4. China's Cyber Influencing and Interference

At the turn of the century, Chinese leaders had an epiphany about the strategic character of cyberspace. The content of their revelation was conveyed in a series of secret speeches to the Central Military Commission (CMC) beginning in 2000. It was also evident in China's hosting of the World Computer Congress that year and the evolution of policy for monitoring Chinese citizens in cyberspace through a system of social control – even as Beijing began to plan the construction of the 'Great Firewall' to enable technology-based blocking of unwanted foreign content.[1] These developments followed years of engagement by a small group within the Chinese leadership dedicated to information policy, as well as the policy advocacy of leading civilian and military specialists from inside and outside China. In 2003, Beijing began its now notorious large-scale cyber-espionage efforts. It took until 2014 for China to recognise how seriously it lagged behind the US in cyber capabilities more broadly, when President Xi Jinping declared the government's intention to make China a 'cyber power'.[2]

By 2014, China had already created the world's most powerful cyber-based system for internal political surveillance, supported by a citizen army willing to monitor their peers in workplaces, universities and schools for signs of deviant political thought. It was around this time (2013–15) that China began to make changes to its military policy to prepare for offensive cyber operations in combat. The 2013 edition of *The Science of Military Strategy* advocated ideas about achieving superiority in the space and cyberspace domains.[3] China's Military Strategy, unveiled in 2015, declared cyberspace a new domain of national security and referenced the intense international strategic competition in cyberspace that was under way with the development of cyber military forces.[4] It appears that as early as 2012 China began to deploy offensive cyber capabilities against political adversaries outside the country through mini-campaigns of political-influence-seeking and exploitation of international social media for propaganda. This chapter examines three of those cyber campaigns:

- the anti-independence drive against the Democratic Progressive Party (DPP) in Taiwan
- the 'anti-terrorist' drive against Uighurs
- the consolidation of China's territorial claims in the South China Sea

These campaigns are quite different from those discussed in the United States and Russia chapters. The reason for this is simple: compared to these countries, China has so far conducted offensive cyber operations against quite different types of targets.

By examining these cases studies, the chapter seeks to answer two questions:

- How well has China organised for offensive cyber campaigns?
- How has China used offensive cyber operations for strategic gain?

As noted in the methodology, there is limited information about China's offensive cyber operations. The US government and US-based corporations are the primary sources of information and the data they provide is far from comprehensive. Usually, these sources only contain as much information as serves the purposes of a particular publication – either a political purpose or a business purpose often focused on select technical aspects. Moreover, there is very little information in the public domain about the organisations involved in China's cyber operations and how they interact in the execution of cyber campaigns. In addition, the few

available non-government sources on Chinese organisational factors generally lack corroborating evidence. No Chinese journalistic sources can match the scale and scope of the credible reporting on the United States' cyber operations. There are no significant memoirs on these subjects from retired Chinese officials of the sort seen in the US. These limitations acknowledged, this study can offer some broad generalisations about China's offensive cyber operations.

Organisational setting

In 2000, the organisational setting in China was more attuned for influence-oriented cyber campaigns than sabotage-oriented campaigns.[5] At this time, China was better prepared to conduct influence-oriented campaigns than the US and Russia, a consequence primarily of Beijing's long-standing practice of monitoring and violently repressing unorthodox domestic political thought. Despite a brief window of political liberalisation between 1983 and 1989, China recalled into action its forces of political suppression in June 1989 against student protesters and has retained their services ever since. Suppressive measures were intensified not long after Xi Jinping became general secretary of the Chinese Communist Party (CCP) in 2012. Beijing's preparedness for political-influence campaigns conducted through cyberspace was also buttressed by two equally long-standing CCP institutions, the Propaganda Department and the United Front Work Department, the latter being explicitly designed to persuade foreigners (and Chinese citizens who were not communists) to support or at least not oppose Chinese-government and CCP initiatives. These departments conducted covert operations as well as public-facing activities. They were subject to the same slow process of digital transformation as the rest of China; their cyber-based media only became a significant force on the international stage with the emergence of social-media apps Twitter (2006) and Weibo (2009) and when government promotion of cyber assets began to have a visible impact. While China assigns a high priority to the international mission of political influencing, Beijing feels it has to focus its most capable cyber assets on the task of protecting the CCP rather than on foreign-policy ventures abroad where the agencies have less control. Moreover, as long as China had tried and tested processes for political influence abroad that did not depend on offensive cyber operations, there was less incentive to direct cyber assets to this purpose. Beijing also places a high priority on cyber espionage for theft of state secrets and scientific information because China is relatively backward in some areas of basic science and industrial technologies compared with leading European powers and is militarily less capable than the US. State and industrial secrets are harvested more efficiently by cyber operations than by classic human-intelligence assets. These considerations mean that for CCP leaders there is a sense of urgency around cyber espionage that is absent when it comes to influence-oriented offensive cyber operations.

The CCP has lived and breathed information warfare in political relationships since its founding in 1921. For most of the last decade, its leaders would have been very satisfied with its cyber espionage, quite satisfied with its domestic cyber-influencing activities and so confident of its public diplomacy that they would have seen no need to make changes in favour of influence-oriented offensive cyber operations. However, its less successful performance in these areas since the uprisings in Hong Kong, its genocidal policies towards China's Uighur population and the strategic shock created by its island building in the South China Sea has gradually pushed the leadership to explore the potential of cyber-based influence operations. Chinese leaders will have taken considerable satisfaction and some lessons from the disruptive impacts of Russian cyber-based interventions in the elections of major Western countries.

The Ministry of State Security (MSS) is the main organisation responsible for influence-oriented cyber operations at home and abroad. It operates under the control of the CCP's Political and Legal Commission, whose head is regarded as China's most senior spy (a powerful post normally associated with membership of the inner circle of the CCP Politburo).[6] The People's Liberation Army (PLA) Strategic Support Force (SSF) is the high-level agency that plans and executes military cyber operations (primarily espionage). Established in 2015 one year after Xi's commitment to make China a cyber power, the SSF has a wide range of intelligence and planning functions apart from cyber operations.

The Chinese armed forces began to embrace concepts of information warfare following a series of secret speeches by CMC chairman Jiang Zemin to the commission beginning in 2000. His ideas were reflected in the public writings of Dai Qingmin, a former senior officer of the General Staff. In a series of articles between 2000 and 2003, he proclaimed the upcoming convergence of ground, sea, air, space and electronics into a single battlefield, pioneered the operational concept of 'integrated network electronic warfare'[7] and also highlighted a need to integrate military and civilian forces in the information domain.[8] The 2001 edition of *The Science of Military Strategy*, a key PLA doctrinal publication by the Academy of Military Science, suggested that information warfare would bring all aspects of statecraft within range of attack and involves exerting political, public-opinion and psychological pressure on an adversary to break its will to fight.[9] In 2004, the CMC revised its guidelines on war fighting from winning local wars that might occur under modern (especially high-tech) conditions to winning 'local wars under conditions of informationization'.[10]

The term 'cyber' was first mentioned in defence white papers in 2010, where it was noted that some countries had developed new strategies for cyberspace and enhanced their capabilities to conduct cyber operations in order to occupy the 'commanding heights' in the cyber domain. The 2010 defence white paper also identified maintaining security interests in space, electromagnetic space and cyberspace as a task for China's national defence. Taking note of the unfolding shift in battlefield control from land and sea to space and cyberspace, the 2013 edition of *The Science of Military Strategy* advocated gaining superiority in the space and cyberspace domains.[11]

In 2014, Xi took the lead on national cyber-security initiatives as chairman of the new Small Leading Group on Informatisation and Cyber Security, which is tasked with formulating and implementing national cyber-security and informatisation-development strategies, macro-level plans and policies. Xi called for collective efforts to make China a cyber power. He also prompted the PLA to 'establish a new military doctrine, institutions, equipment systems, strategies and tactics and management modes' for information warfare.[12]

China's 2015 military strategy deemed cyberspace a new domain of national security and highlighted the intense international strategic competition taking place in cyberspace with the development of cyber military forces. The strategy made clear China's intention to expedite the development of its cyber forces to maintain national security and to ensure it was prepared for cyber crises.[13] Soon after its publication, the CMC announced wide-ranging reforms of the PLA, including the creation of the SSF. The reforms were initiated to transform the PLA from a regional-defence-oriented force into a modern combat force. The SSF consolidated China's space-, electronic-, cyber- and information-warfare capabilities, which were dispersed across other departments of the General Staff.[14] The SSF's Network Systems Department unified signals-intelligence, cyber-espionage, electromagnetic-warfare and psychological operations, having mainly inherited the capabilities of the General Staff's third and fourth departments, some of the technical-reconnaissance bureaus from the former military regions, and the psychological operations earlier executed by the former General Political Department.[15]

Policy and strategy documents in the public domain have endorsed the use of the military to secure Chinese interests in cyberspace

The policy and strategy documents in the public domain have endorsed the use of the military to secure Chinese interests in cyberspace. China's National Cyberspace Security Strategy was supportive of military measures, along with others, in the defence of China's sovereignty in cyberspace.[16] The International Strategy of Cooperation on Cyberspace also asserted that the armed forces play a key role in protecting China's sovereignty and other interests in cyberspace.[17] The latter document deemed the enhanced capability of the armed forces in cyberspace – and the building of cyber forces – to be important for China's defence modernisation.

The 2019 defence white paper China's National Defense in the New Era identified safeguarding China's security interests in outer space, electromagnetic space and cyberspace as some of the fundamental goals of China's national defence. It noted that China's armed forces have 'accelerated the building of their cyberspace capabilities consistent with China's international standing and status'.[18] The white paper described the key functions of the SSF as supporting forces in the battlefield and providing information, communications, information security and new technology across the PLA.

Leadership preferences

Xi Jinping is much more engaged than his predecessors in leading China's digital transformation. In 2014, Xi took a lead on cyberspace policy, heading the Small Leading Group, which was renamed to include the policy domain of 'cyber security' as well as the pre-existing function of informatisation.[19] Its mission was and remains macro policy planning in these areas. At the inaugural meeting of the restructured Small Leading Group, Xi called for collective efforts to make China a cyber power. This was followed by a series of structural changes and the publication of strategy documents in both the civilian and military realms. The Cyberspace Administration of China (CAC) was formed as the office of the Small Leading Group, replacing the State Internet Information Office established in 2011. China initiated the annual World Internet Conference in 2014, provisioned the Cybersecurity Law in 2017 and published its National Cyberspace Security Strategy and an International Strategy of Cooperation on Cyberspace in 2016 and 2017 respectively. The Small Leading Group was upgraded and became the Central Cyberspace Affairs Commission (CCAC) as part of institutional reforms in 2018, further consolidating its powers for supervision of cyber policy and regulation of cyberspace.

On the military front, in 2014 Xi had called on the PLA 'to establish a new military doctrine, institutions, equipment systems, strategies and tactics and management modes' for information warfare. With Xi serving as CMC chairman, for the first time in 2015 China published its military strategy in a white paper (titled China's Military Strategy) expressing the intent to develop a cyber force. In December, the CMC initiated wide-ranging reforms to transform the PLA into a modern combat force and dismantled the structure of general departments and military area commands.[20] This also led to the establishment of the SSF.

Xi is more aware of the military and strategic potential of cyber capabilities than any of his predecessors. However, there is insufficient information in the public domain to build a picture of his day-to-day engagement with the ordering or conduct of offensive cyber operations. It might be assumed that he has some engagement in the approval and review of the most sensitive operations. On the other hand, the Chinese leadership's decision-making style favours expressions of general views rather than endorsements of specific action plans. This area of interest remains something of black box.

Anti-independence drive against the Democratic Progressive Party in Taiwan

Since the retreat of Chiang Kai-shek and Kuomintang (KMT) forces to Taiwan in 1949, the CCP has seen reunification (and defeat of the separate political identity of Taiwan) as its primary goal. In operational terms, Beijing's reunification policies (and the urgency with which it has sought to enact them) have varied according to international circumstances and leadership preferences. For instance, in 1950, as Mao Zedong was preparing for the invasion of Taiwan, his decision to intervene in the Korean War forced China to defer the final assault against the KMT forces in Taiwan.

Since then, China has employed most of the traditional instruments of statecraft (diplomacy, military pressure and economic incentives) to advance its geopolitical objectives. Evidence suggests that since the late 1990s China has often resorted to cyber means to achieve selected near-term objectives. Moreover, cyber options became more important once the role of military force in cross-strait relations was downgraded. (There was a shift from a tougher approach during the presidency of Jiang Zemin towards a more moderate approach under Hu Jintao, whose presidency oversaw a reduction in military tensions between China and Taiwan.[21]) The greater focus on cyber means was also visible in two defence white papers published in 2008 and 2010.[22] Xi has taken

a tough stance to curb separatist forces but simultaneously professed a desire to expand cross-strait economic and cultural exchanges, connectivity and cooperation.[23] Though China has never renounced its right to use force to achieve reunification, there has been a reduced reliance on force in practice. However, the situation may be changing at the time of writing as China has increased the frequency and extended the operating areas of some military activities around Taiwan or Taiwan-held territory, such as the Pratas Islands in the northeast of the South China Sea.

