrastructure%22&pg=PA175&printsec=frontcover. (p. 175)
- 466 Ben Buchanan and Fiona S. Cunningham, "Preparing the Cyber Battlefield: Assessing a Novel Escalation Risk in a Sino-American Crisis," Texas National Security Review, Volume 3, Issue 4, Fall 2020, accessed March 28, 2022, <https://tnsr.org/wp-content/uploads/2020/10/TNSR-Vol3-Iss4-Buchanan-and-Cunningham.pdf>. (p. 74)
- 467 "Science of Military Strategy," China's Academy of Military Sciences, 2013, (translated by the China Aerospace Studies Institute), https://www.airuniversity.af.edu/Portals/10/CASI/documents/Translations/2021-02-08%20Chinese%20Military%20Thoughts%20In%20their%20own%20words%20Science%20of%20Military%20Strategy%202013.pdf?ver=NxAWg4BPw_NylEjxaha8Aw%3d%3d. (p.156)
- 468 "China's Military Strategy," The State Council Information Office of the People's Republic of China, May 2015, Beijing, (republished by China Military, June 23, 2021), http://english.chinamil.com.cn/view/2021-06/23/content_10053010.htm.
- 469 "China's National Defense in the New Era," The State Council Information Office of the People's Republic of China, July 2019, (republished by the China Aerospace Studies Institute, 2019), <https://www.airuniversity.af.edu/Portals/10/CASI/documents/Translations/2019-07%20PRC%20White%20Paper%20on%20National%20Defense%20in%20the%20New%20Era.pdf?ver=akpbGkO5ogbDPPbfQkb5A%3d%3d>.
- 470 "China aims to become world-leading cyber power by 2035," The State Council of the People's Republic of China, last modified December 25, 2017, accessed March 28, 2022, http://english.www.gov.cn/state_council/ministries/2017/12/25/content_281475989525696.htm.
- 471 Military and Security Developments Involving the People's Republic of China 2021: Annual Report to Congress, Office of the Secretary of Defense, 2021, accessed March 28, 2022, <https://media.defense.gov/2021/Nov/03/2002885874/-1/-1/0/2021-CMPR-FINAL.PDF>. (p. 79)
- 472 Ned Moran, Joshua Homan, and Mike Scott, "Operation Poisond Hurricane," FireEye, August 6, 2014, accessed March 28, 2022, <https://www.fireeye.com/blog/threat-research/2014/08/operation-poisoned-hurricane.html>.
- 473 Ned Moran, Mike Oppenheim, and Mike Scott, "Operation Poisoned Handover: Unveiling Ties Between APT Activity in Hong Kong's Pro-Democracy Movement," FireEye, November 3, 2014, (archived by Internet Archive on March 31, 2015), <https://www.fireeye.com/blog/threat-research/2014/11/operation-poisoned-handover-unveiling-ties-between-apt-activity-in-hong-kongs-pro-democracy-movement.html>.
- 474 Ned Moran, Joshua Homan, and Mike Scott, "Operation Poisoned Hurricane," FireEye, August 6, 2014, accessed March 28, 2022, <https://www.fireeye.com/blog/threat-research/2014/08/operation-poisoned-hurricane.html>.
- 475 Andy Schworer and Josh Liburdi, "Storm Chasing: Hunting Hurricane Panda," CrowdStrike, January 26, 2015, (archived by Internet Archive on May 14, 2016), <https://web.archive.org/web/20160514113122/https://www.crowdstrike.com/blog/storm-chasing>.
- 476 "When Pandas Attack: Defending A Technology Company," CrowdStrike, n.d., (archived by Internet Archive on April 1, 2015), https://web.archive.org/web/20150401010832/https://www.crowdstrike.com/wp-content/uploads/2015/03/crowdstrike-Case-Study_When-Pandas-Attack.pdf.
- 477 Dmitiri Alperovitch, "Cyber Deterrence in Action? A story of one long HURRICANE PANDA campaign," The Adversary Manifesto by CrowdStrike, April 13, 2015, (archived by Internet Archive on April 11, 2016), <https://web.archive.org/web/20160411003050/https://www.crowdstrike.com/blog/cyber-deterrence-in-action-a-story-of-one-long-hurricane-panda-campaign>.
- 478 Andy Schworer and Josh Liburdi, "Storm Chasing: Hunting Hurricane Panda," CrowdStrike, January 26, 2015, (archived by Internet Archive on May 14, 2016), <https://web.archive.org/web/20160514113122/https://www.crowdstrike.com/blog/storm-chasing>.
- 479 "CrowdStrike Discovers Use of 64-bit Zero-Day Privilege Escalation Exploit (CVE-2014-4113) by Hurricane Panda," CrowdStrike, October 14, 2014, accessed March 28, 2022, <https://www.crowdstrike.com/blog/crowdstrike-discovers-use-64-bit-zero-day-privilege-escalation-exploit-cve-2014-4113-hurricane-panda>.
- 480 "When Pandas Attack: Defending A Technology Company," CrowdStrike, n.d., (archived by Internet Archive on April 1, 2015), https://web.archive.org/web/20150401010832/https://www.crowdstrike.com/wp-content/uploads/2015/03/crowdstrike-Case-Study_When-Pandas-Attack.pdf.
- 481 Dmitri Alperovitch, "Cyber Deterrence in Action? A story of one long HURRICANE PANDA campaign," CrowdStrike, April 13, 2015, (archived by Internet Archive on August 7, 2019), <https://web.archive.org/web/20190807081609/https://www.crowdstrike.com/blog/cyber-deterrence-in-action-a-story-of-one-long-hurricane-panda-campaign>.
- 482 "Democracy in Hong Kong Under Attack," Volexity, October 9, 2014, (archived by Internet Archive on July 30, 2017), <https://web.archive.org/web/20170730230501/https://www.volexity.com/blog/2014/10/09/democracy-in-hong-kong-under-attack>.
- 483 "Democracy in Hong Kong Under Attack," Volexity, October 9, 2014, (archived by Internet Archive on July 30, 2017), <https://web.archive.org/web/20170730230501/https://www.volexity.com/blog/2014/10/09/democracy-in-hong-kong-under-attack>.
- 484 Ned Moran, Mike Oppenheim, and Mike Scott, "Operation Poisoned Handover: Unveiling Ties Between APT Activity in Hong Kong's Pro-Democracy Movement," FireEye, November 3, 2014, (archived by Internet Archive on March 31, 2015), <https://www.fireeye.com/blog/threat-research/2014/11/operation-poisoned-handover-unveiling-ties-between-apt-activity-in-hong-kongs-pro-democracy-movement.html>.
- 485 Jen Miller-Osborn, "Attacks on East Asia using Google Code for Command and Control," Palo Alto Networks, August 15, 2014, accessed March 28, 2022, <https://unit42.paloaltonetworks.com/attacks-east-asia-using-google-code-command-control>.
- 486 Jen Miller-Osborn, "Attacks on East Asia using Google Code for Command and Control," Palo Alto Networks, August 15, 2014, accessed March 28, 2022, <https://unit42.paloaltonetworks.com/attacks-east-asia-using-google-code-command-control>.

- 487 "Operation Poisoned Helmand," ThreatConnect, December 21, 2014, accessed March 28, 2022, <https://threatconnect.com/blog/operation-poisoned-helmand>.
- 488 "Operation Poisoned Helmand," ThreatConnect, December 21, 2014, accessed March 28, 2022, <https://threatconnect.com/blog/operation-poisoned-helmand>.
- 489 UNITED STATES OF AMERICA v. FUJIE WANG and JOHN DOE, Case: 1:19-cr-153-JRS-MJD, United States District Court Southern District of Indiana Indianapolis Division, May 7, 2019, accessed March 28, 2022, <https://www.justice.gov/opa/press-release/file/1161466/download>.