The political imperative was captured in the 2001 edition of China's *The Science of Military Strategy*, which stated that reunification was necessary to ensure China's national sovereignty and territorial integrity, cautioning that 'the independence of Taiwan' equated to war and that separatism was a direct threat to peace. It also recognised the Taiwan issue as the greatest and final obstacle in China's path to rejuvenation.[24] In 2015, China's Military Strategy echoed these sentiments, identifying the continuing 'clamour' of pro-independence voices in Taiwan as proof that the root cause of instability was yet to be removed.[25] In his address at the CCP's 19th Party Congress in 2017, Xi stated: 'We have the resolve, the confidence, and the ability to defeat separatist attempts for "Taiwan independence" in any form.'[26] In July 2021, on the centenary of the CCP's founding, Xi made what was seen by some observers as an even firmer commitment to reunification.[27]

Since 1949, China has repeatedly used a mix of coercive and non-coercive measures in a campaign to coax Taiwan to abandon efforts towards independence

Since 1949, China has repeatedly used a mix of coercive and non-coercive measures in a campaign to coax Taiwan to abandon efforts towards independence and to change the status quo in Beijing's favour. Following Taiwan's democratisation in the mid-1990s, impeding its system of governance became an equally important Chinese goal. For example, in 1995 and 1996, ahead of Taiwan's first presidential elections, the PLA conducted a series of exercises to display its military might and coerce Taiwan from moving towards democracy and independence. By March 1996, Taiwan had its first democratically elected president, the KMT leader, whose party formally held to the 'one-China' policy and supported eventual reunification with the mainland (although the new president also affirmed that the Republic of China was the legitimate government, at least of Taiwan, and that Taiwan was an independent state.[28]) Therefore, China's major dispute is with the KMT's political rival, the DPP, which strongly favours Taiwan's *de jure* independence and rejects China's 'one country, two systems' formula. The DPP's 1991 charter declared one of its goals to be the establishment of a sovereign and independent Republic of Taiwan, while later DPP resolutions – the 1999 Resolution on Taiwan's Future and the 2007 Resolution on Normalization of the Nation – have asserted that Taiwan is already a sovereign and independent nation.[29]

The DPP came to power in 2000 with the election of president Chen Shui-bian. Four years later, Beijing's white paper China's National Defense in 2004 assessed the situation in Taiwan to be 'grim' as Taipei had begun to escalate the issue of Taiwan's independence.[30] Chen was re-elected in 2004, prompting China to pass its Anti-Secession Law in 2005, which explicitly stated that China reserves the right to employ 'non-peaceful means' in the event of Taiwan's secession from China.[31] Elections in 2008 returned the KMT to power, with the new president, Ma Ying-jeou, remaining in office until 2016. This period saw rapprochement and warmer relations with Beijing as Ma promised 'no reunification, no independence, and no war' with China in his inaugural address.[32] Ma's term also saw a leadership transition in China, with Xi becoming CCP general secretary in 2012 and president of China in 2013. In 2015, Xi and Ma held a historic summit in Singapore, the first meeting of CCP and KMT leaders since the founding of the People's Republic of China in 1949. The meeting was symbolic of improving relations.

2015 was also a turning point of sorts, as Beijing came to take a much tougher stance against what it called

separatism in Hong Kong, Taiwan, Tibet and Xinjiang. As CMC chairman, Xi had called on the PLA to develop a new strategy for 'information warfare'[33] and oversaw the consolidation of the PLA's space-, electronic-, cyber- and information-warfare capabilities under the SSF as part of the wide-ranging military and national-defence reforms initiated in December 2015.[34] Following the emergence of the Sunflower movement in Taiwan – a series of protests primarily led by students and civil-society activists in opposition to closer economic integration with China – the DPP returned to power in 2016.[35] To China's dismay, the party retained power in the 2020 presidential elections – an outcome in part the result of negative reactions in Taiwan to China's forceful repression of protesters in Hong Kong and its repudiation of the principle of 'one country, two systems', which had

Table 4.1: **China's cyber operations against the DPP, 1996–2021**

Date	Targets | methods | likely purposes
1996	Taiwanese websites | malware, defacement | to oppose Taiwan's first presidential election
Aug 1999	Taiwanese government, university and commercial websites | malware, defacement | to retaliate against a statement by then Taiwanese president Lee Teng-hui, who referred to cross-strait relations as a 'special state-to-state relationship'
2003	Several dozen Taiwanese government agencies and large Taiwanese companies | malware | espionage
2004	Defacement of DPP website | malware, defacement | to retaliate against the re-election of president Chen Shui-bian
2005	National Security Council of Taiwan | spear-phishing | espionage
2011	Email accounts of DPP officials and senior staff (members of Tsai Ing-wen's presidential campaign) | malware | to steal campaign information
Sep 2013	Government agencies, think tanks and corporations (primarily those with interests in Taiwan) | spear-phishing, 'Taidoor' malware | espionage
Oct 2013	Taiwanese entities | Terminator remote-access tool | espionage
Nov–Dec 2015	Taiwanese organisations, including financial services, high-tech, media and government services | spear-phishing | espionage
Dec 2015	Email accounts of DPP staff | spear-phishing | to steal information before the Taiwanese general election
Apr 2016	DPP's website | malware, spoofing | to profile website visitors for future cyber attacks
2018	Taiwanese public | disinformation campaigns against DPP mayoral candidate for Kaohsiung Chen Chi-Mai on social-media applications such as PTT Bulletin Board System, Facebook, Weibo and Line | discredit the DPP candidate and undermine his election chances
2018–20	At least ten government agencies and 6,000 government official's email accounts | malware against loopholes in the Taiwan government's information service providers | espionage
Dec 2019	Taiwanese public | disinformation against President Tsai Ing-wen (22 websites linked to the Taiwan Affairs Office of the State Council of China) | to undermine Tsai Ing-wen's re-election bid in the 2020 election
2019–20	Taiwanese public | cross-platform disinformation across Facebook, Twitter, Instagram, YouTube, PTT and Line, content farms in Malaysia | to discredit Tsai Ing-wen and her government while promoting KMT candidate Han Kuo-yu, deter voting during the 2020 presidential election, increase social tensions within the Taiwanese population through amplifying political and generational divides
May 2020	Taiwan's Presidential Office, Taiwanese public | phishing, disinformation using hacked internal documents | to undermine Tsai Ing-wen's reputation, integrity and legitimacy days before she is sworn in for a second term
May 2020	CPC Corporation (state-owned refiner in Taiwan) | malware | to disrupt CPC Corporation systems by causing them to lose the ability to process customers' electronic payments
Dec 2020	Taiwanese public | disinformation about US-imported pork | to undermine the Tsai Ing-wen government
Feb 2021	Taiwanese public | training programmes for cultivating online celebrities and e-commerce live broadcasters from Taiwan (Taiwanese businessmen, youths, compatriots and spouses of Chinese mainland citizens) | to leverage Taiwanese online influencers as propaganda tools to promote China's narratives and influence public opinion in Taiwan
Apr 2021	Taiwanese public | disinformation asserting the Taiwanese government planned to accept contaminated wastewater from Japan's nuclear power plant in Fukushima | to increase public mistrust of the DPP and strain the Japan–Taiwan relationship
May 2021	Taiwanese public | disinformation that the US was 'not selling Taipei a single vial of vaccine' | to increase public distrust of Tsai Ing-wen's government
May 2021	Taiwanese public | disinformation claiming Tsai Ing-wen had been infected with COVID-19 amid a government cover-up | to trigger panic in Taiwanese society and decrease government legitimacy
Jun 2021	Taiwanese public | disinformation regarding the government's mishandling of the COVID-19 vaccination programme and the health implications of vaccines (first introduced through private groups on Line or PTT and subsequently to Taiwanese mainstream media) | to undermine government legitimacy and create panic
Jun 2021	National Development Fund in the Executive Yuan (responsible for domestic industrial innovation and spurring overall economic growth) | malware | espionage seeking corporate information

Sources: Al Jazeera, www.aljazeera.com; Bloomberg, www.bloomberg.com; Centre for New American Security, www.cnas.org; *China Times*, www.chinatimes.com. CNA, www.cna.com; CNN, edition.cnn.com; *Financial Times*, www.ft.com; FireEye, www.fireeye.com; Global Taiwan Institute, globaltaiwan.org; Graphika, graphika.com; *Guardian*, www.guardian.co.uk; Institute for the Future, www.iftf.org; International Republican Institute, www.iri.org; Jamestown Foundation, www.jamestown.org; Jayson M. Spade, *Information as Power: China's Cyber Power and America's National Security* (Pennsylvania: US Army War College, 2012); Mandiant, www.mandiant.com; National Bureau of Asian Research, www.nbr.org; New Bloom, newbloommag.net; *New York Times*, www.nytimes.com; Reuters, www.reuters.com; Security Challenges (Institute for Regional Security, regionalsecurity.org.au); *Straits Times*, www.straitstimes.com; Strategic Insights; *Taipei Times*, www.taipeitimes.com; Taiwan News, www.taiwannews.com; Wenhuibao, paper.wenweipo.com.
Note: The likely purposes of the operations are those identified by the sources cited.

been held up as a possible model for the reunification of Taiwan and China.

China's offensive cyber operations have aimed to discredit the DPP and shore up the KMT. Table 4.1 provides a brief timeline of some of the more prominent cyber attacks against Taiwan and information operations contributing to China's campaign against the DPP. (Not all of these meet this report's definition of offensive cyber operations.)

Since the mid-1990s, Taiwan has been the target of incessant politically motivated Chinese cyber attacks and information operations. Low-level website defacements began in 1996 in response to the presidential elections, and later in retaliation for a statement made by then-president Lee Teng-hui referring to cross-strait relations as a 'special state-to-state relationship'.[36]

Later Chinese cyber attacks targeted government computer networks, such as the Ministry of National Defense, National Security Bureau and National Security Council; public services and private-sector organisations, including telecom-service providers;[37] and, more recently, the semiconductor industry.[38] Top government officials and lawmakers are more prone to targeted cyber attacks.[39] Low-level disruption and information theft were the primary aims of the attacks,[40] while website defacements could better be categorised as mere nuisance. These incidents were reported as early as 2000 and 2004,[41] again in 2011,[42] continually throughout the 2016 elections,[43] after elections when the DPP came into power,[44] during the 2018 local elections[45] and during the 2020 general elections. The intensity of these attacks has generally increased in the lead-up to local or general elections in Taiwan.

More seriously, China has conducted cyber-based disinformation campaigns and election interference – modelled on Russia's intervention in the 2016 US presidential elections – that have had a much greater impact on Taiwanese democracy. The 2019 Annual Democracy Report produced by the V-Dem Institute found that Taiwan's democracy is one of the most affected by foreign online disinformation campaigns, with false and misleading information originating mainly from China being spread via social media and traditional media outlets.[46] Taiwan is the primary target of China's cyber-enabled election interference, with President Tsai Ing-wen and the DPP receiving the most attention.[47]

Beijing seeks to shift Taiwanese public opinion in its favour by cultivating factions or groups there sympathetic to China's vision for cross-strait relations. Other near-term objectives are to pressure opponents of China's vision to submit to its will and to exacerbate feelings of abandonment or isolation in Taiwanese society.[48] These goals are intended to facilitate China's long-term geopolitical objectives: to extinguish the very idea of an independent Taiwan and facilitate its deeper economic and cultural integration with China.

China's cyber-influence operations were evident during Kaohsiung City's mayoral elections in 2018, when an information campaign and mobilisation of support for candidate Han Kuo-yu saw him receive unprecedented coverage in pro-China television channels and ultimately facilitated his meteoric rise and eventual victory. Beijing also uses established Taiwanese media outlets to influence political sentiment in Taiwan, such as Want China Times Media Group, whose content is coordinated with the Taiwan Affairs Office of the State Council of China.[49] In the build-up to the 2018 local elections, DPP candidate Chen Chi-mai was targeted by disinformation campaigns on the PTT Bulletin Board System, social-media platforms (Facebook), micro-blogging services (Weibo) and messaging applications (Line).[50] Wang Liqiang, an alleged Chinese spy who defected to Australia in November 2019, reported that China had meddled in the 2018 local elections in Taiwan to back Han and had been preparing to repeat its activities during the 2020 national elections with the aim of toppling DPP candidates, including incumbent president Tsai Ing-wen.[51] China's strategy appeared to have worked in 2018 – Kaohsiung was previously a DPP stronghold for over two decades – and Han went on to be the KMT candidate in the 2020 presidential election. In sum, China's disinformation campaigns against the DPP have spared no effort with a view to facilitating its broader geopolitical objectives.

One 'fake news' story disseminated in 2018 claimed that Taiwan's representative office in Japan had failed to help Taiwanese people trapped at Kansai International Airport in Osaka when Typhoon Jebi hit the city.[52] The story, which claimed that the Chinese Consulate-General

in Osaka had helped evacuate '32 Taiwan compatriots', was spread by PTT users in China[53] and initially posted on Chinese news websites.[54] It was later picked up by Taiwanese social-media platforms without being fact-checked.[55] A dismayed Taiwan representative in Osaka later committed suicide following the false allegations.[56] In essence, the entire disinformation campaign intended to convey the message that the DPP-led government had failed to protect its citizens. In fact, these incidents gave the DPP additional impetus to defend itself and Taiwan from China's cyber and disinformation campaigns as it prepared for the 2020 presidential elections.

The deluge of disinformation continued in the run-up to the elections. Ahead of the elections DPP researchers identified 22 websites in Taiwan engaged in disinformation with alleged ties to the Taiwan Affairs Office of the State Council of China. Taiwanese researchers analysed the spread of disinformation from China to unearth networks producing and amplifying content and manipulating opinion on social media, as well as the 'subliminal attacks' or search boosters that placed content at the top of search-engine indexes to ensure greater visibility.[57] The elections also witnessed the use of artificial intelligence (AI) to produce and disseminate content augmenting the disinformation campaigns.[58] Taiwan was able to thwart the disinformation campaigns through heightened defences, enhanced institutional response and awareness and close coordination with social-media platforms. Tsai received 57.1% of the vote and Han 38.61%, with the incumbent president receiving more votes and a wider margin of victory than in 2016.[59]

Cyber-enabled election interference delegitimises the DPP-led government by stoking accusations that it is stifling dissent and by exaggerating claims of electoral interference for political purposes.[60] Cyber operations fit neatly into Beijing's long-term campaign to pressure political parties antagonistic to China's vision for cross-strait relations to submit to its will and also to mould a favourable public opinion in Taiwanese society – especially since the role of military force has been downplayed. Cyber operations have been employed in conjunction with so-called 'non-cyber' measures, such as isolating Taiwan diplomatically, pressuring others to adopt Beijing-specified nomenclature about Taiwan or placing restrictions on tourism.[61] The effectiveness of this campaign is evaluated in the final section of this chapter.

There have been few reports of cyber sabotage by China against Taiwan's critical infrastructure or IT networks and systems. Unlike Russia's offensive cyber operations in Ukraine, China does not appear to have reached for cyber-sabotage tools to achieve political goals, perhaps because it sees little need, or it believes such attacks would be politically damaging to its interests.