- 490 Bishr Tabbaa, "Take Out – How Anthem was Breached," DataSeries, February 17, 2019, accessed March 28, 2022, <https://medium.com/dataseries/take-out-how-anthem-was-breached-276b9ffca8da>.
- 491 "The Anthem Hack: All Roads Lead to China," ThreatConnect, February 27, 2015, accessed March 28, 2022, <https://threatconnect.com/blog/the-anthem-hack-all-roads-lead-to-china>.
- 492 "The Anthem Hack: All Roads Lead to China," ThreatConnect, February 27, 2015, accessed March 28, 2022, <https://threatconnect.com/blog/the-anthem-hack-all-roads-lead-to-china>.
- 493 Matt Dahl, "I am Ironman: DEEP PANDA Uses Sakula Malware to Target Organizations in Multiple Sectors," CrowdStrike, November 24, 2014, accessed March 28, 2022, <https://www.crowdstrike.com/blog/ironman-deep-panda-uses-sakula-malware-target-organizations-multiple-sectors>.
- 494 Matt Dahl, "I am Ironman: DEEP PANDA Uses Sakula Malware to Target Organizations in Multiple Sectors," CrowdStrike, November 24, 2014, accessed March 28, 2022, <https://www.crowdstrike.com/blog/ironman-deep-panda-uses-sakula-malware-target-organizations-multiple-sectors>.
- 495 Matt Dahl, "I am Ironman: DEEP PANDA Uses Sakula Malware to Target Organizations in Multiple Sectors," CrowdStrike, November 24, 2014, accessed March 28, 2022, <https://www.crowdstrike.com/blog/ironman-deep-panda-uses-sakula-malware-target-organizations-multiple-sectors>.
- 496 Suzanne Sataline, "Hong Kong activists fear they are being monitored by Beijing," *The Guardian*, December 14, 2019, accessed March 28, 2022, <http://www.theguardian.com/world/2014/dec/14/hong-kong-activists-beijing-chinese-spying-pro-democracy>.
- 497 John DiMaggio, "The Black Vine cyberespionage group," Symantec, last modified August 6, 2015, accessed March 28, 2022, <https://docs.broadcom.com/doc/the-black-vine-cyberespionage-group>.
- 498 John DiMaggio, "The Black Vine cyberespionage group," Symantec, last modified August 6, 2015, accessed March 28, 2022, <https://docs.broadcom.com/doc/the-black-vine-cyberespionage-group>.
- 499 John DiMaggio, "The Black Vine cyberespionage group," Symantec, last modified August 6, 2015, accessed March 28, 2022, <https://docs.broadcom.com/doc/the-black-vine-cyberespionage-group>.
- 500 "ThreatScape Media Highlights Update – Week Of July 29th," iSight Partners, July 29, 2015, accessed March 28, 2022, https://isight39/rssing.com/chan-53793970/all_p1.html.
- 501 "The Anthem Hack: All Roads Lead to China," ThreatConnect, February 27, 2015, accessed March 28, 2022, <https://threatconnect.com/blog/the-anthem-hack-all-roads-lead-to-china>.
- 502 Owen Fletcher, "Patriotic Chinese Hacking Group Reboots," *The Wall Street Journal*, October 5, 2011, accessed March 28, 2022, <https://www.wsj.com/articles/BL-CJB-14435>.
- 503 王文文 (Wang Wenwen), "中国黑客盛会——COG2011现场直击 ("Chinese Hacker Extravaganza - COG2011 Live Strike")," 51CTO.COM, September 25, 2011 (archived by Internet Archive on February 20, 2017), <https://web.archive.org/web/20170220171544/http://netsecurity.51cto.com/art/201109/294184.htm>.
- 504 "Advanced Persistent Threat Groups," Mandiant, n.d., accessed March 28, 2022, <https://www.mandiant.com/resources/apt-groups>.
- 505 Morgan Demboski, Joey Fitzpatrick, and Peter Rydzynski, "China cyber attacks: the current threat landscape," IronNet, October 26, 2021, <https://www.ironnet.com/blog/china-cyber-attacks-the-current-threat-landscape>.
- 506 "Positive Technologies: APT group targeting government agencies around the world detected in Russia for the first time," Positive Technologies, August 3, 2021, accessed March 28, 2022, <https://www.ptsecurity.com/ww-en/about/news/positive-technologies-apt-group-targeting-government-agencies-around-the-world-detected-in-russia-for-the-first-time>.
- 507 "APT31," Rapid7, n.d., accessed March 28, 2022, <https://docs.rapid7.com/insightidr/apt-groups/#apt31>.
- 508 "Advanced Persistent Threat Groups," Mandiant, n.d., accessed March 28, 2022, <https://www.mandiant.com/resources/apt-groups>.
- 509 Morgan Demboski, Joey Fitzpatrick, and Peter Rydzynski, "China cyber attacks: the current threat landscape," IronNet, October 26, 2021, <https://www.ironnet.com/blog/china-cyber-attacks-the-current-threat-landscape>.
- 510 "APT31," Rapid7, n.d., accessed March 28, 2022, <https://docs.rapid7.com/insightidr/apt-groups/#apt31>.
- 511 "Four Chinese Nationals Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including Infectious Disease Research," The United States Department of Justice, July 19, 2021, accessed March 28, 2022, <https://www.justice.gov/opa/pr/four-chinese-nationals-working-ministry-state-security-charged-global-computer-intrusion>.
- 512 Mark A. Stokes, Jenny Lin, and L.C. Russell Hsiao, "The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure," Project 2049, November 11, 2011, accessed March 28, 2022, https://project2049.net/wp-content/uploads/2018/05/pla_third_department_sigin_t Cyber Stokes lin hsiao.pdf.
- 513 Leng Shumei and Bai Yunyi, "Alleged hackers deny Vietnam job," *Global Times*, August 1, 2016, accessed September 21, 2016, <http://www.globaltimes.cn/content/997588.shtml>.
- 514 "中国网军公盟 ("China Internet Army Alliance)", Baidu Baike, n.d., (archived by Internet Archive on December 21, 2014), <https://web.archive.org/web/20141221034230/http://baike.com/wiki/%E4%B8%AD%E5%9B%BD%E7%BD%91%E5%86%9B%E5%85%AC%E7%9B%9F>.
- 515 "中国网军公盟 ("China Internet Army Alliance)", Baidu Baike, (archived by Internet Archive on October 10, 2016), <https://web.archive.org/web/20161010001731/http://www.baike.com/wiki/%E4%B8%AD%E5%9B%BD%E7%BD%91%E5%86%9B%E5%85%AC%E7%9B%9F>.
- 516 越南邻国宰相V ("Prime Minister of Vietnam's Neighbor V"), "1937CN停止解析公告 ("1937CN stop parsing announcement")," 越南邻国宰相V的博客 ("Blog of Prime Minister of Vietnam's Neighbor V"), August 28, 2016, accessed March 28, 2022, http://blog.sina.com.cn/s/blog_13abb4b010102x847.html.
- 517 越南邻国宰相V ("Prime Minister of Vietnam's Neighbor V"), "1937CN停止解析公告," 越南邻国宰相V的博客 ("Blog of Prime Minister of Vietnam's Neighbor V"), August 28, 2016, accessed March 28, 2022, http://blog.sina.com.cn/s/blog_13abb4b010102x847.html.
- 518 "Alleged hackers deny Vietnam job," Sina, August 1, 2016, (archived by Internet Archive on August 2, 2016), <https://web.archive.org/web/20160802182930/english.sina.com/china/s/2016-08-01-detail-ifxunyya2915888.shtml>.

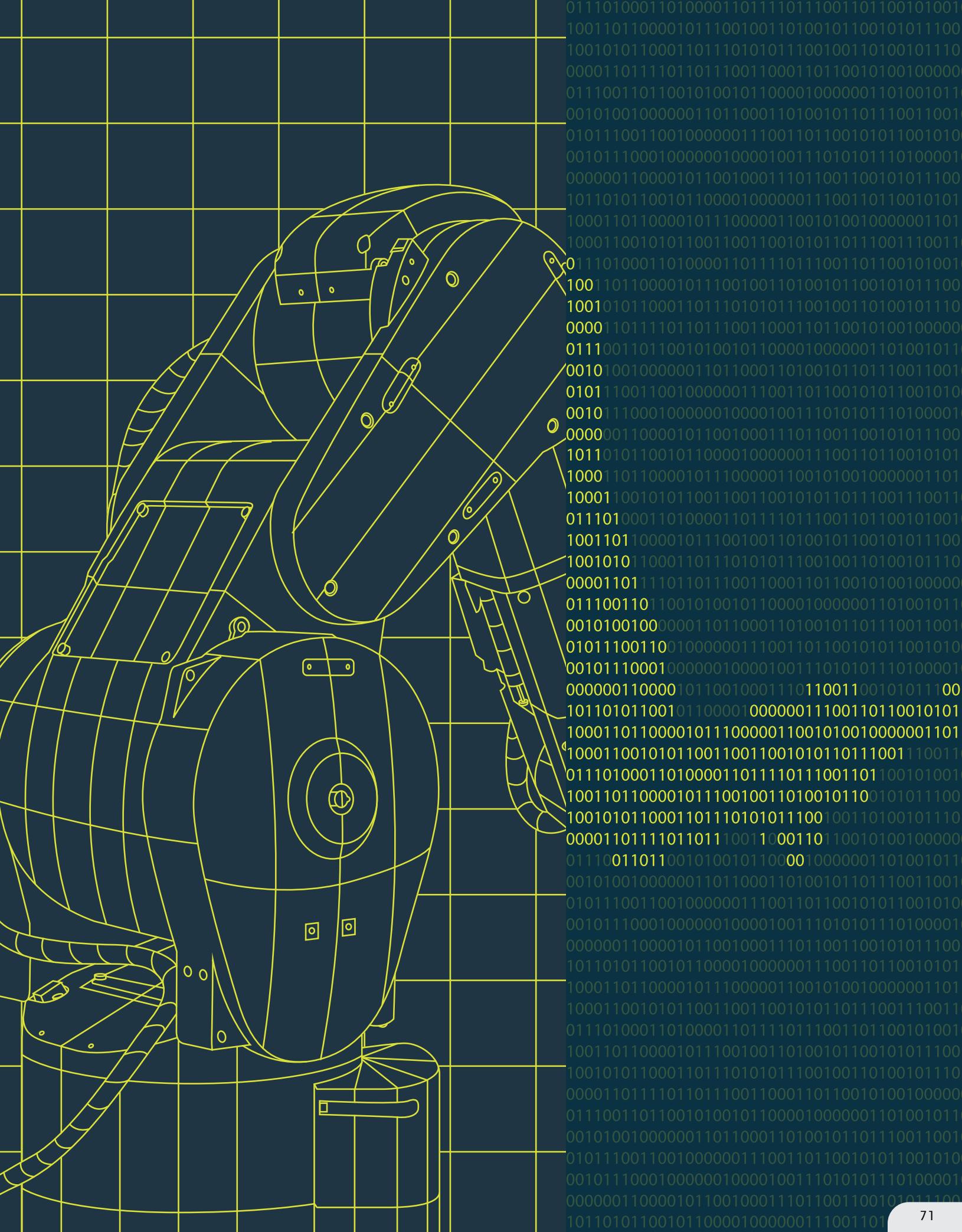
- 519 Thành Luân, "Nhóm tin tặc 1937CN tấn công Vietnam Airlines là ai?" ("Who are the 1937CN hackers who attacked Vietnam Airlines?"), *Thanh Niên* ("Youth Newspaper"), <https://thanhnien.vn/cong-nghe/nhom-tin-tac-1937cn-tan-cong-vietnam-airlines-la-ai-728392.html>.
- 520 "Mã độc tấn công VNA xuất hiện tại nhiều cơ quan, doanh nghiệp" ("Malware that attacks VNA appears in many agencies and businesses"), *BKav*, August 8, 2016, accessed March 23, 2022, <https://www.bkav.com.vn/tin-tuc-noi-bat/-/view-content/139443/ma-octan-cong-vna-xuat-hien-tai-nhieu-co-quan-doanh-nghiep>.
- 521 Hoàng Diên, "Theo dõi, ngăn chặn kết nối và xóa các tập tin chứa mã độc" ("Monitor, prevent connections and delete malicious files"), *Công Thông Tin Điện Tử Chính Phủ* ("Government E-Portal"), n.d., accessed March 28, 2022, <http://e.gov.vn/theo-doi-ngan-chan-ket-noi-va-xoa-cac-tap-tin-chua-ma-doc-a-NewsDetails-37486-14-186.html>.
- 522 "Mã độc tấn công VNA xuất hiện tại nhiều cơ quan, doanh nghiệp" ("Malware that attacks VNA appears in many agencies and businesses"), *BKav*, August 8, 2016, accessed March 23, 2022, <https://www.bkav.com.vn/tin-tuc-noi-bat/-/view-content/139443/ma-octan-cong-vna-xuat-hien-tai-nhieu-co-quan-doanh-nghiep>.
- 523 Hoàng Diên, "Theo dõi, ngăn chặn kết nối và xóa các tập tin chứa mã độc" ("Monitor, prevent connections and delete malicious files"), *Công Thông Tin Điện Tử Chính Phủ* ("Government E-Portal"), n.d., accessed March 28, 2022, <http://e.gov.vn/theo-doi-ngan-chan-ket-noi-va-xoa-cac-tap-tin-chua-ma-doc-a-NewsDetails-37486-14-186.html>.
- 524 "Vụ giả mạo email kết luận Thủ tướng: Phát hiện biến thể 'Virus Biển Đông'" ("Fake email spoofs Prime Minister announcement: Detecting 'East Sea Virus' variant"), *Genk*, June 6, 2014, accessed March 29, 2022, <https://genk.vn/internet/vu-gia-mao-email-ket-luan-thu-tuong-phat-hien-bien-the-virus-bien-dong-2015060612185601.chn>
- 525 Yonathan Klijnsma, "Remote Control Interloper: Analyzing New Chinese htpRAT Malware Attacks Against ASEAN," *RiskIQ*, October 2017, accessed March 29, 2022, <https://cdn.riskiq.com/wp-content/uploads/2017/10/RiskIQ-htpRAT-Malware-Attacks.pdf>.
- 526 "Votiro Labs Exposed A New Hacking Campaign Targeting Vietnamese Organisations Using Weaponized Word Documents," *Votiro*, August 23, 2017, accessed March 29, 2022, <https://votiro.com/blog/votiro-labs-exposed-a-new-hacking-campaign-targeting-vietnamese-organisations-using-weaponized-word-documents>.
- 527 "Votiro Labs Exposed A New Hacking Campaign Targeting Vietnamese Organisations Using Weaponized Word Documents," *Votiro*, August 23, 2017, accessed March 29, 2022, <https://votiro.com/blog/votiro-labs-exposed-a-new-hacking-campaign-targeting-vietnamese-organisations-using-weaponized-word-documents>.