Campaign summary

The primary lines of effort of China's anti-independence drive against the DPP are:

- persistent and long-term cyber espionage against Taiwanese government agencies, political targets and corporations, including companies linked to the government
- election interference through disinformation campaigns, augmented by intensified cyber espionage to undermine the DPP and delegitimise its political candidates while supporting preferred candidates
- defacement of government websites to signal displeasure with political events in Taiwan

The political significance of any 'use of force' in relation to the cross-strait dynamic elevates the importance of cyber operations for Beijing since they serve as a non-lethal instrument of statecraft against Taiwan (as long as China does not cross a threshold in cyber operations that Taiwan or the US could regard as a 'use of force'). While the use of traditional kinetic instruments of coercion can be directly attributed to China, cyber options may allow Beijing to maintain plausible deniability long enough to achieve certain strategic effects.

One observation arising from this analysis is Taiwan's heightening of defences in light of incessant offensive cyber and information campaigns. Since 2001, the Taiwanese government has initiated five iterations of the National Cyber Security Program. Organisational and legal measures (such as the establishment of the Department of Cyber Security in 2016 and the entry into force of the Anti-Infiltration Act and Cyber Security

Management Act in 2019) enacted under the DPP-led government, coupled with proactive fact-checking and counter-narrative development, intend to make Taiwanese society resilient to cyber-enabled interference in the electoral processes.

'Anti-terrorist' drive against Uighurs

Beijing is embroiled in a protracted conflict with China's Uighur ethnic minority as a result of its efforts to assimilate the population under a Han Chinese identity and to defeat an established, if ineffective, separatist movement in the Uighur community. In 1996, China introduced a 'Strike Hard campaign' targeting regions with communities harbouring separatist sympathies (and members of these communities living in other parts of China). The campaign imposed stringent restrictions on cultural expression and religious practice, which were perceived by Uighurs as a threat to their faith and cultural identity.[62] Uighur demands for equality, religious freedom and political autonomy eventually gained momentum but also turned increasingly violent.

The movement took the form of an armed revolt, conducting terrorist attacks and bomb attacks in Xinjiang and later in other parts of China. Prominent incidents included the 1990 Baren Township riots; 1992 and 1997 Ürümqi bus bombings;[63] 2009 Ürümqi riots;[64] 2013 Tiananmen Square terror attack;[65] 2014 street-market attack in Ürümqi;[66] 2014 knife attack and bombings at Ürümqi railway station;[67] and the 2014 knife attack at Kunming railway station in China's south, where there are smaller Muslim communities.[68] The perceived threat from this broad opposition movement – often equated incorrectly with the East Turkestan Islamic Movement (ETIM), which is just one manifestation of the resistance – was first mentioned in the defence white paper China's National Defense in 2008.[69] China's Military Strategy (2015) noted that separatist forces seeking East Turkestan independence had inflicted serious damage, particularly through escalating violent terrorist activities.[70]

Xi Jinping, who had to respond to major attacks early in his presidency (Tiananmen Square 2013; Ürümqi 2014; Kunming 2014) has adopted a tough stance on separatist movements, whether in Taiwan, Tibet or Xinjiang. In May 2014, China launched an upgraded 'Strike Hard Campaign against Violent Terrorism' in Xinjiang.[71] It was further strengthened by the Counter-Terrorism Law, which came into effect in early 2016 and established a framework for designating, investigating and preventing terrorism.[72] Following the appointment of Chen Quanguo – the CCP secretary of Tibet – as secretary of Xinjiang Uyghur Autonomous Region in 2016, a slew of repressive counter-terrorism measures were introduced to stabilise Xinjiang. These included increased surveillance, excessive force deployment, facial recognition, mass detention and ideological re-education. Cyber espionage and information operations were also expanded against Uighurs in Xinjiang as well as the diaspora spread across the world.

From 2016, cyber espionage and information operations were expanded against Uighurs in Xinjiang as well as the diaspora

An early instance of cyber espionage against Uighur dissidents dates to the late 1990s and early 2000s,[73] but more reports began to emerge towards the late 2000s as the Uighur movement gained traction. Phishing and later spear-phishing attacks targeted email communications; one instance of hacking of Hotmail accounts belonging to Uighur leaders was traced back to 2009.[74] A campaign began targeting Uighur activists using MacOS exploits from 2012.[75] (The majority of previous attacks had been against Windows operating systems, though attacks on Windows continued to be reported.[76]) With the growing adoption of mobile phones, attacks targeting mobile platforms began to emerge from 2013. One such attack targeted Android OS and stole data from contacts, call logs, messages and other telephone details.[77] With the launch of the augmented Strike Hard campaign in 2014, the development of malware targeting the Uighur population and diaspora also gained pace.

In 2016, an investigation by cyber-security company Palo Alto Networks identified malware with

the primary mission of gathering information about minority-rights activists. It was mainly targeting Uighur and Tibetan activists and those interested in their causes.[78] In 2018, the company exposed an Android malware family, 'HenBox', that was masquerading as legitimate apps (virtual private networks (VPN) and privacy-enabling apps used by Uighurs, as well as other apps in the Uighur language). They primarily target Uighurs to steal from compromised devices information related to chat, communication, location and social-media apps.[79]

In 2019, another cyber-security company, Cybereason, revealed a major state-backed hacking operation, allegedly of Chinese origin, targeting global telecommunications providers. Through gaining access to the providers' billing systems, it sought to acquire users' call-data records and location and personal information. Active since 2017, it impacted some ten telecoms operators around the world and stood apart from other operations as it targeted the critical infrastructure of other countries.[80] Between mid-2019 and mid-2020, other cyber-security organisations (Google's Threat Analysis Group,[81] Volexity[82] and the Citizen Lab[83]) made overlapping discoveries of malware that had targeted Uighurs' and Tibetans' iPhones and Android phones for the previous two years. Delivered through compromised Uighur and East Turkestan websites and targeting mobile devices, the malware was designed to access end-to-end encrypted apps like WhatsApp, Telegram and iMessage, as well as emails from Gmail accounts, bypassing two-factor authentication. It aimed to steal files and upload live location data, indicating that its prime objective was to track the Uighur diaspora's movements and gather details about its communications. The fact that different strains of malware were detected by different threat-analysis teams at different points in time indicates the sheer scale of the operation. Putting all of the pieces together and analysing the command-and-control infrastructure, the Citizen Lab later concluded that it is likely the campaigns were conducted by the same operator or a coordinated group of operators with shared resources. The common link was the targets – China's Uighur and Tibetan ethnic minorities. In early 2020 Volexity again observed new activity across previously compromised Uighur websites.[84]

In mid-2020, cyber-security firm Lookout revealed that it had discovered four Android malware families ('SilkBean', 'DoubleAgent', 'CarbonSteal' and 'GoldenEagle') with overlapping command-and-control infrastructure used for surveillance of Uighurs (through websites and third-party-app stores that serve Uighur-focused applications). Some of the campaigns dated back to 2013.[85] It also observed that the development timelines of these families broadly coincided with developments in China's security landscape – especially the counter-terrorism efforts that followed the Strike Hard campaign in Xinjiang and the passing of the National Security Law and the Counter-Terrorism Law – underscoring the possibility that the campaign had a strategic objective. Also in 2020, Trend Micro discovered a malware that had been impersonating legitimate Uighur video app Ekran for three years.[86] Table 4.2 summarises the cyber operations contributing to China's campaign against Uighurs.

The primary motive of cyber operations against Uighurs appears to have been espionage for the purposes of repression and control

The primary motive of these operations appears to have been espionage for the purposes of repression and control. It is evident that malware targeting the Uighurs tends to seek information about the social contacts of the targeted individuals, intimate details about their communications and their whereabouts or movements. However, there is an apparent political motive behind the espionage operations. As far as the Uighur movement is concerned, Beijing's near-term geopolitical objective is to end the violence, which predominantly targets the Han population and Chinese government agencies. Additionally, Beijing seeks to deter activists of the Uighur and East Turkestan movements (which China conflates) from engaging in activities that could undermine its control in Xinjiang and to ultimately

Table 4.2: **China's cyber operations against Uighurs, 2002–21**

Date	Targets | methods | likely purposes
2002	Uighur dissident groups based overseas | spear-phishing | espionage
2009–11	Hotmail accounts belonging to international leaders of China's Uighur and Tibetan minorities | malware | espionage and possible coercion
2012–13	Uighurs and Tibetans using Mac and Android OS, World Uighur Congress | spear-phishing, MacOS and Android OS exploits | espionage
2016	Uighur and Tibetan activists and their supporters | spear-phishing, watering-hole attacks, Windows, Mac OS X and Android OS exploits | espionage
2018	VPN and Android system apps used by Uighurs (such as Uighur-language keyboard app) | Android OS malware ('HenBox') | to steal location data and information from chats and social-media apps, cameras and microphones of infected devices
2019	Global telecommunications-service providers | 'hTran' malware | to gain access to users' call-data records, location and personal information
2019–20	iPhones and Android mobile devices belonging to Uighurs and Tibetans globally | watering-hole attacks, malware (via compromised Uighur and East Turkestan websites) | to track movement and gain access to communications of the Uighur diaspora
2019–21	International audience | disinformation campaigns on Western social media (Facebook, Instagram, YouTube, Twitter) and on Chinese social media (TikTok) - including paying for ads to promote state propaganda, censorship of negative content about Xinjiang (on TikTok) | to win the public-opinion struggle through undermining independent investigations of Xinjiang and silencing critics of Beijing's Xinjiang policies, salvage its international reputation
Mid-2020	Mainly Uighurs in China and the Uighur diaspora | four Android malware families (through Uighur-targeted third-party-app stores and websites | espionage against Uighurs in China and the Uighur diaspora
2020–21	Small group of Uighurs in Xinjiang and Pakistan | phishing using fake United Nations documents and human-rights websites | espionage against Uighur minority and organisations supporting them (no clear attribution to China, attribution to a Chinese-speaking threat actor is of low to medium confidence)
Feb 2021	International audience | disinformation campaign against the BBC using state media and diplomatic accounts on Twitter, Facebook and YouTube | to discredit a BBC show that aired a report featuring Uighur women reporting on detainees in Xinjiang camps; and to distract the international audience away from its activities in Xinjiang while regaining control of the narrative
Mar 2021	Uighur diaspora (activists, journalists and dissidents) | malware, watering-hole attack, spear-phishing | espionage to identify targets and enable surveillance
2021	International audience | disinformation campaign via Western social-media platforms, including incorporating a wider group of pro-CCP individuals, such as influencers and other proxies, into its network and portraying them as organic content | to retaliate against specific allegations (e.g., Mike Pompeo's declaration of genocide in Xinjiang on 19 January 2021, and international clothing brands such as H&M for their allegations of labour abuse), deflect attention from criticisms of Xinjiang policies, promote positive narratives of life in Xinjiang, propose alternative views to concepts such as human rights

Sources: AT&T Cybersecurity, cybersecurity.att.com; Australian Strategic Policy Institute, www.aspi.org.au; *Bangkok Post*, www.bangkokpost.com; Bloomberg, www.bloomberg.com; Check Point, blog.checkpoint.com; Citizen Lab, citizenlab.ca; Cybereason, www.cybereason.com; Lookout Threat Intelligence, www.lookout.com; *New York Times*, www.nytimes.com; Palo Alto Networks, unit42.paloaltonetworks.com; Press Gazette, pressgazette.co.uk; Project Zero (Google), googleprojectzero.blogspot.com; Reuters, www.reuters.com; Securelist, securelistcom; *South China Morning Post*, www.scmp.com; Uyghur Human Rights Project, uhrp.org; Volexity, www.volexity.com.
Note: The likely purposes of the operations are those identified by the sources cited.

coerce them to abandon the movement. Isolating the Uighur movement and denying it international support is another of Beijing's near-term geopolitical objectives (the endeavour to label the movement as a 'terrorist' movement is a step in that direction).

China's cyber operations extend beyond its borders, targeting Uighur activists in exile or the Uighur diaspora over whom China has limited control compared to the domestic Uighur population, which is subject to excessive surveillance. The true impact of these cyber operations is far-reaching and goes beyond espionage and information gathering. They severely restrict activists' ability to make effective use of freely available communication media and other online tools for communication and dissemination of information, such as news portals and apps, which are known to be subject to watering-hole attacks. These operations further restrict their ability to communicate with the wider public and especially those sympathetic to their cause. The operations could also be seen as a 'form of repression' transcending national boundaries to constrain activists from exercising the civil liberties and political freedoms guaranteed by the democratic countries in which they live.[87] Given the deluge of phishing and spear-phishing attacks the threat of intrusion through malware always looms large, stifling activists' exchange of documents and content. The incessant targeting of activists across all the popular communication platforms, be it emails or messaging applications, makes it difficult to trust unknown individuals, likely limiting the expansion of activist networks. Moreover, it impedes cooperation with international organisations, journalists and media, as well as human-rights activists and non-governmental organisations that could actually help to aggregate Uighur voices against the oppression they experience in China. Rampant

cyber threats actually raise the costs for Uighur activist groups (who, like other activist groups, have limited financial resources) as they have to invest in technology and security consultancy to heighten their defences. Cyber operations are a rewarding option for China, enabling it to penetrate the Uighur diaspora to identify individuals politically active in the separatist movement or critical of the Chinese government and use the information collected to coerce them to cease their activities or silence critical voices. In aggregate, it exerts pressure on the Uighur diaspora and its transnational social and mobilisation networks to abandon the movement. China's information operations, over and above, strive to prevent access to accurate information on the present situation in Xinjiang and label the Uighur activists as 'terrorists' to discredit the entire independence movement for East Turkestan and deny it international support, sympathy and visibility.

One observation arising from analysis of this case study relates to the publicly available information available on China's cyber operations targeting Uighurs. This information is much more detailed compared to that available about Chinese operations targeting state or government targets. It is supported by exhaustive technical analyses and evidence, as several threat-analysis companies and groups have worked closely with the targeted activist groups to expose the cyber operations, explaining the functioning of the malware, details of their command-and-control infrastructure and their tactics and procedures and thereby facilitating their attribution – mostly to China-based threat actors or Chinese state-backed advanced persistent threat (APT) actors.