- 528 Jasper Manuel and Artem Semenchenko, "Rehashed RAT Used in APT Campaign Against Vietnamese Organizations," *Fortinet*, September 5, 2017, accessed March 29, 2022, <https://www.fortinet.com/blog/threat-research/rehashed-rat-used-in-apt-campaign-against-vietnamese-organizations>.
- 529 "CTA Adversary Playbook: Goblin Panda," *Fortinet*, November 1, 2018, accessed March 29, 2022, <https://www.fortinet.com/blog/threat-research/cta-security-playbook-goblin-panda>.
- 530 "Chiến dịch của nhóm APT Trung Quốc Goblin Panda tấn công vào Việt Nam lợi dụng đại dịch Covid-19" ("A campaign of Chinese APT group Goblin Panda targeted Vietnam to take advantage of the Covid-19 pandemic"), *Viettel Security*, March 29, 2022, accessed March 29, 2022, <https://blog.viettelcybersecurity.com/p1-chien-dich-cua-nhom-apt-trung-quoc-goblin-panda-tan-cong-vao-viet-nam-loi-dung-dai-dich-COVID-19>.
- 531 "Analyzing Digital Quartermasters in Asia – Do Chinese and Indian APTs Have a Shared Supply Chain?," *Anomali*, February 5, 2019, accessed March 29, 2022, <https://www.anomali.com/blog/analyzing-digital-quartermasters-in-asia-do-chinese-and-indian-apts-have-a-shared-supply-chain>.
- 532 "CrowdCasts Monthly: You Have an Adversary Problem," *CrowdStrike*, October 16, 2014, accessed March 29, 2022, <https://www.slideshare.net/crowdstrike/crowd-casts-monthly-you-have-an-adversary-problem>.
- 533 Adam Meyers, "Meet CrowdStrike's Adversary of the Month for August: GOBLIN PANDA," *CrowdStrike*, August 29, 2018, accessed March 29, 2022, <https://www.crowdstrike.com/blog/meet-crowd-strikes-adversary-of-the-month-for-august-goblin-panda>.
- 534 "What Is An Advanced Persistent Threat (APT)?," *CrowdStrike*, April 1, 2021, accessed March 29, 2022, <https://www.crowdstrike.com/cybersecurity-101/advanced-persistent-threat-apt>.
- 535 "CTA Adversary Playbook: Goblin Panda," *Fortinet*, November 1, 2018, accessed March 29, 2022, <https://www.fortinet.com/blog/threat-research/cta-security-playbook-goblin-panda>.
- 536 "Viettel on the way to becoming a world leading defense industry group," *People's Army Newspaper*, February 28, 2021, accessed March 23, 2022, <https://en.qdnd.vn/economy/military-businesses/viettel-on-the-way-to-becoming-a-world-leading-defense-industry-group-527325>.
- 537 "Chiến dịch của nhóm APT Trung Quốc Goblin Panda tấn công vào Việt Nam lợi dụng đại dịch Covid-19, ("China's APT Goblin Panda campaign attacks on Vietnam take advantage of Covid-19 pandemic"), *Viettel Security*, May 1, 2020, accessed March 23, 2022, <https://blog.viettelcybersecurity.com/p1-chien-dich-cua-nhom-apt-trung-quoc-goblin-panda-tan-cong-vao-viet-nam-loi-dung-dai-dich-COVID-19>.
- 538 "Analyzing Digital Quartermasters in Asia – Do Chinese and Indian APTs Have a Shared Supply Chain?," *Anomali*, February 5, 2019, accessed March 29, 2022, <https://www.anomali.com/blog/analyzing-digital-quartermasters-in-asia-do-chinese-and-indian-apts-have-a-shared-supply-chain>.
- 539 "India targeted through cyber intrusions by RedFoxtriot linked to Chinese military," *The Economic Times*, last modified June 17, 2021, accessed March 29, 2022, <https://economictimes.indiatimes.com/news/defence/india-targeted-through-cyber-intrusions-by-redfoxtriot-linked-to-chinese-military/articleshow/83602134.cms?from=mdr>.
- 540 "Four Chinese Nationals Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including Infectious Disease Research," *The United States Department of Justice*, July 19, 2021, accessed March 28, 2022, <https://www.justice.gov/opa/pr/four-chinese-nationals-working-ministry-state-security-charged-global-computer-intrusion>.
- 541 "India targeted through cyber intrusions by RedFoxtriot linked to Chinese military," *The Economic Times*, last modified June 17, 2021, accessed March 29, 2022, <https://economictimes.indiatimes.com/news/defence/india-targeted-through-cyber-intrusions-by-redfoxtriot-linked-to-chinese-military/articleshow/83602134.cms?from=mdr>.
- 542 "Sophisticated APT group targeting high-profile entities in Southeast Asia sharpens its toolkit," *Kaspersky*, June 3, 2020, accessed March 29, 2022, https://www.kaspersky.com/about/press-releases/2020_sophisticated-apt-group-targeting-high-profile-entities-in-southeast-asia-sharpens-its-toolkit.
- 543 Ivan Kwiatkowski, Pierre Delcher, and Mark Lechtik, "The leap of a Cycldek-related threat actor," *Securelist* by Kaspersky Lab, April 5, 2021, <https://securelist.com/the-leap-of-a-cycldek-related-threat-actor/101243>.

- 544 "Sophisticated APT group targeting high-profile entities in Southeast Asia sharpens its toolkit," Kaspersky, June 3, 2020, accessed March 29, 2022, https://www.kaspersky.com/about/press-releases/2020_sophisticated-apt-group-targeting-high-profile-entities-in-southeast-asia-sharpens-its-toolkit.
- 545 Tara Seals, "Sophisticated Info-Stealer Targets Air-Gapped Devices via USB," ThreatPost, June 3, 2020, accessed March 29, 2022, <https://threatpost.com/info-stealer-air-gapped-devices-usb/156262>.
- 546 Costin Raiu and Maxim Golovkin, "The Chronicles of the Hellsing APT: the Empire Strikes Back," Securelist by Kaspersky Lab, April 15, 2015, accessed March 29, 2022, <https://securelist.com/the-chronicles-of-the-hellsing-apt-the-empire-strikes-back/69567>.
- 547 "API: Advanced Search," FireEye, n.d., accessed March 29, 2022, https://docs.fireeye.com/iSight/index.html#/advanced_search.
- 548 Jinsuk Oh, "통합적, 효율적 보안 운영을 위한 플랫폼 구축 방안, ("How to build a platform for integrated and efficient security operation")," FireEye, (archived by Internet Archive on November 10, 2020), https://web.archive.org/web/20201110165731/http://freeeyeday.com/event/pdf/T1_3.CyberDefenseLive2018.pdf.
- 549 Matthew Tostevin, "Chinese cyber spies broaden attacks in Vietnam, security firm says," Reuters, August 31, 2017, accessed March 29, 2022, <https://www.reuters.com/article/us-vietnam-china-cyber-chinese-cyber-spies-broaden-attacks-in-vietnam-security-firm-says-idUSKCN1BBOI5>.
- 550 "'Winnti': More than a game," Kaspersky Lab, April 2013, accessed March 29, 2022, <https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2019/10/02153102/winnti-more-than-just-a-game-130410.pdf>.
- 551 Nart Villeneuve and Kyle Wilhoit, "Malicious PDFs On The Rise," TrendMicro, April 29, 2013 (archived by Internet Archive on September 3, 2021), <https://web.archive.org/web/20210903041330/https://blog.trendmicro.com/trendlabs-security-intelligence/malicious-pdfs-on-the-rise>.
- 552 "CrowdCasts Monthly: You Have an Adversary Problem," CrowdStrike, October 16, 2014, accessed March 29, 2022, <https://www.slideshare.net/crowdstrike/crowd-casts-monthly-you-have-an-adversary-problem>.
- 553 "Hive0045 Analysis Report," IBM X-Force, last modified October 17, 2021, accessed March 29, 2022, [dhttps://exchange.xforce.ibmcloud.com/threat-group/guid:c1269ad911f37598a8345d7bbca7a594](https://exchange.xforce.ibmcloud.com/threat-group/guid:c1269ad911f37598a8345d7bbca7a594).
- 554 UNITED STATES OF AMERICA CRIMINAL v. JIANG LIZHI, QIAN CHUAN, and FU QIANG, United States District Court for The District of Columbia, August 11, 2020, accessed March 17, 2022, <https://www.justice.gov/opa/press-release/file/1317206/download>. (p. 3, 6).
- 555 ASEC Report, Volume 93, AhnLab, April 2018, accessed March 29, 2022, https://image.ahnlab.com/file_upload/asecissue_files/ASEC%20REPORT_v0l.93.pdf.
- 556 ASEC Report, Volume 93, AhnLab, April 2018, accessed March 29, 2022, https://image.ahnlab.com/file_upload/asecissue_files/ASEC%20REPORT_v0l.93.pdf.
- 557 UNITED STATES OF AMERICA CRIMINAL v. JIANG LIZHI, QIAN CHUAN, and FU QIANG, United States District Court for The District of Columbia, August 11, 2020, accessed March 17, 2022, <https://www.justice.gov/opa/press-release/file/1317206/download>. (p. 3, 6).
- 558 "Advanced Persistent Threat Groups," FireEye, n.d., accessed March 29, 2022, <https://www.fireeye.com/current-threats/apt-groups.html#china>.
- 559 "Shadowpad: A Masterpiece Of Privately Sold Malware In Chinese Espionage," SentinelOne, n.d., accessed March 29, 2022, <https://assets.sentinelone.com/c/Shadowpad?x=P42eqA>.
- 560 Nikita Rostovcev, "Big airline heist: APT41 likely behind a third-party attack on Air India," Group-IB, last modified August 12, 2021, accessed March 29, 2022, https://blog.group-ib.com/columntk_apt41.
- 561 APT41 Perfects Code Signing Abuse to Escalate Supply Chain Attacks, Venafi, 2021, accessed May 30, 2022, https://www.venafi.com/sites/default/files/2021-11/Venafi_WhitePaper_CodeSigningAPT41_2021_f_0.pdf.
- 562 "Advanced Persistent Threat Groups," FireEye, n.d., accessed March 29, 2022, <https://www.fireeye.com/current-threats/apt-groups.html#china>.
- 563 "Double Dragon: APT41, a dual espionage and cyber crime operation," FireEye, 2019, accessed March 29, 2022, <https://content.fireeye.com/apt-41/rpt-apt41>.
- 564 "Double Dragon: APT41, a dual espionage and cyber crime operation," FireEye, 2019, accessed March 29, 2022, <https://content.fireeye.com/apt-41/rpt-apt41>.
- 565 Nalani Fraser et al., "APT41: A Dual Espionage and Cyber Crime Operation," FireEye, August 7, 2019, accessed March 29, 2022, <https://www.fireeye.com/blog/threat-research/2019/08/apt41-dual-espionage-and-cyber-crime-operation.html>.
- 566 "Winnti. More than just a game," Securelist by Kaspersky, April 11, 2013, accessed March 17, 2022, <https://securelist.com/winnti-more-than-just-a-game/37029>.
- 567 Marc-Etienne M. Léveillé, "Gaming industry still in the scope of attackers in Asia," WeLiveSecurity by ESET, March 11, 2019, accessed March 28, 2028, <https://www.welivesecurity.com/2019/03/11/gaming-industry-scope-attackers-asia>.
- 568 "Recent Winnti Infrastructure and Samples," ClearSky, July 18, 2017, accessed March 29, 2022, <https://www.clearskysec.com/winnti>.
- 569 Yi-Jhen Hsieh, "ShadowPad | A Masterpiece of Privately Sold Malware in Chinese Espionage," SentinelLabs by SentinelOne, August 19, 2021, accessed March 29, 2022, <https://labs.sentinelone.com/shadowpad-a-masterpiece-of-privately-sold-malware-in-chinese-espionage>.
- 570 Yi-Jhen Hsieh, "ShadowPad | A Masterpiece of Privately Sold Malware in Chinese Espionage," SentinelLabs by SentinelOne, August 19, 2021, accessed March 29, 2022, <https://labs.sentinelone.com/shadowpad-a-masterpiece-of-privately-sold-malware-in-chinese-espionage>.
- 571 Nikita Rostovcev, "Big airline heist: APT41 likely behind a third-party attack on Air India," Group-IB, last modified August 12, 2021, accessed March 29, 2022, https://blog.group-ib.com/columntk_apt41.
- 572 APT41 Perfects Code Signing Abuse to Escalate Supply Chain Attacks, Venafi, 2021, accessed March 29, 2022, https://www.venafi.com/sites/default/files/2021-11/Venafi_WhitePaper_CodeSignin-gAPT41_2021_f_0.pdf.
- 573 James T. Bennett and Mike Scott, "Forced to Adapt: XSLCmd Backdoor Now on OS X," FireEye, September 4, 2014, (archived by Internet Archive on January 15, 2015), <https://web.archive.org/web/20150115145927/https://www.fireeye.com/blog/threat-research/2014/09/forced-to-adapt-xslcmd-backdoor-now-on-os-x.html>.
- 574 "Double Dragon: APT41, a dual espionage and cyber crime operation," FireEye, 2019, accessed March 29, 2022, <https://content.fireeye.com/apt-41/rpt-apt41>.
- 575 "Double Dragon: APT41, a dual espionage and cyber crime operation," FireEye, 2019, accessed March 29, 2022, <https://content.fireeye.com/apt-41/rpt-apt41>.
- 576 Adam Meyers, "Meet CrowdStrike's Adversary of the Month for July: WICKED SPIDER," CrowdStrike, July 26, 2018, accessed March 28, 2022, <https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-july-wicked-spider>.

- 577 Adam Meyers, "Meet CrowdStrike's Adversary of the Month for July: WICKED SPIDER," CrowdStrike, July 26, 2018, accessed March 28, 2022, <https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-july-wicked-spider>.
- 578 Adam Meyers, "Meet CrowdStrike's Adversary of the Month for July: WICKED SPIDER," CrowdStrike, July 26, 2018, accessed March 28, 2022, <https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-july-wicked-spider>.
- 579 "Adversary: Wicked Panda," CrowdStrike, n.d., accessed March 29, 2022, <https://adversary.crowdstrike.com/en-US/adversary/wicked-panda>.
- 580 "Detecting threat actors in recent German industrial attacks with Windows Defender ATP," Microsoft, January 25, 2017, accessed March 29, 2022, <https://www.microsoft.com/security/blog/2017/01/25/detecting-threat-actors-in-recent-german-industrial-attacks-with-windows-defender-atp>.
- 581 "Detecting threat actors in recent German industrial attacks with Windows Defender ATP," Microsoft, January 25, 2017, accessed March 29, 2022, <https://www.microsoft.com/security/blog/2017/01/25/detecting-threat-actors-in-recent-german-industrial-attacks-with-windows-defender-atp>.
- 582 MICROSOFT CORPORATION vs. JOHN DOES 1-2, Civil Action No: 1:17-CV-1224, United States District Court for the Eastern District of Virginia Alexandria Division. October 26, 2017, accessed March 29, 2022, <https://www.courtousenews.com/wp-content/uploads/2017/11/barium.pdf>.