Campaign summary

The primary lines of effort of China's 'anti-terrorist' drive against Uighurs are:

- long-term cyber espionage against the Uighur diaspora through interception of all prevalent communication platforms to identify political activists and dissidents for subsequent coercion to cease activities
- information operations through designating Uighur activists as terrorists and their independence movement as a terrorist movement

Consolidation of China's territorial claims in the South China Sea

China claims as sovereign territory three groups of island features in the South China Sea (the Paracel Islands, Spratly Islands and Pratas Islands) and the Macclesfield Bank (a submerged feature).[88] Its claims date from the early twentieth century and not, as China purports, from time immemorial. For example, the earliest Chinese claims to the Paracel Islands and the Spratly Islands seemed to arise in 1902 and 1943 respectively.[89] The claims are complicated by several geopolitical considerations and international law. One of the most challenging is the fact that the claims were first made by the Republic of China (ROC) government, which was subsequently driven from the mainland following 22 years of intermittent civil war with the CCP, which then formed the People's Republic of China (PRC) in 1949. Seeing itself as the successor state to the ROC, China (the PRC) makes no territorial claim in the South China Sea that was not already asserted in 1949. There are many complicated legal considerations in the disputes over these territorial claims but in essence, as early as 1943, China's wartime allies (France, the United Kingdom and the US) could not agree to explicitly recognise the Chinese claims because of balance-of-power considerations in the strategically important area, including their own colonial interests in Southeast Asia.[90] China's position was further complicated by the fact that its forces did not control any of the disputed island groups until 1974 – when it forcibly evicted South Vietnamese troops from the Paracel Islands – while the ROC government in Taiwan has controlled at least one island of the Spratly group since 1946 (Itu Aba).

The strategic picture became even more complicated in the 1970s, as the Third United Nations Conference on the Law of the Sea debated new legal regimes for maritime-resource jurisdiction. It was in this period that the Philippines and Malaysia moved towards their first territorial claims of the disputed Spratly group (as defined by China, the ROC and Vietnam). These claims challenged those of China, as well as those of the ROC and Vietnam.

China sees Japan's surrender of sovereignty over the island groups in peace treaties marking the end of the Second World War as evidence of China's sovereignty,

won by blood sacrifice during the brutal Japanese invasion and the long-running second Sino-Japanese War (which the CCP recognises as occurring 1931–45). There is no segment of Chinese opinion that sees the Chinese claims as unjustified, excessive or illegitimate. In 1986, CCP secretary general Hu Yaobang (considered one of China's more liberal leaders) visited the Paracel Islands before China had any physical presence in the Spratly Islands (apart from Taiwan's occupation of one island). Hu declared that the Spratly Islands were immutable Chinese territory.

The disputes about maritime-resource jurisdiction that were already in play pushed China to begin establishing a physical military presence on several submerged features of the Spratly Islands in 1988 (all natural islands had been physically occupied during the 1970s by other claimants). By 2021, following complex diplomatic and strategic bargaining – involving the claimants, the Association of Southeast Asian Nations (ASEAN), Australia, India, Japan, the US and even the UK – China's position had hardened considerably. The extent of China's hostile actions had been tempered previously by its desire to maintain at least a semblance of cooperative relations with ASEAN members. This impulse waxed and waned between 1999 and 2021, but at no point in this period did China feel a need to use military force to displace rival claimants from occupied features. However, it did increasingly make known its displeasure through dramatic measures, such as the construction of military airfields on new artificial islands beginning in 2014, and stepped up military and coastguard patrols to challenge the access of foreign military vessels and fishing boats, as well as harass oil-drilling platforms. By the end of 2020, China had outraged Indonesia with its escalating implied claims to maritime resources in the Indonesian exclusive economic zone (EEZ) off Natuna Island. Also in 2020, China had its first confrontation with Malaysia over potential oil drilling on one of the disputed reefs. In 2021, China stepped up its harassment of Malaysian activities in disputed areas.

One of China's strategies is to use naval exercises to increase its military presence in the region. In 2020 it held at least three military drills near the Paracel Islands and conducted simultaneous exercises along its entire maritime periphery, including in the South China Sea.[91] China also fired two carrier-killer missiles into the sea and performed bomber-attack exercises in response to increased US military presence.[92] These moves not only help to boost China's presence in the region but also signal its military might and combat readiness. China combines these maritime exercises with diplomatic pressure to achieve specific objectives. For example, in 2017 Vietnam's state-owned company PetroVietnam was forced to abruptly terminate a drilling operation conducted jointly with its Spanish partner following Chinese pressure.[93] The intimidation included deployment of an aircraft carrier flanked by at least 40 ships and submarines near the coast of Hainan, just two days' sailing from the drilling site.[94]

Chinese grey-area tactics involve a psychological element, testing an adversary's will and power to maintain its claims

A second Chinese strategy is to use grey-zone tactics to gradually and systemically boost the legitimacy of its claims. These tactics are also known as 'salami-slicing' and involve a 'slow accumulation of small actions' to impact a strategic change without any individual action crossing the threshold of war.[95] A Chinese maritime-strategy expert acknowledged the value of grey-zone tactics in a recent analysis, stating that the PLA Navy (PLAN) and other maritime forces (especially the Naval Militia[96]) have proven their value in slowing down territorial infringements by other countries and keeping conflict at a low level of intensity.[97] Chinese grey-area tactics involve a psychological element, testing an adversary's will and power to maintain its claims.

China has also created artificial islands and equipped them with military assets, including aircraft hangars, radar and barracks facilities and surface-to-air missiles. Fiery Cross Reef, once a small coral reef in the disputed Spratly Islands, has been transformed by China into one of the 'most advanced' artificial bases in the South

China Sea, ten times its original size and equipped with missile launchers and a runway.[98] China also built an extensive undersea surveillance network, ostensibly for civilian purposes.[99]

China's maritime operations in recent years have also focused on harassing oil and gas development by Southeast Asian countries within contested areas. In October 2019, Petronas, a Malaysian state-owned company, sent the *West Capella* to operate in a disputed oil and gas block claimed by China, Malaysia and Vietnam. In response, China deployed coastguard vessels and maritime militia to perform intimidation operations that lasted more than three months.[100] In April 2020, China escalated the situation by deploying *Haiyang Dizhi* 8, the same vessel used to harass Vietnamese ships undertaking oil-exploration works in July–October 2019,[101] which eventually caused the *West Capella* to leave the disputed waters.

China also capitalises on its economic relationships with its rivals to pressure and motivate them to accept – or at least not contest – Chinese claims and activity in the disputed areas. In a stand-off with the Philippines in the Scarborough Shoal in 2012, Beijing retaliated by imposing bans on bananas exported by the Philippines, causing many banana traders to file for bankruptcy.[102] When in 2016 the Permanent Court of Arbitration (PCA) found in favour of the Philippines in a case related to China's expansive claim, the former kept its silence regarding the ruling following Chinese economic enticement of US$13.5 billion in deals.[103]

Despite Beijing's efforts, littoral states have been more vocal in calling out Chinese intimidation. On the fourth anniversary of the PCA ruling, the Philippines announced its first official acknowledgement of the outcome of the award, reflecting a broader hardening of its stance against China's claims.[104] Following the withdrawal of the *West Capella*, in July 2020 Malaysia sent a diplomatic note to the UN to reinforce its application to pursue its rights as a coastal state under the UN Convention on the Law of the Sea (UNCLOS) and also rebuke China's previous dismissal of its claimed rights.[105] Similarly, after a Chinese surveillance vessel sank a Vietnamese fishing boat carrying eight fishermen near the Paracel Islands in April 2020, Hanoi filed a diplomatic protest note to the UN regarding China's actions and restated its sovereignty over Hoang Sa (Paracel Islands) and Truong Sa (Spratly Islands).[106] The fifth anniversary of the PCA award also saw an intensification of activity by all parties, the most important of which may have been sharply confrontational statements from the Philippines and a formal US statement reaffirming 'that an armed attack on Philippine armed forces, public vessels, or aircraft in the South China Sea would invoke US mutual defense commitments under Article IV of the 1951 US–Philippines Mutual Defense Treaty'.[107]

Besides military, political and economic tools, cyber operations are another way for China to pressure or intimidate rivals, though the vast majority of its operations against them have been espionage-related. These are discussed here in some detail to illustrate the considerable evidence for Chinese cyber-espionage operations in comparison to its cyber-sabotage and cyber-influence operations. The imbalance of evidence leads us to conclude in this particular case study that China has not used offensive cyber operations against rival South China Sea claimants anywhere near as extensively as Russia has used them against Ukraine.

Cyber operations are another way for China to pressure or intimidate rivals

Most of the China-based APT groups, including Leviathan,[108] Pirate Panda,[109] Naikon,[110] Lotus Blossom[111] and Goblin Panda, have conducted cyber-espionage operations against China's rival claimants for at least seven years. Although most cyber-security reports do not directly attribute these APTs to Beijing, the governments and political entities targeted implies political and strategic motives that suggest the tacit approval or active sponsorship of the Chinese government. For instance, in May 2020, Check Point Research revealed that Naikon had used a backdoor named 'Aria-body' to target the foreign, science and technology ministries of Brunei, Indonesia, the Philippines and Vietnam, as well as state-owned companies in these countries.[112] Naikon is linked to PLA Unit 78020, which has been active since 2010.[113] According to an earlier report, Naikon also infiltrated the military agencies of a number of ASEAN

countries (Laos, Malaysia, the Philippines, Singapore and Vietnam), as well as various state-owned energy organisations, revealing a motive to exploit entities related to China's strategic and economic interests. The campaigns have targeted intellectual property from leading Southeast Asian companies in the energy, telecoms, high-tech, finance and transportation sectors, as well as claimant governments involved in the maritime dispute.[114] The compromise of telecoms companies allows an attacker to monitor communications passing through these providers, while intrusion of transportation companies provides access to crucial communications with military or regional security partners. The APT groups also gather political and military intelligence by stealing military documents, internal communications and equipment specifications, among other things. Lotus Blossom engages in persistent cyber espionage against government and military organisations in Southeast Asia, with the bulk of the targets in Vietnam and the Philippines.[115] It mainly relies on spear-phishing to lure users to open decoy files containing exploits tailored for Microsoft Office vulnerabilities. Lotus Blossom has continued to evolve and create new tools, amassing over 200 unique IP addresses for command and control by 2017.[116] US software company Symantec notes that the group tends to leverage legitimate features of operating systems and administrative tools in their exploits to evade detection and establish persistence in target networks.[117] While Lotus Blossom focuses primarily on government institutions and political parties, it also targets satellite-communication operators and maritime-communication organisations to gather intelligence.

Reports in 2020 continued to present findings about the cyber-espionage activities of established APT threat actors. Pirate Panda targeted government employees in Da Nang[118] and has penetrated air-gapped environments in Taiwan's and the Philippines' armed forces since 2014.[119] Similarly, Goblin Panda, an APT with a primary threat focus on Vietnam government organisations, has been attempting attacks against air-gapped networks.[120] Also in 2020, Kasperksy observed a new APT, FunnyDream, that has long-term espionage objectives consistent with previous campaigns against Southeast Asian governments. Kasperksy noted that the group had targeted high-profile entities in Malaysia, the Philippines, Taiwan and especially Vietnam since mid-2018,[121] focusing on stealing sensitive information pertaining to national security and conducting industrial espionage.[122]

China's cyber-espionage operations primarily target its two main opponents in the region – the Philippines and Vietnam. During the 2012 stand-off between China and the Philippines in the Scarborough Shoal, Chinese cyber units intruded into the latter's government and military networks to steal confidential military documents and related diplomatic communications.[123] Similarly, during China's mid-2014 HYSY-981 oil-rig stand-off with Vietnam, US cyber-security company CrowdStrike detected heavy targeting activities by Goblin Panda against Vietnam's government and defence and energy sectors.[124] Following the Philippines' initiation in 2013 to defend its maritime legal rights at the PCA, in 2015 China used spear-phishing to deploy the 'Nanhaishu' malware against several organisations, including the Philippines' Department of Justice and a major international law firm involved in representing one of the parties to the dispute.[125] It also infected the PCA website in a bid to acquire useful data from website visitors.[126] In the midst of more recent tensions with Vietnam and the Philippines in 2017[127] and 2019[128] respectively, China again stepped up its cyber-espionage operations against government and corporate targets. Evidently, during crises China conducts reactionary cyber-espionage operations in a bid to acquire intelligence to gain a better bargaining position. Its near-term objective is to challenge and undermine the diplomatic activities of claimant states.

Besides cyber-espionage campaigns, China has also leveraged social media to propagate disinformation to influence public discourse in its favour on issues related to the maritime disputes. In 2020, Facebook took down a number of fake accounts on Facebook and Instagram that were attributed to individuals in China.[129] These accounts, which defended China's policies in the region and promoted the PLAN's achievements, were dubbed 'Operation Naval Gazing'. Interestingly, two of its most influential pages related to Philippines politics, where China's favoured politicians at that time, such as President Rodrigo Duterte, were promoted.