- 583 "APT41: Indictments Put Chinese Espionage Group in the Spotlight." Symantec Enterprise Blogs / Threat Intelligence by Broadcom, September 17, 2020, accessed March 29, 2022, <https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/apt41-indictments-china-espionage>.
- 584 <https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/apt41-indictments-china-espionage>.
- 585 "Winnti. More than just a game," Securelist by Kaspersky, April 11, 2013, accessed March 17, 2022, <https://securelist.com/winnti-more-than-just-a-game/37029>.
- 586 Marc-Etienne M.Léveillé, "Gaming industry still in the scope of attackers in Asia," WeLiveSecurity by ESET, March 11, 2019, accessed March 28, 2028, <https://www.welivesecurity.com/2019/03/11/gaming-industry-scope-attackers-asia>.
- 587 "Recent Winnti Infrastructure and Samples," ClearSky, July 18, 2017, accessed March 29, 2022, <https://www.clearskysec.com/winnti>.
- 588 Cedric Pernet, "Winnti Abuses GitHub for C&C Communications," TrendMicro, March 22, 2017, accessed March 29, 2022, (archived by Internet Archive on November 16, 2018), <https://web.archive.org/web/20181116101226/https://blog.trendmicro.com/trendlabs-security-intelligence/winnti-abuses-github>.
- 589 "Winnti. More than just a game," Securelist by Kaspersky, April 11, 2013, accessed March 17, 2022, <https://securelist.com/winnti-more-than-just-a-game/37029>.
- 590 Marc-Etienne M.Léveillé, "Gaming industry still in the scope of attackers in Asia," WeLiveSecurity by ESET, March 11, 2019, accessed March 28, 2028, <https://www.welivesecurity.com/2019/03/11/gaming-industry-scope-attackers-asia>.
- 591 Tom Hegel, "Burning Umbrella: An Intelligence Report on the Winnti Umbrella and Associated State-Sponsored Attackers," 401 TRG, May 3, 2018, (archived by Internet Archive on January 29, 2019), <https://web.archive.org/web/20190129032504/https://401trg.com/burning-umbrella>.
- 592 Tom Hegel, "Burning Umbrella: An Intelligence Report on the Winnti Umbrella and Associated State-Sponsored Attackers," 401 TRG, May 3, 2018, (archived by Internet Archive on January 29, 2019), <https://web.archive.org/web/20190129032504/https://401trg.com/burning-umbrella>.
- 593 "Threat Group-3279 Targets the Video Game Industry," Secureworks, July 29, 2014, accessed March 29, 2022, <https://www.secureworks.com/research/threat-group-3279-targets-the-video-game-industry>.
- 594 "Threat Group-3279 Targets the Video Game Industry," Secureworks, July 29, 2014, accessed March 29, 2022, <https://www.secureworks.com/research/threat-group-3279-targets-the-video-game-industry>.
- 595 "Cyber Threats 2020: A Year in Retrospect," PwC, 2021., accessed March 28, 2022, <https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf>.
- 596 "Cyber Threats 2020: A Year in Retrospect," PwC, 2021., accessed March 28, 2022, <https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf>.
- 597 "Bronze Atlas," Secureworks, n.d., accessed March 29, 2022, <https://www.secureworks.com/research/threat-profiles/bronze-atlas>.
- 598 "Bronze Atlas," Secureworks, n.d., accessed March 29, 2022, <https://www.secureworks.com/research/threat-profiles/bronze-atlas>.
- 599 "Cyber Security Coalition Releases Full Report on Large-Scale Interdiction of Chinese State Sponsored Espionage Effort," Novetta, October 24, 2014, accessed March 29, 2022, <https://www.novetta.com/2014/10/cyber-security-coalition-releases-full-report-on-large-scale-interdiction-of-chinese-state-sponsored-espionage-effort>.
- 600 "Cyber Security Coalition Releases Full Report on Large-Scale Interdiction of Chinese State Sponsored Espionage Effort," Novetta, October 24, 2014, accessed March 29, 2022, <https://www.novetta.com/2014/10/cyber-security-coalition-releases-full-report-on-large-scale-interdiction-of-chinese-state-sponsored-espionage-effort>.
- 601 Hara Hiroaki and Ted Lee, "APT41 Resurfaces as Earth Baku With New Cyberespionage Campaign," TrendMicro, August 24, 2021, accessed March 29, 2022, https://www.trendmicro.com/en_us/research/21/h/apt41-resurfaces-as-earth-baku-with-new-cyberespionage-campaign.html.
- 602 Hara Hiroaki and Ted Lee, "Earth Baku: An APT Group Targeting Indo-Pacific Countries With New Stealth Loaders and Backdoor," TrendMicro, 2021, accessed March 29, 2022, https://documents.trendmicro.com/assets/white_papers/wp-earth-baku-an-apt-group-targeting-indo-pacific-countries.pdf.
- 603 "Cyber Security Coalition Releases Full Report on Large-Scale Interdiction of Chinese State Sponsored Espionage Effort," Novetta, October 24, 2014, accessed March 29, 2022, <https://www.novetta.com/2014/10/cyber-security-coalition-releases-full-report-on-large-scale-interdiction-of-chinese-state-sponsored-espionage-effort>.
- 604 "Operation SMN: Axiom Threat Actor Group Report | 公理队 ("Axiom Team")," Novetta, n.d., March 29, 2022, <https://www.novetta.com/wp-content/uploads/2020/10/Axiom-Executive-Summary.pdf>.
- 605 Snorre Fagerland, "The Korean Gaming Industry Is Still Under Fire," BlueCoat, August 21, 2014, reposted on Naver by @bluecoatkr on Naver on April 3, 2015, accessed March 29, 2022, <https://m.blog.naver.com/PostView.naver?isHttpsRedirect=true&blogId=bluecoatkr&logNo=220319357366>.
- 606 "Digitally Signed Malware Targeting Gaming Companies," BlackBerry, October 18, 2016, accessed March 29, 2022, <https://blogs.blackberry.com/en/2016/10/digitally-signed-malware-targeting-gaming-companies>.

- 607 Mark A. Stokes, Jenny Lin, and L.C. Russell Hsiao, "The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure," Project 2049, November 11, 2011, accessed March 28, 2022, https://project2049.net/wp-content/uploads/2018/05/pla_third_department_sigint_cyber_stokes_lin_hsiao.pdf.
- 608 Military and Security Developments Involving the People's Republic of China 2021: Annual Report to Congress, Office of the Secretary of Defense, 2021, accessed March 28, 2022, <https://media.defense.gov/2021/Nov/03/2002885874/-1/-1/0/2021-CMPR-FINAL.PDF>. (p. 110)
- 609 Nalani Fraser and Kelli Vanderlee, "Achievement Unlocked: Cyber Espionage Evolves to Support Higher Level Missions," FireEye, 2019, accessed March 29, 2022, <https://www.fireeye.com/content/dam/fireeye-www/summit/cds-2019/presentations/cds19-executive-s08-achievement-unlocked.pdf>.
- 610 Warren Mercer, Paul Rascagneres and Vitor Ventura, "Bisonal: 10 years of play," Cisco Talos, last modified June 3, 2020, accessed March 29, 2022, <https://blog.talosintelligence.com/2020/03/bisonal-10-years-of-play.html>.
- 611 "The 'Big Four' Spotlight on China," FireEye, n.d., accessed March 29, 2022, <https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/pf/podcasts/transcript-big-four-spotlight-china.pdf>.
- 612 Charlie Osborne, "Chinese hackers use decade-old Bisonal Trojan in cyberespionage campaigns," ZDNet, March 5, 2020, accessed March 29, 2022, <https://www.zdnet.com/article/chinese-hackers-use-decade-old-bisonal-trojan-to-strike-russian-targets>.