China-based hackers have also conducted defacement and distributed denial-of-service (DDoS) campaigns against China's rivals to signal displeasure with their actions. After the PCA ruled against it in July 2016, in a case brought by the Philippines, China launched DDoS attacks lasting over several days against 68 Philippines government websites and defaced local-government portals.[130] In the same period, China-based group 1937cn conducted a series of attacks against Vietnam Airlines, hijacking its flight monitors and announcement systems to display derogatory messages about Vietnam's and the Philippines' territorial claims.[131] Although this group is

Table 4.3: **China's cyber operations against rival South China Sea claimants, 2010–21**

Date	Targets | methods | likely purposes
2010–15	Government and military agencies, state media and public and private energy companies in Laos, Malaysia, Myanmar, the Philippines, Singapore and Vietnam | spear-phishing | espionage
2012	The Philippines' government and military networks | malware | to steal confidential documents and diplomatic communications during the stand-off between Chinese and Philippine vessels in the Scarborough Shoal
2012–15	Philippine government institutions and military agencies | spear-phishing | espionage
Sep 2013–18	Defense, energy and government sectors in Southeast Asia, particularly Vietnam | spear-phishing | espionage, with heavy activities observed in mid-2014 during the HYSY-981 oil-rig stand-off
2013–14	Military agencies, government organisations and companies in Vietnam and the Philippines | spear-phishing, 'Elise' backdoor Trojan | espionage
Dec 2014–20	Philippine military and government agencies, physically isolated networks | used air-gapped environment, especially in military hospitals and national banks, to establish initial footholds, spear-phishing, 'USBferry' malware | espionage to steal defence and marine intelligence
Feb–Oct 2015	Organisations involved in the Permanent Court of Arbitration (PCA) case regarding claims in the South China Sea (Philippines Department of Justice, the Asia-Pacific Economic Cooperation and an international law firm) | spear-phishing | espionage
Jul 2015	PCA webpage detailing the legal case between the Philippines and China | watering-hole attack | espionage against parties interested in the legal case and to compromise webpage visitors
2015–20	Foreign, science and technology ministries and government-owned companies in countries including Brunei, Indonesia, Myanmar, the Philippines, Thailand and Vietnam | 'Aria-body' backdoor | espionage
Jul 2016	Philippine government networks, including those of key government agencies including the foreign-affairs and national-defence departments, central bank and the Presidential Management Staff | DDoS attacks | to retaliate against the PCA ruling that rebuked China's territorial claims
Jul 2016	Vietnam Airlines' systems | malware, leaking of hacked information (personal data of frequent-flyer club members), defacement of flight-monitor screens | to retaliate against the PCA ruling that rebuked China's territorial claims
2016–20	International public | disinformation using fake Facebook accounts | to promote China's policies in the South China Sea and highlight the achievements of the PLA Navy, advocate for China's preferred political candidates in Indonesia and the Philippines
2017	Government organisations, political parties, education institutions and telecommunications companies in countries including Indonesia, Vietnam, the Philippines, Malaysia and Thailand | spear-phishing, watering-hole attacks, malware | espionage
Jul–Aug 2017	Government agencies and corporations in Vietnam | malware | to steal information during a period of increased tensions over Vietnam's oil-drilling operations in a contested area of the South China Sea
Oct 2018–20	High-profile entities in Malaysia, the Philippines, Taiwan and Vietnam | malware ('Chinoxy', 'PCShare' and 'FunnyDream') | to steal information pertaining to national security and conduct industrial espionage
2018–20	Southeast Asian organisations, especially high-profile targets in Vietnam | 'USBCulprit' malware to reach air-gapped networks through USB media | espionage
Apr 2019	Government and private organisations in the Philippines | malware | to steal information amidst intensified political sentiments in the Philippines over China's activity in the South China Sea
Apr 2019	Philippine civilian, military and government websites | malicious script | espionage against website visitors
Jun 2019 – Mar 2021	Military organisations in Southeast Asia | 'RainyDay' backdoor, 'Aria-Body' loader, 'Nebulae' backdoor as backup | espionage and data theft
2019	Military organisations, satellite-communications operators, maritime-communications organisations, media and education sectors in Southeast Asia | 'Sagerunex' backdoor, 'living-off-the-land' techniques (utilises legitimate features of the operating system to conduct cyber attacks) | espionage
Jun 2020–Jan 2021	Mostly Vietnamese government, military, health, diplomacy, education and political organisations | DLL sideloading | to gather political intelligence (low-confidence attribution to China-linked APT)
Oct 2020–21	Government entities mostly in Philippines | spear-phishing (LuminousMoth APT) | espionage
Nov 2020–Mar 2021	At least four critical information infrastructures in an unnamed Southeast Asian country (water, power, defence and communications) | malware | espionage (evidence of China-linked hackers, but no definite attribution)
Mar 2021	Indonesian government ministries and agencies, including Badan Intelijen Negara (Indonesia's main intelligence agency) | malware | espionage
2021	Military and government organisations across Southeast Asia (navies, prime ministers' offices, defence and foreign ministries) | custom malware 'FunnyDream' and 'Chinoxy' | to gather intelligence regarding South China Sea issues and deepen China's regional influence

Sources: BBC, www.bbc.co.uk; Bitdefender, labs.bitdefender.com; Checkpoint Research, research.checkpoint.com; China–US Focus, www.chinausfocus.com; CrowdStrike, www.crowdstrike.com; CyberScoop, www.cyberscoop.com; *Diplomat*, thediplomat.com; *Forbes*, www.forbes.com; GMA News, www.gmanetwork.com; Graphika, graphika.com; Hacker News, thehackernews.com; Insikit (Recorded Future), www.recordedfuture.com; Ironnet, www.ironnet.com; Kaspersky, www.kaspersky.com; Palo Alto Networks, unit42.paloaltonetworks.com; Reuters, www.reuters.com; Secure List, securelistcom; *South China Morning Pos*t, www.scmp.com; Symantec, symantec-enterprise-blogs.security.com; Record, therecord.media; ThreatConnect, threatconnect.com; Threatpost, threatpost.com; TrendMicro, Proofpoint, www.proofpoint.com; ZDNet, www.zdnet.com.
Note: The likely purposes of the operations are those identified by the sources cited.

known to consist of nationalistic hackers, they help to support China's strategic goals since China's monitoring of these groups tends to relax during times of conflict.[132] Table 4.3 summarises known Chinese cyber operations against rival claimants.

By maintaining a long-term presence in rival claimants' government or military networks, China can gain military, political and economic intelligence to help it navigate changes in the regional geopolitical landscape. Aside from their direct intelligence value, low-level and persistent cyber operations grant China strategic access to its rivals' military and critical-infrastructure networks and hold these assets at risk. By tilting the balance of information in China's favour, cyber espionage creates an information asymmetry that may lower adversaries' expectations that they will gain from future coercive exchanges, and may increase the credibility of Beijing's threats to escalate in the event of conflict.[133]

China's track record demonstrates its preference for low-level cyber operations against rival South China Sea claimants. Importantly, it does not leverage these operations in an escalatory manner towards sabotage in the physical domain. One possible reason for this is that cyber operations are just one of many tools that China can use to assert itself in maritime disputes. Other tools include economic coercion and building artificial islands with military features. Compared to cyber operations, grey-zone strategies – conducted in the physical realm through a long series of visible alterations on the ground – arguably produce greater change in China's favour that is also harder for rivals to counter.

A second reason is that China's focus on low-intensity cyber campaigns aligns with China's preference for ambiguity. They augment China's 'Three Warfares' strategy, which includes psychological warfare, public-opinion warfare and legal warfare.[134] Long-term cyber-espionage campaigns help China attain strategic leverage in rival claimants' critical networks and simultaneously signal escalation risks. In addition, China's Digital Silk Road initiative and digital economic cooperation with regional states moves them further into China's sphere of influence and discourages opposition.[135] China's cyber strategies function as a form of psychological warfare, manipulating an adversary's perception about the utility of future escalatory actions and potentially undermining its will to act.[136] China also conducts public-opinion warfare in cyberspace via its disinformation campaigns, aiming to justify its policies and create a dominant public discourse favourable to its actions in the South China Sea. In terms of legal warfare, China passed the Coast Guard Law, which authorised its coastguard to use force against foreign vessels under specific conditions.[137]

Finally, the low-intensity nature of China's cyber campaigns can be attributed to the relative restraint shown by neighbouring states. Dissatisfaction with China's aggressive actions in the disputes led to tit-for-tat defacement and DDoS attacks without spillage into the physical domain.[138] When Vietnam's airports were hacked in 2016, Vietnamese government officials' response was to call for a 'calm and discreet' approach.[139] The claimant states' economic dependence on China, and the latter's military power, deter smaller claimants from retaliating with high-level destructive cyber attacks. Even though the United States' hardened stance[140] in the South China Sea may have provided assurance to China's neighbouring states, many leaders in the region have reasons to doubt Washington's resolve as the guarantor of regional security, further highlighting the need for a measured response to China's cyber activities.

Low-level and persistent cyber operations grant China strategic access to its rivals' military and critical-infrastructure networks

Campaign summary

The primary lines of effort of China's campaign to consolidate its territorial claims in the South China Sea are:

- persistent and long-term cyber espionage against rival governments' ministries, military agencies and corporations, with intensified operations during periods of heightened political tension

- information operations on social media to defend and promote China's policies in the South China Sea
- disruptive (DDoS) attacks and web-defacement attacks to signal China's displeasure in response to unfavourable political events surrounding the South China Sea

In general, apart from espionage, China's cyber operations have been infrequent, low-level and low-intensity, intended more for disruption and minor influence seeking. There is no information available about more serious sabotage or influence-seeking attacks by China against even its most vocal rival claimants.

Assessing and mapping Chinese campaigns

The lines of effort used in the three cyber campaigns are summarised in Table 4.4.

Figure 4.1 provides a provisional mapping of cyber operations against the background of changes in China's diplomatic sentiment – meaning broadly the attitude of the Chinese leadership towards the target country or group.

Table 4.5 summarises the campaigns against three analytical criteria: intent, character and effect. The intent column contains our assessment of the precise purpose of the lines of effort for each campaign.

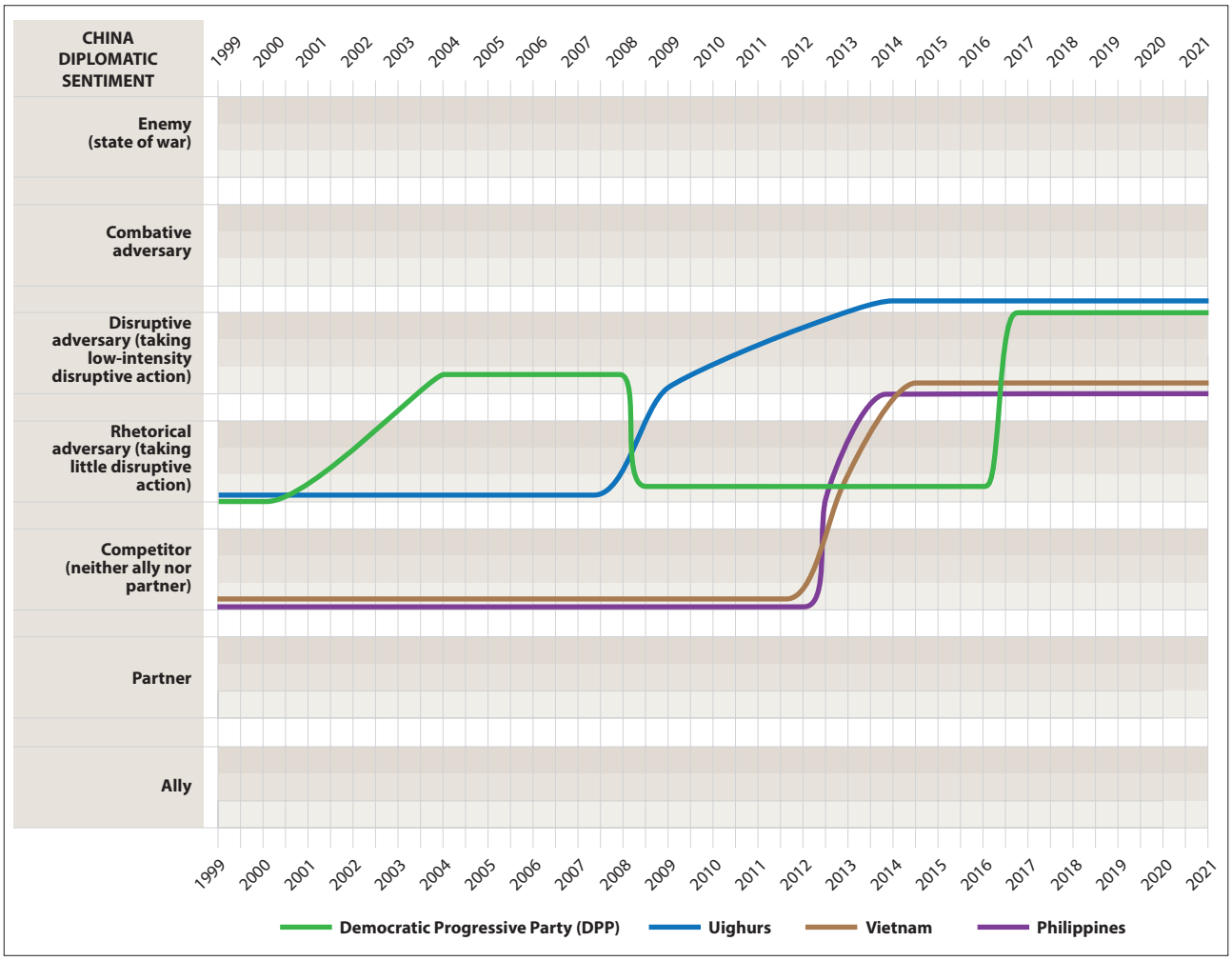
The three case studies highlight China's consistently conservative use of offensive cyber tools. In each campaign China employed persistent and long-term cyber espionage combined with wider information operations using new and traditional media to spread disinformation and propaganda about China's adversaries. Short-term disruptive and nuisance cyber operations were also used to signal to adversaries the risks of escalation and China's displeasure in response to political events. Beijing's persistent and long-term espionage operations in adversaries' networks broadly reflect the ability of Chinese cyber hackers (from the SSF or the MSS) to continually adapt to the changing security climate in cyberspace and innovate new and sophisticated tools to evade detection. Their ability to compromise high-value and challenging targets, such as global telecoms operators, air-gapped military networks and ubiquitous Android and iPhone software, proves China's continual advancement in offensive cyber techniques. There are also clear signs of high levels of coordination in China's cyber-espionage efforts, evidenced in its global targeting of the Uighur diaspora, which has led to extradition of Chinese Uighurs from countries such as Egypt, Malaysia and Thailand.[141]

In contrast to its cyber-espionage capabilities, China's information operations mediated via traditional- and social-media platforms appeared less mature and less rampant (according to publicly available information). Efforts to shape public opinion in Taiwan and with regard to the South China Sea have reaped limited results, and international sentiments have intensified against China, with diplomatic sanctions and increasing international opprobrium against it. The relatively rudimentary efforts in cyber-enabled influence operations may indicate that the CCP leadership accords a lower priority to this aspect. A reasonable explanation may be that China has a far richer set of diplomatic and political tools that it can leverage to achieve its political objectives – propaganda, economic coercion, traditional coercion, salami-slicing tactics and legal tools, among others. Cyber espionage often serves as

Table 4.4: **Primary lines of effort in Chinese campaigns**

Anti-independence drive against the DPP in Taiwan	• Persistent and long-term cyber espionage against Taiwanese government agencies, political targets and corporations, including companies linked to the government • Election interference through disinformation campaigns, augmented by intensified cyber espionage to undermine the DPP and delegitimise its political candidates while supporting preferred candidates • Defacement of government websites to signal displeasure with political events in Taiwan
'Anti-terrorist' drive against Uighurs	• Long-term cyber espionage against the Uighur diaspora through interception of all prevalent communication platforms to identify political activists and dissidents for subsequent coercion to cease activities • Information operations through designating Uighur activists as terrorists and their independence movement as a terrorist movement
Consolidation of China's territorial claims in the South China Sea	• Persistent and long-term cyber espionage against rival governments' ministries, military agencies and corporations, with intensified operations during periods of heightened political tension • Information operations on social media to defend and promote China's policies in the South China Sea • Disruptive (DDoS) attacks and web-defacement attacks to signal China's displeasure in response to unfavourable political events surrounding the South China Sea

Figure 4.1: Mapping China's diplomatic sentiment and cyber campaigns



Note: The authors have chosen to represent each phase of the diplomatic sentiment as a straight line while recognising that there are positive or negative changes in a particular phase. The characterisations are based as closely as possible on explicit positions of the Chinese government.

an enabler to augment and support China's actions in the physical realm.

Nevertheless, this assessment of China's cyber campaigns is based on observations of actions conducted against relatively less capable targets during peacetime. The nature of China's cyber operations may evolve to include more destructive elements should an armed conflict occur.

Two questions

How well has China organised for offensive cyber campaigns?

The intelligence agencies are well prepared to project power through cyberspace for political purposes but the armed forces are at a far earlier stage of maturity to use force in cyberspace against adversaries.

How has China used offensive cyber operations for strategic gain?

China has used cyber campaigns for political influencing against adversaries at a lower level of intensity than might have been expected given the stakes involved, especially in respect of Taiwan. There is as yet no evidence of the PLA using an offensive cyber campaign or even low-level cyber operations for sabotage or influence in military combat.

Table 4.5: **Summary of intent, character and effect of each campaign**

Campaign	Intent	Character	Effect
Anti-independence drive against the DPP in Taiwan	• To undermine DPP legitimacy and weaken public trust in the party, its elected representatives and political candidates while providing support to Beijing's favoured candidates • To weaken the separatist movement in Taiwan while cultivating pro-China factions • To obtain confidential information from Taiwanese private and public organisations, including those that could be leveraged against the DPP in its information operations	• Low intensity but widespread and long-term espionage operations • Short-term disruptive operations • Covert and overt information operations, including disinformation and leveraging of intelligence siphoned from cyber espionage	• DPP prevailed against the Kuomintang in the 2020 elections • Public sentiment in Taiwan rates China less favourably than the US • Improved Taiwan–US relationship under the Trump administration (normalised arms sales, removal of diplomatic restrictions)
'Anti-terrorist' drive against Uighurs	• To seek intelligence on political activists and dissidents within the Uighur diaspora regarding their locations, movements, communications and contacts, and to subsequently coerce them through traditional means • To raise costs on political activism supporting the Uighur cause and discrediting the Chinese government • To isolate the Uighur movement and deny it international support and visibility • To curb and deter violent attacks and separatist activities	• Low intensity, but widespread and long-term cyber espionage operations • Cyber-enabled coercion against targeted Uighurs	• Increased extradition of the Uighur diaspora to China • Heightened international scrutiny of Uighurs' experiences, with sanctions imposed by the UK and the US • US delisted the East Turkestan Islamic Movement in November 2020 • No major violent terrorist attacks in China since 2017
Consolidation of China's territorial claims in the South China Sea	• To obtain political, economic and military intelligence to navigate the changing regional geopolitical landscape and shape a better bargaining position during times of political crises or military tensions • To impose sustained costs and undermine adversaries' will to act in an escalatory manner through a long-term presence in adversaries' critical networks • To manipulate international public opinion regarding the South China Sea dispute in Beijing's favour • To signal displeasure against unfavourable political events surrounding the dispute	• Low intensity, but widespread and long-term cyber espionage • Occasional disruptive operations • Overt and covert (fake accounts on social media) information operations, including disinformation	• Relative restraint demonstrated in the low-level cyber retaliation from most vocal adversaries, Vietnam and the Philippines, without spillover into the physical domain • Increased efforts by claimant states to strengthen cyber defence on a regional and national level • International opinion of China's policies in the South China Sea has worsened, with concerted calls for China to abide by the PCA ruling, and US sanctions on companies helping advance Beijing's claims

Sources: Al Jazeera, www.aljazeera.com; BBC News, www.bbcnews.com; Bernama, www.bernama.com; Channel Asia, channelasia.tech; CNN, edition.cnn.com; Jamestown Foundation, www.jamestown.org; New Lens, international.thenewlens.com; Nikkei Asia, asia.nikkei.com; OpenGov Asia, opengovasia.com; Pew Research Center, www.pewresearch.org; *South China Morning Post*, www.scmp.com; *Straits Times*, www.straitstimes.com; VOA News, www.voanews.com.

Notes

1 See Greg Austin, *Cyber Policy in China* (Cambridge: Polity, 2014).

2 'Ba woguo cong wangluo daguo jianshe chengwei wangluo qiangguo' [Xi Jinping: Build Our Country from a Network Power to a Network Superpower], Xinhua, 27 February 2014, http://news.xinhuanet.com/politics/2014-02/27/c_119538788.htm.

3 China Aerospace Studies Institute, 'In Their Own Words: Foreign Military Thought – Science of Military Strategy 2013', 8 February 2021, pp. 96–9, 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.

4 State Council Information Office of the People's Republic of China (PRC), 'China's Military Strategy', 27 May 2015, http://english.www.gov.cn/archive/white_paper/2015/05/27/content_281475115610833.htm.

5 In this report, cyber espionage is not included in the definition of offensive cyber operations.

6 In 2012, after the person in this post, Zhou Yongkang, was replaced, the new appointee remained an ordinary Politburo member rather than a member of the Standing Committee (the inner circle), which his predecessors had been for the most part since the 1980s. Zhou was subsequently convicted of corruption, charges assumed to be the public face of more serious political charges including an attempt to derail Xi's ascension.

7 James S. Johnson, 'China's Vision of the Future Network-centric Battlefield: Cyber, Space and Electromagnetic Asymmetric Challenges to the US', *Comparative Strategy*, vol. 37, no. 5, March 2019, pp. 373–90, https://www.tandfonline.com/doi/full/10.1080/01495933.2018.1526563.

8 See Timothy L. Thomas, *Dragon Bytes: Chinese Information-War*

Theory and Practice from 1995–2003 (Leavenworth, KS: US Army Foreign Military Studies Office, 2004).

9 Peng Guangqian and Youzhi Yao (eds), *The Science of Military Strategy* (Beijing: Military Science Publishing House, 2005), p. 406.

10 Xinhua, 'Full Text: China's Military Strategy', *China Daily*, 26 May 2015, https://www.chinadaily.com.cn/china/2015-05/26/content_20820628_3.htm.

11 China Aerospace Studies Institute, 'In Their Own Words: Foreign Military Thought – Science of Military Strategy 2013', pp. 117–22.

12 'Army Needs "Information Warfare" Plan, Declares Xi', *China Daily*, 1 September 2014, http://www.chinadaily.com.cn/china/2014-09/01/content_18520930.htm.

13 State Council Information Office of the PRC, 'China's Military Strategy'.

14 Adam Ni and Bates Gill, 'The People's Liberation Army Strategic Support Force: Update 2019', *China Brief*, vol. 19, no. 10, 29 May 2019, https://jamestown.org/program/the-peoples-liberation-army-strategic-support-force-update-2019/.

15 John Costello and Joe McReynolds, 'China's Strategic Support Force: A Force for a New Era', *China Strategic Perspectives*, Institute for National Strategic Studies, National Defense University, October 2018, p. 9, https://ndupress.ndu.edu/Portals/68/Documents/stratperspective/china/china-perspectives_13.pdf.

16 Cyberspace Administration of China, '《国家网络空间安全战略》全文' [Full Text of 'National Cyberspace Security Strategy'], 27 December 2016, http://www.cac.gov.cn/2016-12/27/c_1120195926.htm.

17 Ministry of Foreign Affairs, 'International Strategy of Cooperation on Cyberspace', March 2017, https://www.fmprc.gov.cn/mfa_eng/wjb_663304/zzjg_663340/jks_665232/kjlc_665236/qtwt_665250/t1442390.shtml.

18 State Council Information Office of the PRC, 'China's National Defense in the New Era', 24 July 2019, https://english.www.gov.cn/archive/whitepaper/201907/24/content_WS5d3941ddc6d08408f502283d.html.

19 This group had existed in different forms since 1993 but had never been led by the general secretary until 2014.

20 John Costello, 'China Finally Centralizes Its Space, Cyber, Information Forces', *Diplomat*, 20 January 2016, https://thediplomat.com/2016/01/china-finally-its-centralizes-space-cyber-information-forces/.

21 Arthur S. Ding and Paul A. Huang, 'Taiwan's Paradoxical Perceptions of the Chinese Military: More Capable but Less Threatening?', *China Perspectives*, April 2011, pp. 43–51.

22 See State Council Information Office of the PRC, 'China's National Defense in 2008', January 2009, http://www.china.org.cn/government/whitepaper/node_7060059.htm; and State Council Information Office of the PRC, 'China's National Defense in 2010', March 2011, http://www.china.org.cn/government/whitepaper/node_7114675.htm.

23 See 'Full Text of Xi Jinping's Report at 19th CPC National Congress', Xinhua, 3 November 2017, http://www.xinhuanet.com/english/special/2017-11/03/c_136725942.htm; and 'Highlights of Xi's Speech at Gathering Marking 40th Anniversary of Message to Compatriots in Taiwan', Xinhua, 2 January 2019, http://www.xinhuanet.com/english/2019-01/02/c_137715300.htm.

24 Peng Guangqian and Youzhi Yao (eds), *The Science of Military Strategy*.

25 State Council Information Office of the PRC, 'China's Military Strategy'.

26 'Full Text of Xi Jinping's Report at 19th CPC National Congress', *China Daily*, 4 November 2017, https://www.chinadaily.com.cn/china/19thcpcnationalcongress/2017-11/04/content_34115212.htm.

27 Yew Lun Tian and Yimou Lee, 'China's Xi Pledges "Reunification" with Taiwan, Gets Stern Rebuke', Reuters, 1 July 2021, https://www.reuters.com/world/china/chinas-xi-pledges-reunification-with-taiwan-partys-birthday-2021-07-01/.

28 See International Crisis Group, 'Taiwan Strait I: What's Left of "One-China"?', 6 June 2003, p. 13, https://www.crisisgroup.org/asia/north-east-asia/taiwan-strait/taiwan-strait-i-what-s-left-one-china.

29 Loa Iok-sin, 'Members Spark DPP Charter Debate', *Taipei Times*, 17 June 2016, https://www.taipeitimes.com/News/taiwan/archives/2016/06/17/2003648821.

30 State Council Information Office of the PRC, 'China's National Defense in 2004', December 2004, http://en.people.cn/whitepaper/defense2004/defense2004.html.

31 'China, Law No. 34 of 2005, Anti-Secession Law', UN High Commissioner for Refugees, 29 November 2021, https://www.refworld.org/docid/474403752.html.

32 'Nothing to Celebrate, Except in China', *Taipei Times*, 20 May 2011, http://www.taipeitimes.com/News/editorials/archives/2011/05/20/2003503665.

33 Costello, 'China Finally Centralizes Its Space, Cyber, Information Forces'.

34 See State Council of the PRC, 'China's National Defense in the New Era'; and 'China Establishes Rocket Force and Strategic

Support Force', Defence Talk, 5 January 2016, https://www.defencetalk.com/china-establishes-rocket-force-and-strategic-support-force-66236/.

35 See J. Michael Cole, 'Was Taiwan's Sunflower Movement Successful?', *Diplomat*, 1 July 2014, https://thediplomat.com/2014/07/was-taiwans-sunflower-movement-successful/; and Ming-Sho Ho, 'The Activist Legacy of Taiwan's Sunflower Movement', Carnegie Endowment for International Peace, 2 August 2018, https://carnegieendowment.org/2018/08/02/activist-legacy-of-taiwan-s-sunflower-movement-pub-76966.

36 'Interview of Taiwan President Lee Teng-hui with Deutsche Welle Radio', 9 July 1999, New Taiwan, https://www.taiwandc.org/nws-9926.htm.

37 For examples, see Ko Shu-ling, 'Cabinet Says Computers Under Attack', *Taipei Times*, 4 September 2003, http://www.taipeitimes.com/News/front/archives/2003/09/04/2003066387; Russell Hsiao, 'Critical Node: Taiwan's Cyber Defense and Chinese Cyber-espionage', 19 December 2015, https://russellhsiao.wordpress.com/2015/12/19/120513-critical-node-taiwans-cyber-defense-and-chinese-cyber-espionage/; 'Suspected Chinese Hacker Attacks Target AIT, MND', *Taipei Times*, 19 June 2006, https://www.taipeitimes.com/News/taiwan/archives/2006/06/19/2003314414; Ministry of National Defense of the Republic of China, 'National Defense Report', 2015, p. 69; 'Taiwan to Open New Cyberwar Unit', *Bangkok Post*, 30 May 2013, https://www.bangkokpost.com/world/352527/taiwan-to-open-new-cyberwar-unit; Ned Moran and Mike Oppenheim, 'Darwin's Favorite APT Group', FireEye Threat Research, 3 September 2014, https://www.fireeye.com/blog/threat-research/2014/09/darwins-favorite-apt-group-2.html; Matthew Strong, 'China Hackers Steal 3 Million Taipei Health Department Files', *Taiwan News*, 2 January 2019, https://www.taiwannews.com.tw/en/news/3608912; Sherry Hsiao, 'Chinese Hackers Suspected in Attack', *Taipei Times*, 3 January 2019, http://www.taipeitimes.com/News/front/archives/2019/01/03/2003707246; and FireEye Threat Intelligence, 'Southeast Asia: An Evolving Cyber Threat Landscape', March 2015, https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-southeast-asia-threat-landscape.pdf.