- 613 Nalani Fraser and Kelli Vanderlee, "Achievement Unlocked: Cyber Espionage Evolves to Support Higher Level Missions," FireEye, 2019, accessed March 29, 2022, <https://www.fireeye.com/content/dam/fireeye-www/summit/cds-2019/presentations/cds19-executive-s08-achievement-unlocked.pdf>.
- 614 Warren Mercer, Paul Rascagneres and Vitor Ventura, "Bisonal: 10 years of play," Cisco Talos, last modified June 3, 2020, accessed March 29, 2022, <https://blog.talosintelligence.com/2020/03/bisonal-10-years-of-play.html>.
- 615 Roland Dela Paz, "Pulsing the HeartBeat APT," TrendMicro, January 3, 2013, (archived by Internet Archive on February 12, 2013), <https://web.archive.org/web/20130212122136/https://blog.trendmicro.com/trendlabs-security-intelligence/pulsing-the-heartbeat-apt>.
- 616 Kaoru Hayashi and Vicky Ray, "Bisonal Malware Used in Attacks Against Russia and South Korea," Palo Alto Networks, July 21, 2018, accessed March 29, 2022, <https://unit42.paloaltonetworks.com/unit42-bisonal-malware-used-attacks-russia-south-korea>.
- 617 "Bronze Huntley," Secureworks, n.d., accessed March 29, 2022, <https://www.secureworks.com/research/threat-profiles/bronze-huntley>.
- 618 "Bronze Huntley," Secureworks, n.d., accessed March 29, 2022, <https://www.secureworks.com/research/threat-profiles/bronze-huntley>.
- 619 "Cyber Threats 2020: A Year in Retrospect," PwC, 2021., accessed March 28, 2022, <https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf>.
- 620 Konstantin Zykov, "CactusPete APT group's updated Bisonal backdoor," SecureList by Kaspersky, August 13, 2020, accessed March 29, 2020, <https://securelist.com/cactuspete-apt-groups-updated-bisonal-backdoor/97962>.
- 621 "Curious Korlia," Adventures in Security, November 25, 2014, accessed March 29, 2022, <https://web.archive.org/web/20200915000205/https://securitykitten.github.io/2014/11/25/curious-korlia.html>.
- 622 Konstantin Zykov, "CactusPete APT group's updated Bisonal backdoor," SecureList by Kaspersky, August 13, 2020, accessed March 29, 2020, <https://securelist.com/cactuspete-apt-groups-updated-bisonal-backdoor/97962>.
- 623 Wendy Rafferty and Christopher Scott, "The New State of Incident Response: Remediating Under Fire," CrowdStrike, n.d., accessed March 29, 2022, <https://issala.org/wp-content/uploads/2019/11/CrowdStrike-ISSA-LA-20150318.pdf>.
- 624 Adam Meyers and Elia Zaitsev, "CrowdCast Monthly: Operationalizing Intelligence," CrowdStrike April 30, 2014, accessed March 29, 2022, <https://www.slideshare.net/crowdstrike/crowdcast-monthly-operationalizing-intelligence-34141777>.
- 625 "SECURING TODAY'S DISTRIBUTED WORKFORCE: Resources for Ensuring Optimal Security During the Global Pandemic," CrowdStrike, n.d., accessed March 29, 2022, <https://www.crowdstrike.com/falcon/wp-content/uploads/2020/10/eBookCybersecurityCOVID-19.pdf>.
- 626 Adam Meyers, "Situational Awareness: Cyber Threats Heightened by COVID-19 and How to Protect Against Them," CrowdStrike, March 24, 2020, accessed March 29, 2022, <https://www.crowdstrike.com/blog/covid-19-cyber-threats>.
- 627 ASEC Report, Volume 93, AhnLab, April 2018, accessed March 29, 2022, https://image.ahnlab.com/file_upload/asecissue_files/ASEC%20REPORT_vol.93.pdf.
- 628 ASEC Report, Volume 93, AhnLab, April 2018, accessed March 29, 2022, https://image.ahnlab.com/file_upload/asecissue_files/ASEC%20REPORT_vol.93.pdf.
- 629 "Beware, Bioazih virus on prowl in Indian cyberspace: Cert-In," The Times of India, May 14, 2015, accessed May 30, 2022, <https://www.gadgetsnow.com/tech-news/Beware-Bioazih-virus-on-prowl-in-Indian-cyberspace-Cert-In-warns/articleshow/47281885.cms>.
- 630 Mark A. Stokes, Jenny Lin, and L.C. Russell Hsiao, "The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure," Project 2049, November 11, 2011, accessed March 28, 2022, https://project2049.net/wp-content/uploads/2018/05/pla_third_department_sigint_cyber_stokes_lin_hsiao.pdf.
- 631 Military and Security Developments Involving the People's Republic of China 2021: Annual Report to Congress, Office of the Secretary of Defense, 2021, accessed March 28, 2022, <https://media.defense.gov/2021/Nov/03/2002885874/-1/-1/0/2021-CMPR-FINAL.PDF>. (p. 98)
- 632 John DiMaggio, "Tick cyberespionage group zeros in on Japan," Broadcom, April 28, 2016, accessed March 29, 2022, <https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=5da7ee8f-e251-4e14-acf5-693bdd61bde6&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments>.
- 633 "Tick'ing Time Bomb: Critical Analysis of the Tick Threat Actor Group," Cyfirma, September 19, 2019, accessed March 29, 2022, <https://www.cyfirma.com/blogs/ticking-time-bomb-critical-analysis-of-the-tick-threat-actor-group>.
- 634 "Attackers that Target Critical Infrastructure Providers in Japan," Cyber Grid View, Vol. 2, 2016, LAC Co., 2016, accessed March 29, 2022, https://www.lac.co.jp/english/report/pdf/cgview_vol2_en.pdf.
- 635 Joey Chen, Kakara Hiroyuki, and Shoji Masaoki, "Operation ENDTRADE: Multi-Stage Backdoors that TICK," TrendMicro, November 29, 2019, accessed March 29, 2022, https://www.trendmicro.com/en_us/research/19/k/operation-endtrade-finding-multi-stage-backdoors-that-tick.html.
- 636 "China's PLA allegedly behind cyberattacks in Japan," NHK World-Japan, April 19, 2021, (archived by Internet Archive on April 21, 2021), https://web.archive.org/web/20210421103530/https://www3.nhk.or.jp/nhkworld/en/news/20210420_10.

- 637 John DiMaggio, "Tick cyberespionage group zeros in on Japan," Broadcom, April 28, 2016, accessed March 29, 2022, <https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=5da7ee8f-e251-4e14-acf5-693bdd61bde6&CommunityKey=1ecf5f55-545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments>.
- 638 "Tick'ing Time Bomb: Critical Analysis of the Tick Threat Actor Group," Cyfirma, September 19, 2019, accessed March 29, 2022, <https://www.cyfirma.com/blogs/ticking-time-bomb-critical-analysis-of-the-tick-threat-actor-group>.
- 639 Joey Chen, Kakara Hiroyuki, and Shoji Masaoki, "Operation ENDTRADE: Multi-Stage Backdoors that TICK," TrendMicro, November 29, 2019, accessed March 29, 2022, https://www.trendmicro.com/en_us/research/19/k/operation-endtrade-finding-multi-stage-backdoors-that-tick.html.
- 640 Joey Chen and MingYen Hsieh, "REDBALDKNIGHT's Daserf Backdoor Now Uses Steganography," TrendMicro, November 7, 2017, accessed March 29, 2017, https://www.trendmicro.com/en_us/research/17/k/redbaldknight-bronze-butler-daserf-backdoor-now-using-steganography.html.