38 'CNACOM – Open Source Exploitation via Strategic Web Compromise', Zscaler, 1 December 2016, https://www.zscaler.com/blogs/security-research/cnacom-open-source-exploitation-strategic-web-compromise; and Sean Lyngaas, 'Hacking Group Has Hit Taiwan's Prized Semiconductor Industry, Taiwanese Firm Says', *Cyberscoop*, 6 August 2020, https://www.cyberscoop.com/cycraft-taiwan-semiconductor-espionage-black-hat/.

39 Kelly Jackson Higgins, 'Taiwan Says China Accounts for Most Cyber Attacks', *Dark Reading*, 17 January 2008, https://www.darkreading.com/vulnerabilities---threats/taiwan-says-china-accounts-for-most-cyber-attacks-/d/d-id/1129242.

40 Michael Behr, 'Taiwan Subject to String of Chinese Cyberattacks Since 2018', *Digit*, 19 August 2020, https://digit.fyi/taiwan-subject-to-string-of-chinese-cyberattacks-since-2018/; Debby Wu, 'Taiwan Accuses Chinese Hackers of Targeting Its Citizens' Data', Bloomberg, 19 August 2020, https://www.bloomberg.com/news/articles/2020-08-19/chinese-hackers-target-taiwan-data-through-government-systems; and Lee, 'Taiwan Says China Behind Cyberattacks on Government Agencies, Emails'.

41 'Hackers Deface DPP's Web Site', *Taipei Times*, 23 June 2004, https://www.taipeitimes.com/News/taiwan/archives/2004/06/23/2003176179.

42 Chris Wang, 'Hackers Attack DPP's Presidential Campaign Office', *Taipei Times*, 10 August 2011, http://www.taipeitimes.com/News/front/archives/2011/08/10/2003510374.

43 'Chinese State-backed Hacker Group Attacks the DPP and Taiwanese Media', *News Lens*, 21 December 2015, https://international.thenewslens.com/article/32999.

44 In June 2016, the DPP's website was hacked and replaced with a website that profiled visitors. See David Tweed, 'Taiwan Ruling Party's Website Hacked in Cyberspying Campaign', Bloomberg, 2 June 2016, https://www.bloomberg.com/news/articles/2016-06-02/taiwan-ruling-party-s-website-hacked-in-cyberspying-campaign; and James Griffiths, 'Chinese Hackers Target Taiwan Political Party to Spy on Website Visitors', CNN, 2 June 2016, https://edition.cnn.com/2016/06/01/asia/taiwan-dpp-chinese-hackers/index.html.

45 See Sophia Yang, 'Taiwan's DPP Website Hacked by Chinese Hackers', *Taiwan News*, 3 July 2018, https://www.taiwannews.com.tw/en/news/3473203; and John Follain, Adela Lin and Samson Ellis, 'China Ramps Up Cyberattacks on Taiwan', Bloomberg, 19 September 2018, https://www.bloomberg.com/news/articles/2018-09-19/chinese-cyber-spies-target-taiwan-s-leader-before-elections.

46 V-Dem Institute, 'Democracy Facing Global Challenges: V-Dem Annual Report 2019', May 2019, pp. 5, 34, https://www.v-dem.net/media/filer_public/99/de/99dedd73-f8bc-484c-8b91-44ba601b6e6b/v-dem_democracy_report_2019.pdf.

47 Sarah O'Connor et al., 'Cyber-enabled Foreign Interference

in Elections and Referendums', International Cyber Policy Centre, Australian Strategic Policy Institute (ASPI), *Policy Brief*, report no. 41, 2020, p. 15.

48 'June 13: Swinging the Vote: How the CCP Influences the Media and Elections in Taiwan and Beyond', Global Taiwan Institute, 13 June 2019, https://globaltaiwan.org/2019/06/june-13-swinging-the-vote-how-the-ccp-influences-the-media-and-elections-in-taiwan-and-beyond/.

49 Joshua Kurlantzick, 'How China Is Interfering in Taiwan's Election', Council on Foreign Relations, 7 November 2019, https://www.cfr.org/in-brief/how-china-interfering-taiwans-election.

50 See Brian Hioe, 'Is Chinese Election Interference Behind the Han Kuo-Yu Phenomenon?', *New Bloom*, 13 November 2018, https://newbloommag.net/2018/11/13/han-phenomenon-china/; and J. Michael Cole, 'That's What "Fake News" Looks Like and What It Does to Democracy', *Taiwan Sentinel*, 12 November 2018, https://sentinel.tw/fake-news-kaohsiung-democracy/.

51 Nick McKenzie, Grace Tobin and Paul Sakkal, 'The Moment a Chinese Spy Decided to Defect to Australia', Age, 23 November 2019, https://www.theage.com.au/national/the-moment-a-chinese-spy-decided-to-defect-to-australia-20191122-p53dox.html; and Nick McKenzie, Grace Tobin and Paul Sakkal, 'Defecting Chinese Spy Offers Information Trove to Australian Government', *Sydney Morning Herald*, 25 November 2019, https://www.smh.com.au/national/defecting-chinese-spy-offers-information-trove-to-australian-government-20191122-p53d1l.html.

52 See Keoni Everington, 'Witnesses Refute Report Stranded Taiwanese in Japan Had to Identify Themselves As Chinese', *Taiwan News*, 7 September 2018, https://www.taiwannews.com.tw/en/news/3524492; and Lee Hsin-fang and William Hetherington, 'Chinese Kansai Evacuation Story "Fake News": DPP', *Taipei Times*, 9 September 2018, http://www.taipeitimes.com/News/taiwan/archives/2018/09/09/2003700087.

53 Keoni Everington, 'Beijing-based PTT Users Spread Fake Osaka Airport Bus Story', *Taiwan News*, 17 September 2018, https://www.taiwannews.com.tw/en/news/3531772.

54 See '滞留日本大阪关西国际机场的中国旅客全部撤离' [All Chinese Passengers Stranded At Kansai International Airport in Osaka, Japan Evacuated], Xinhua, 6 September 2018, http://www.xinhuanet.com/asia/2018-09/06/c_1123388370.htm; and '1,044 Chinese Tourists Evacuated from Typhoon-hit Japan', *People's Daily Online*, 6 September 2018, http://en.people.cn/n3/2018/0906/c90000-9498253.html.

55 Stanford Internet Observatory, 'Taiwan Election: The Final Countdown', Cyber Policy Center, 12 December 2019, https://cyber.fsi.stanford.edu/io/news/taiwan-election-final-countdown.

56 Kurlantzick, 'How China Is Interfering in Taiwan's Election'.

57 See Sheridan Prasso and Samson Ellis, 'China's Information War on Taiwan Ramps Up as Election Nears', Bloomberg, 23 October 2019, https://www.bloomberg.com/news/articles/2019-10-23/china-s-information-war-on-taiwan-ramps-up-as-election-nears; and Lily Kuo and Lillian Yang, 'Taiwan's Citizens Battle Pro-China Fake News Campaigns as Election Nears', *Guardian*, 30 December 2019, https://www.theguardian.com/world/2019/dec/30/taiwan-presidential-election-referendum-on-ties-with-china.

58 Philip Sherwell, 'China Uses Taiwan for AI Target Practice to Influence Elections', *Australian*, 5 January 2020, https://www.theaustralian.com.au/world/the-times/china-uses-taiwan-for-ai-target-practice-to-influence-elections/news-story/57499d2650d4d359a3857688d416d1e5.

59 Shannon Tiezzi, 'Taiwan "Shouts Back": President Tsai Wins Re-election Despite China's Pressure Campaign', *Diplomat*, 12 January 2020, https://thediplomat.com/2020/01/taiwan-shouts-back-president-tsai-wins-re-election-despite-chinas-pressure-campaign/.

60 Tom Fowdy, 'DPP's Use of "The Mainland Card" in Taiwan Leadership Elections', *CGTN*, 5 January 2020, https://news.cgtn.com/news/2020-01-05/DPP-s-use-of-the-mainland-card-in-Taiwan-leadership-elections-NotK313Gbm/index.html.

61 Richard Bush, 'From Persuasion to Coercion: Beijing's Approach to Taiwan and Taiwan's Response', Brookings Institution, November 2019, p. 6, https://www.brookings.edu/wp-content/uploads/2019/11/FP_20191118_beijing_taiwan_bush.pdf.

62 Dana Carver Boehm, 'China's Failed War on Terror: Fanning the Flames of Uighur Separatist Violence', *Berkeley Journal of Middle Eastern & Islamic Law,* vol. 2, no. 1, April 2009, pp. 61–124.

63 'Chronology for Turkmen in China', Minorities at Risk Project, University of Maryland, http://www.mar.umd.edu/chronology.asp?groupId=71003.

64 Tania Branigan, 'China Locks Down Western Province After Ethnic Riots Kill 140', *Guardian*, 6 July 2009, https://www.theguardian.com/world/2009/jul/06/china-Uyghur-urumqi-riots.

65 'Tiananmen Square Terror Attack', *South China Morning*

Post, October 2013, https://www.scmp.com/topics/tiananmen-square-terror-attack.

66 'Urumqi Car and Bomb Attack Kills Dozens', *Guardian*, 22 May 2014, https://www.theguardian.com/world/2014/may/22/china-urumqi-car-bomb-attack-xinjiang.

67 Shannon Tiezzi, 'China Confirms 3 Dead, 79 Injured in Urumqi Terrorist Attack', *Diplomat*, 1 May 2014, https://thediplomat.com/2014/05/china-confirms-3-dead-79-injured-in-urumqi-terrorist-attack/.

68 Jonathan Kaiman and Tania Branigan, 'Kunming Knife Attack: Xinjiang Separatists Blamed for "Chinese 9/11"', *Guardian*, 2 March 2014, https://www.theguardian.com/world/2014/mar/02/kunming-knife-attack-muslim-separatists-xinjiang-china.

69 See State Council Information Office of the PRC, 'China's National Defense in 2008'.

70 State Council Information Office of the PRC, 'China's Military Strategy'.

71 Human Rights Watch, '"Eradicating Ideological Viruses": China's Campaign of Repression Against Xinjiang's Muslims', 9 September 2018, https://www.hrw.org/report/2018/09/09/eradicating-ideological-viruses/chinas-campaign-repression-against-xinjiangs.

72 Zunyou Zhou, 'China's Comprehensive Counter-terrorism Law', *Diplomat*, 23 January 2016, https://thediplomat.com/2016/01/chinas-comprehensive-counter-terrorism-law/.

73 See Doug Nairne, 'State Hackers Spying On Us, Say Dissidents', *South China Morning Post*, 18 September 2002, https://www.scmp.com/article/391734/state-hackers-spying-us-say-dissidents; and Maarten Van Horenbeeck, 'Cyber Attacks Against Tibetan Communities', SANS Internet Storm Center, 21 March 2008, https://isc.sans.edu/diary/Cyber+attacks+against+Tibetan+communities/4176.

74 Joseph Menn, 'Microsoft Failed to Warn Victims of Chinese Email Hack: Former Employees', Reuters, 31 December 2015, https://in.reuters.com/article/us-microsoft-china-insight/microsoft-failed-to-warn-victims-of-chinese-email-hack-former-employees-idUSKBN0UE01Z20151231.

75 Costin Raiu, 'New MacOS X Backdoor Variant Used in APT Attacks', Securelist by Kaspersky, 29 June 2012, https://securelist.com/new-macos-x-backdoor-variant-used-in-apt-attacks/33214/; Kurt Baumgartner and Costin Raiu, 'Cyber Attacks Against Uyghur Mac OS X Users Intensify', Securelist by Kaspersky, 13 February 2013, https://securelist.com/cyber-attacks-against-uyghur-mac-os-x-users-intensify/64259/; and Jaime Blasco, 'Cyber Espionage Campaign Against the Uyghur Community, Targeting MacOSX Systems', AT&T Cybersecurity, 13 February 2013, https://cybersecurity.att.com/blogs/labs-research/cyber-espionage-campaign-against-the-uyghur-community-targeting-macosx-syst.

76 Jaime Blasco, 'New MaControl Variant Targeting Uyghur Users, the Windows Version Using Ghost RAT', AT&T Cybersecurity, 29 June 2012, https://cybersecurity.att.com/blogs/labs-research/new-macontrol-variant-targeting-uyghur-users-the-windows-version-using-ghos.

77 Kurt Baumgartner and Denis Maslennikov, 'Android Trojan Found in Targeted Attack', Securelist by Kaspersky, 26 March 2013, https://securelist.com/android-trojan-found-in-targeted-attack-58/35552/.

78 Robert Falcone and Jen Miller-Osborn, 'Scarlet Mimic: Years-Long Espionage Campaign Targets Minority Activists', Unit 42, Palo Alto Networks, 24 January 2016, https://unit42.paloaltonetworks.com/scarlet-mimic-years-long-espionage-targets-minority-activists/.

79 Alex Hinchliffe et al., 'HenBox: The Chickens Come Home to Roost', Unit 42, Palo Alto Networks, 13 March 2018, https://unit42.paloaltonetworks.com/unit42-henbox-chickens-come-home-roost/.

80 Cybereason Nocturnus, 'Operation Soft Cell: A Worldwide Campaign against Telecommunications Providers', Cybereason, 25 June 2019, https://www.cybereason.com/blog/operation-soft-cell-a-worldwide-campaign-against-telecommunications-providers.

81 See Ian Beer, 'A Very Deep Dive into iOS Exploit Chains Found in the Wild', Project Zero, Google, 29 August 2019, https://googleprojectzero.blogspot.com/2019/08/a-very-deep-dive-into-ios-exploit.html; and Ian Beer, 'Implant Teardown', Project Zero, Google, 29 August 2019, https://googleprojectzero.blogspot.com/2019/08/implant-teardown.html.

82 Andrew Case, Matthew Meltzer and Steven Adair, 'Digital Crackdown: Large-scale Surveillance and Exploitation of Uyghurs', Volexity, 2 September 2019, https://www.volexity.com/blog/2019/09/02/digital-crackdown-large-scale-surveillance-and-exploitation-of-uyghurs/.

83 Bill Marczak et al., 'Missing Link: Tibetan Groups Targeted with 1-Click Mobile Exploits', Citizen Lab, Munk School of Global Affairs and Public Policy, 24 September 2019, https://citizenlab.ca/2019/09/poison-carp-tibetan-groups-targeted-with-1-click-mobile-exploits/.