- 641 "China's PLA allegedly behind cyberattacks in Japan," NHK World-Japan, April 19, 2021, accessed March 29, 2022, (archived by Internet Archive on April 21, 2021), https://web.archive.org/web/20210421103530/https://www3.nhk.or.jp/nhkworld/en/news/20210420_10.
- 642 "China's PLA allegedly behind cyberattacks in Japan," NHK World-Japan, April 19, 2021, accessed March 29, 2022, (archived by Internet Archive on April 21, 2021), https://web.archive.org/web/20210421103530/https://www3.nhk.or.jp/nhkworld/en/news/20210420_10.
- 643 "China's PLA allegedly behind cyberattacks in Japan," NHK World-Japan, April 19, 2021, accessed March 29, 2022, (archived by Internet Archive on April 21, 2021), https://web.archive.org/web/20210421103530/https://www3.nhk.or.jp/nhkworld/en/news/20210420_10.
- 644 "Bronze Butler," Secureworks, n.d., accessed March 29, 2022, <https://www.secureworks.com/research/threat-profiles/bronze-butler>.
- 645 "Bronze Butler," Secureworks, n.d., accessed March 29, 2022, <https://www.secureworks.com/research/threat-profiles/bronze-butler>.
- 646 "Cyber Espionage Tradecraft in the Real World: Adversaries targeting Japan in the second half of 2019," Macnica Networks and TeamT5, May 1, 2020, accessed March 29, 2022, https://www.macnica.co.jp/business/security/manufacturers/files/mppressioncss_ta_report_2019_4_en.pdf.
- 647 "Cyber Espionage Tradecraft in the Real World: Adversaries targeting Japan in the second half of 2019," Macnica Networks and TeamT5, May 1, 2020, accessed March 29, 2022, https://www.macnica.co.jp/business/security/manufacturers/files/mppressioncss_ta_report_2019_4_en.pdf.
- 648 2020 GLOBAL THREAT REPORT, CrowdStrike, 2020, accessed March 29, 2022, https://www.newcastle.edu.au/_data/assets/pdf_file/0006/616875/2020_Global-Threat-Report.pdf.
- 649 2018 GLOBAL THREAT REPORT, CrowdStrike, n.d., accessed March 29, 2022, <https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2018GlobalThreatReport.pdf>.
- 650 Kevin McCauley, "Snapshot: China's Western Theater Command," China Brief, Volume: 17 Issue: 1, The Jamestown Foundation, January 13, 2017, accessed March 28, 2022, <https://jamestown.org/program/snapshot-chinas-western-theater-command>.
- 651 Sahil Joshi and Divyesh Singh, "Mega Mumbai power outage may be result of cyber attack, final report awaited," *India Today*, November 20, 2020, accessed March 28, 2022, <https://www.indiatoday.in/india/story/mumbai-power-outage-malware-attack-1742538-2020-11-20>.
- 652 "China-Linked Group RedEcho Targets the Indian Power Sector Amid Heightened Border Tensions," Recorded Future, 2021, accessed March 28, 2022, <https://go.recordedfuture.com/hubfs/reports/cta-2021-0228.pdf>.
- 653 "China-Linked Group RedEcho Targets the Indian Power Sector Amid Heightened Border Tensions," Recorded Future, 2021, accessed March 28, 2022, <https://go.recordedfuture.com/hubfs/reports/cta-2021-0228.pdf>.
- 654 "China-Linked Group RedEcho Targets the Indian Power Sector Amid Heightened Border Tensions," Recorded Future, 2021, accessed March 28, 2022, <https://go.recordedfuture.com/hubfs/reports/cta-2021-0228.pdf>.
- 655 Mark Stokes, "The PLA General Staff Department Third Department Second Bureau: An Organizational Overview of Unit 61398," Project 2049 Institute, July 27, 2015, accessed March 29, 2022, <https://project2049.net/2015/07/27/the-pla-general-staff-department-third-department-second-bureau-an-organizational-overview-of-unit-61398>.
- 656 Elsa Kania, "PLA Strategic Support Force: The 'Information Umbrella' for China's Military," *The Diplomat*, April 1, 2017, accessed March 29, 2022, <https://thediplomat.com/2017/04/pla-strategic-support-force-the-information-umbrella-for-chinas-military>.
- 657 "U.S. Charges Five Chinese Military Hackers For Cyber Espionage Against U.S. Corporations And A Labor Organization For Commercial Advantage," United States Department of Justice, May 19, 2014, accessed March 29, 2022, <https://www.justice.gov/usao-wdpa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and>.
- 658 "U.S. Charges Five Chinese Military Hackers For Cyber Espionage Against U.S. Corporations And A Labor Organization For Commercial Advantage," United States Department of Justice, May 19, 2014, accessed March 29, 2022, <https://www.justice.gov/usao-wdpa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and>.
- 659 Richard Bejtlich, "DoJ Indicts Chinese Military Hackers: First Impressions," FireEye, May 19, 2014, (archived by Internet Archive on January 22, 2015), <https://web.archive.org/web/20150122211209/https://www.fireeye.com/blog/executive-perspective/2014/05/doj-indicts-chinese-military-hackers-first-impressions.html>.
- 660 "APT1: Exposing One of China's Cyber Espionage Units," Mandiant, 2013, accessed March 25, 2022, <https://www.mandiant.com/sites/default/files/2021-09/mandiant-apt1-report.pdf>.
- 661 A L Johnson, "APT1: Q&A on Attacks by the Comment Crew," Broadcom, February 19, 2013, accessed March 29, 2022, <https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=f1265df5-6e5e-4fc-9828-d4ddbaf3d7&CommunityKey=1ecf55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments>.
- 662 "Hat-tribution to PLA Unit 61486," CrowdStrike, June 9, 2014, (archived by Internet Archive on March 20, 2016), <https://web.archive.org/web/20160320035717/https://www.crowdstrike.com/blog/hat-tribution-pla-unit-61486>.
- 663 "Hat-tribution to PLA Unit 61486," CrowdStrike, June 9, 2014, (archived by Internet Archive on March 20, 2016), <https://web.archive.org/web/20160320035717/https://www.crowdstrike.com/blog/hat-tribution-pla-unit-61486>.
- 664 Mark Clayton, "Stealing US business secrets: Experts ID two huge cyber 'gangs' in China" *The Christian Science Monitor*, September 14, 2012, accessed March 25, 2015, <https://www.csmonitor.com/USA/2012/0914/Stealing-US-business-secrets-Experts-ID-two-huge-cyber-gangs-in-China>.
- 665 "Operation Oceansalt' Attacks South Korea, U.S., and Canada With SourceCode From Chinese Hacker Group," McAfee, October 18, 2018, accessed March 29, 2022, <https://www.mcafee.com/enterprise/en-us/assets/reports/rp-operation-oceansalt.pdf>.



EMPOWER PEOPLE TO CHANGE THE WORLD®

For more than 100 years, military, government, and business leaders have turned to Booz Allen Hamilton to solve their most complex problems. As a consulting firm with experts in analytics, digital solutions, engineering, and cyber, we help organizations transform. We are a key partner on some of the most innovative programs for governments worldwide and trusted by its most sensitive agencies. We work shoulder-to-shoulder with clients, using a mission-first approach to choose the right strategy and technology to help them realize their vision.

With global headquarters in McLean, Virginia, our firm employs approximately 29,500 people globally as of March 31, 2022, and had revenue of \$8.4 billion for the 12 months ended March 31, 2022. To learn more, visit www.boozallen.com. (NYSE: BAH)