84 Andrew Case et al., 'Evil Eye Threat Actor Resurfaces with iOS Exploit and Updated Implant', Volexity, 21 April 2020,

https://www.volexity.com/blog/2020/04/21/evil-eye-threat-actor-resurfaces-with-ios-exploit-and-updated-implant/.

85 'Mobile APT Surveillance Campaigns Targeting Uyghurs: A Collection of Long-running Android Tooling Connected to a Chinese mAPT Actor', Lookout Threat Intellience, June 2020, https://www.lookout.com/documents/threat-reports/us/lookout-uyghur-malware-tr-us.pdf.

86 Ecular Xu and Joseph C Chen, 'Phishing Attacks from Earth Empusa Reveal ActionSpy', Trend Micro, 11 June 2020, https://www.trendmicro.com/en_us/research/20/f/new-android-spyware-actionspy-revealed-via-phishing-attacks-from-earth-empusa.html.

87 See statement of Louisa Greve in US Government Publishing Office, 'Chinese Hacking: Impact on Human Rights and Commercial Rule of Law', Hearing before the Congressional-Executive Commission on China, 113th Congress, 1st session, 25 June 2013, https://www.govinfo.gov/content/pkg/CHRG-113hhrg81855/html/CHRG-113hhrg81855.htm.

88 For an overview of the history of these claims, see Greg Austin, *China's Ocean Frontier: International Law, Military Force and National Development* (Sydney: Allen & Unwin, 1998). Like the 2016 International Arbitration on the South China Sea, this book notes that China's claims to submerged features like Macclesfield Bank were not in line with international law and that the EEZ boundary provisions of the UN Convention on the Law of the Sea did not apply to islands that could not support human habitation. See also Greg Austin, 'Strategic Military Geographies in the South China Sea', in Stuart Pearson, Jane L. Holloway and Richard Thackway (eds), *Australian Contributions to Strategic and Military Geography,* (Gewerbestrasse: Springer, 2018), pp. 109–27.

89 Or, in the case of the Spratly Islands, possibly 1939, when Japan annexed them two weeks prior to its invasion of Hainan Island.

90 See Kimie Hara, 'Rethinking the "Cold War" in the Asia-Pacific', *Pacific Review,* vol. 12, no. 4, 1999, pp. 515–36.

91 Kristen Huang, 'South China Sea: Chinese Military Holds Drills Near Paracel Islands for a Third Time This Year', *South China Morning Post*, 28 September 2020, https://www.scmp.com/news/china/military/article/3103393/south-china-sea-chinese-military-holds-drills-near-paracel; and Kristen Huang, 'China's Navy Drills in 4 Regions Show Ability to Counter US, Observers Say', *South China Morning Post*, 24 August 2020, https://www.scmp.com/news/china/military/article/3098671/chinas-navy-drills-4-regions-show-ability-counter-us-observers.

92 Kristen Huang, 'Chinese Military Fires "Aircraft-carrier Killer" Missile into South China Sea in "Warning to the US"', *South China Morning Post*, 26 August 2020, https://www.scmp.com/news/china/military/article/3098972/chinese-military-launches-two-missiles-south-china-sea-warning; and Catherine Wong, 'US–China Relations: PLA Bombers Carry Out "Attack Exercise" in South China Sea', *South China Morning Post*, 30 July 2020, https://www.scmp.com/news/china/military/article/3095398/us-china-relations-pla-bombers-carry-out-attack-exercise-south.

93 Bill Hayton, 'China's Pressure Costs Vietnam $1 Billion in the South China Sea', *Diplomat*, 22 July 2020, https://thediplomat.com/2020/07/chinas-pressure-costs-vietnam-1-billion-in-the-south-china-sea/.

94 *Ibid*.

95 Robert Haddick, 'Salami Slicing in the South China Sea', *Foreign Policy*, 3 August 2012, https://foreignpolicy.com/2012/08/03/salami-slicing-in-the-south-china-sea/.

96 Demetri Sevastopulo and Kathrin Hille, 'US Warns China on Aggressive Acts by Fishing Boats and Coast Guard', *Financial Times*, 28 April 2019, https://www.ft.com/content/ab4b1602-696a-11e9-80c7-60ee53e6681d.

97 Bo Hu, '胡波：全球海上多极格局与中国海军的崛起' [Hu Bo: Global Maritime Multipolarity and the Rise of the Chinese Navy], Center for International Security and Strategy, Tsinghua University, 17 November 2020, http://ciss.tsinghua.edu.cn/info/nhwt/2655.

98 Stephen Chen, 'Freshwater Reservoir Found at One of Beijing's Artificial Islands in the South China Sea', *South China Morning Post*, 28 June 2020, https://www.scmp.com/news/china/science/article/3090761/freshwater-reservoir-found-one-beijings-artificial-islands-south.

99 H.I. Sutton, 'China Builds Surveillance Network in South China Sea', *Forbes*, 5 August 2020, https://www.forbes.com/sites/hisutton/2020/08/05/china-builds-surveillance-network-in-international-waters-of-south-china-sea/.

100 'Malaysia Picks a Three-way Fight in the South China Sea', Asia Maritime Transparency Initiative (AMTI), 21 February 2020, https://amti.csis.org/malaysia-picks-a-three-way-fight-in-the-south-china-sea/.

101 'Update: Chinese Survey Ship Escalates Three-way Standoff', AMTI, 30 April 2020, https://amti.csis.org/chinese-survey-ship-escalates-three-way-standoff/.

102 Cliff Venzon, 'China Uses Banana Diplomacy in Philippines to Edge Out Japan', *Nikkei Asia*, 26 July 2019, https://asia.

nikkei.com/Politics/International-relations/China-uses-banana-diplomacy-in-Philippines-to-edge-out-Japan.

103 S.D. Pradhan, 'South China Sea: Dragon's Deployment of Coercive Economic Measures to Prop Up Its Position', *Times of India*, 22 October 2020, https://timesofindia.indiatimes.com/blogs/ChanakyaCode/south-china-sea-dragons-deployment-of-coercive-economic-measures-to-prop-up-its-position/.

104 Renato Cruz de Castro, 'After Four Years, the Philippines Acknowledges the 2016 Arbitral Tribunal Award!', AMTI, 27 July 2020, https://amti.csis.org/after-four-years-the-philippines-acknowledges-the-2016-arbitral-tribunal-award/.

105 Tashny Sukumaran and Bhavan Jaipragas, 'Malaysia Rebukes Beijing as South China Sea "Lawfare" Heats Up', *South China Morning Post*, 30 July 2020, https://www.scmp.com/week-asia/politics/article/3095406/malaysia-rebukes-beijing-south-china-sea-lawfare-heats.

106 S.D. Pradhan, 'South China Sea: Vietnam Approaches UN against China', *Times of India*, 14 April 2020, https://timesofindia.indiatimes.com/blogs/ChanakyaCode/south-china-sea-vietnam-approaches-un-against-china/.

107 US State Department, 'Fifth Anniversary of the Arbitral Tribunal Ruling on the South China Sea: Press Statement, Antony J. Blinken, Secretary of State', 11 July 2021, https://www.state.gov/fifth-anniversary-of-the-arbitral-tribunal-ruling-on-the-south-china-sea/.

108 Linked to Remote Access Trojan Nanhaishu, also known as TEMP.Periscope or APT40.

109 Also known as TropicTrooper, Keyboy or APT23.

110 Also known as APT30.

111 Also known as Spring Dragon or Thrip.

112 'Naikon APT: Cyber Espionage Reloaded', Check Point Research, 7 May 2020, https://research.checkpoint.com/2020/naikon-apt-cyber-espionage-reloaded/.

113 Unit 78020 was a technical-reconnaissance bureau in Kunming. See ThreatConnect, 'Project CameraShy: Closing the Aperture on China's Unit 78020', 2015, p. 74.

114 FireEye Threat Intelligence, 'Southeast Asia: An Evolving Cyber Threat Landscape', Special Report, March 2015.

115 Robert Falcone et al., 'Operation Lotus Blossom', Palo Alto Networks, 16 June 2015, https://www.paloaltonetworks.com/resources/research/unit42-operation-lotus-blossom.

116 Noushin Shabab, 'Spring Dragon – Updated Activity', SecureList by Kaspersky, 24 July 2017, https://securelist.com/spring-dragon-updated-activity/79067/.

117 Shannon Vavra, 'Symantec Finds That a "New" Chinese Hacking Group Has Actually Been Around for a Decade', *CyberScoop*, 9 September 2019, https://www.cyberscoop.com/thrip-lotus-blossom-symantec-china/.

118 Sara Moore et al., 'Anomali Suspects that China-backed APT Pirate Panda May Be Seeking Access to Vietnam Government Data Center', Anomali, 30 April 2020, https://www.anomali.com/blog/anomali-suspects-that-china-backed-apt-pirate-panda-may-be-seeking-access-to-vietnam-government-data-center.

119 Joey Chen, 'Tropic Trooper's USBferry Targets Air-gapped Environments', Technical Brief, Trend Micro, 12 May 2020, https://www.trendmicro.com/en_gb/research/20/e/tropic-troopers-back-usbferry-attack-targets-air-gapped-environments.html. 'Air-gapped' systems are computers or networks that have no permanent link to an external or internet-facing system outside an organisation. There is a presumption, entirely false, that air-gapped systems cannot be successfully penetrated by cyber attacks simply because they are not connected to external systems.

120 Mark Lechtik and Giampaolo Dedola, 'Cycldek: Bridging the (Air) Gap', Securelist by Kaspersky, 3 June 2020, https://securelist.com/cycldek-bridging-the-air-gap/97157/.

121 Global Research & Analysis Team, 'APT Trends Report Q1 2020', Securelist by Kaspersky, 30 April 2020, https://securelist.com/apt-trends-report-q1-2020/96826/.

122 Catalin Cimpanu, 'More than 200 Systems Infected by New Chinese APT "FunnyDream"', ZDNet, 17 November 2020, https://www.zdnet.com/article/more-than-200-systems-infected-by-new-chinese-apt-funnydream/.

123 Anni Piiparinen, 'Phishing in the South China Sea: Cyber Operations and Hybrid Warfare in the Troubled Waters', China–US Focus, 12 July 2017, https://www.chinausfocus.com/peace-security/phishing-in-the-south-china-sea-cyber-operations-and-hybrid-warfare-in-the-troubled-waters.

124 Adam Meyers, 'Meet CrowdStrike's Adversary of the Month for August: GOBLIN PANDA', CrowdStrike, 29 August 2018, https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-august-goblin-panda/.

125 'NanHaiShu: RATing the South China Sea', F-Secure, July 2016, https://blog-assets.f-secure.com/wp-content/uploads/2019/10/15163422/NanHaiShu.pdf.

126 'China Hacks the Peace Palace: All Your EEZ's Are Belong to Us', ThreatConnect, 20 July 2015, https://threatconnect.com/blog/china-hacks-the-peace-palace-all-your-eezs-are-belong-to-us/.

127 Matthew Tostevin, 'Chinese Cyber Spies Broaden Attacks in Vietnam, Security Firm Says', Reuters,

31 August 2017, https://www.reuters.com/article/us-vietnam-china-cyber-idUSKCN1BB0I5.

128 Mark Manantan, 'The Cyber Dimension of the South China Sea Clashes', *Diplomat*, 5 August 2019, https://thediplomat.com/2019/08/the-cyber-dimension-of-the-south-china-sea-clashes/.

129 *Ibid*.

130 Anni Piiparinen, 'China's Secret Weapon in the South China Sea: Cyber Attacks', *Diplomat*, 22 July 2016, https://thediplomat.com/2016/07/chinas-secret-weapon-in-the-south-china-sea-cyber-attacks/.

131 Brett Davis, 'Hacking Attack at Vietnam Airports Another Chapter in South China Sea Dispute', *Forbes*, 13 August 2016, https://www.forbes.com/sites/davisbrett/2016/08/13/hacking-attack-at-vietnam-airports-another-chapter-in-south-china-sea-dispute/.

132 Adam Kozy, 'Rhetoric Foreshadows Cyber Activity in the South China Sea', CrowdStrike, 1 June 2015, https://www.crowdstrike.com/blog/rhetoric-foreshadows-cyber-activity-in-the-south-china-sea/.

133 China reportedly issued a threat to attack Vietnamese bases if Vietnam did not stop its gas-drilling expedition in a contested block. See Bill Hayton, 'South China Sea: Vietnam Halts Drilling after "China Threats"'.

134 Elsa Kania, 'The PLA's Latest Strategic Thinking on the Three Warfares', *China Brief*, vol. 16, no. 13, 22 August 2016, https://jamestown.org/program/the-plas-latest-strategic-thinking-on-the-three-warfares/.

135 Cuihong Cai, '网络地缘政治:中美关系分析的新视角', 国际政治研究' 'Wǎngluò dìyuán zhèngzhì: zhōngměi guānxì fēnxī de xīn shìjiǎo' [Cyber Geopolitics: A New Perspective for the Analysis of Sino–US Relations], *International Politics Studies*, vol. 39, no. 1, 2018, p. 35.

136 See Mark Bryan Manantan, 'The People's Republic of China's Cyber Coercion: Taiwan, Hong Kong, and the South China Sea', *Issues & Studies*, vol. 56, no. 3, September 2020, pp. 1–29.

137 See 'Japan Urges China to Ensure New Coast Guard Law Follows Int'l Law', *Mainichi Daily News*, 29 January 2021; and Shuxian Luo, 'China's Coast Guard Law: Destabilizing or Reassuring?', *Diplomat*, 29 January 2021, https://thediplomat.com/2021/01/chinas-coast-guard-law-destabilizing-or-reassuring/.

138 See Marco Balduzzi et al., 'A Deep Dive into Defacement: How Geopolitical Events Trigger Web Attacks', Trend Micro, 2018, https://documents.trendmicro.com/assets/white_papers/wp-a-deep-dive-into-defacement.pdf.

139 Davis, 'Hacking Attack at Vietnam Airports Another Chapter in South China Sea Dispute'.

140 US State Department, 'US Position on Maritime Claims in the South China Sea', 13 July 2020, https://www.state.gov/u-s-position-on-maritime-claims-in-the-south-china-sea/.

141 James Dorsey, 'Uyghur Extraditions Reveal China's Growing Surveillance State', New Lens, 13 February 2018.