SecAlliance

China's Next 5 Year Plan

Implications for the Cyber Threat Landscape

May 2021

TLP: WHITE

Contents

This assessment seeks to frame The Chinese Communist Party's (CCP) upcoming, '5 Year Plan' (FYP) in the context of the cyber domain. In doing so, it provides assessments into how the CCP's priorities will affect the cyber threat landscape in the short, medium and long term.

Key Assessments

- There are several indications that the Chinese Communist Party (CCP) are becoming more overt, confident, and threatening globally.
- The scale and tempo of offensive cyber operations will almost certainly reflect this approach.
- The upcoming 5 Year Plan will likely be underpinned by a desire to drastically reduce foreign leverage and influence over the Chinese economy and the population. This will be coupled with an equally aggressive push to exert influence and control over international business, supply chains, information and governments.
- Cyber operations will play a key role in not only acquiring access and therefore a degree of control in these areas, but also in the manipulation of and exploitation of information and systems to further their objectives.
- The CCP is highly likely to continue engaging in M&A activity, whilst investing heavily in strategic industries with the intent of persuading nations in the outer sphere of western influence to adopt Chinese systems, services and technologies.
- It is highly likely they will continue to disentangle supply chains, focus on securing their own whilst discrediting and undermining Western supply chains. The CCP will continue to apply significant effort to dealing with the so-called ‘Five Poisons’.
- Alongside this, the CCP will concentrate heavily on trying to control the narrative around their handling of these issues, including through blocking and undermining information flows from social media, news outlets, and physical presence within institutions like universities.
- Based on these priorities, offensive cyber operations will likely consist of focused targeting of key sectors, critical national infrastructure, and the supply chain with the purpose of intellectual property theft, prepositioning, and supporting information operations.
- In the longer term, as China looks to exert dominance, undermine western technologies and systems and promote Chinese produced solutions, it is likely they will utilise disruption TTPs in both cyber and information operations.

> **Contested space always leads to rapid innovation that will help drive the 4th Industrial Revolution.**

Cyber security, if it was not already, will become more significant and will hopefully drive a resilience in the supply chain not yet seen. Finally, as the CCP adopts a higher operational tempo, possibly leveraging less skilled actors and proxies, this may provide intelligence researchers greater opportunity to observe activity and in turn provide better intelligence led decisions and security control optimisation.

Shanghai Interchange

What is a Five Year Plan?

FYPs are typically government initiatives that frame a nation's social and economic goals over a five year period. They typically align national goals and targets with detailed plans. The People's Republic of China have been framing their national objectives with five year plans since 1953 with the long term goal of transforming the Chinese economy from a "planned economy" to a "socialist market economy".

China's 14th FYP is set to be finalised and released in early 2021, but the 5th Plenum which occurred between 26th-29th October 2020 has given indications of what will be in the next plan. Following the 5th Plenum, two blueprints were released, the FYP and a 2035 vision. The 2035 vision is an extension of the FYP and provides a guide to the midterm vision. The release of a midterm vision is not typical and has major political implications, with clear indication from President Xi Jinping that he intends to remain in power for the mid-long term.

Shanghai, China

Uyghurs women reported providing prison labour

President Xi Jinping

What broad factors are driving the next Five Year Plan?

Wrestling with the ‘Five Poisons”

Currently, there are five issues that the CCP perceive as prominent threats to their control of mainland China. These are the Uyghurs and the associated independence movement, Tibetan independence movement, the pro-democracy movement within China, proponents of Taiwanese independence, and the Falun Gong religious movement.

Many of the current and proposed CCP policies, especially those that are designed to establish domestic socio-cultural control, as well as efforts to drive the narrative abroad, can be framed as a means of attempting to deal with these ‘poisons’.

This dual approach to establishing domestic control alongside projecting influence abroad is a principle that underpins not only the CCP’s approach to socio-cultural issues, but also their geopolitical and economic strategy as well. It is a concept that is likely to permeate the upcoming 5 year plan.

Socio-cultural control and projection

Current and future policies driven by the CCP are already seeping into socio-cultural domestic and foreign institutions. Language, education, sport, and social media are all a focus, and will likely be targeted by new laws and government-sponsored (cyber) operations in the short-to-long term. In addition to blocking external social influences (e.g. film, sport, social media), the CCP will likely seek to leverage their 'softer' influence in social media, via apps like TikTok and Twitter, through to the Chinese student communities within universities.

It is also of significance that China has more diplomatic sites – like embassies and consulates – across the world than any other country. This extensive physical presence and across different forms of media provides the CCP with the platform to steer the narrative and to block any form of criticism of the CCP in general and their operations against the Five Poisons. Overhauling Hong Kong's education system[1] and banning the BBC's world service[2] are recent examples of this.

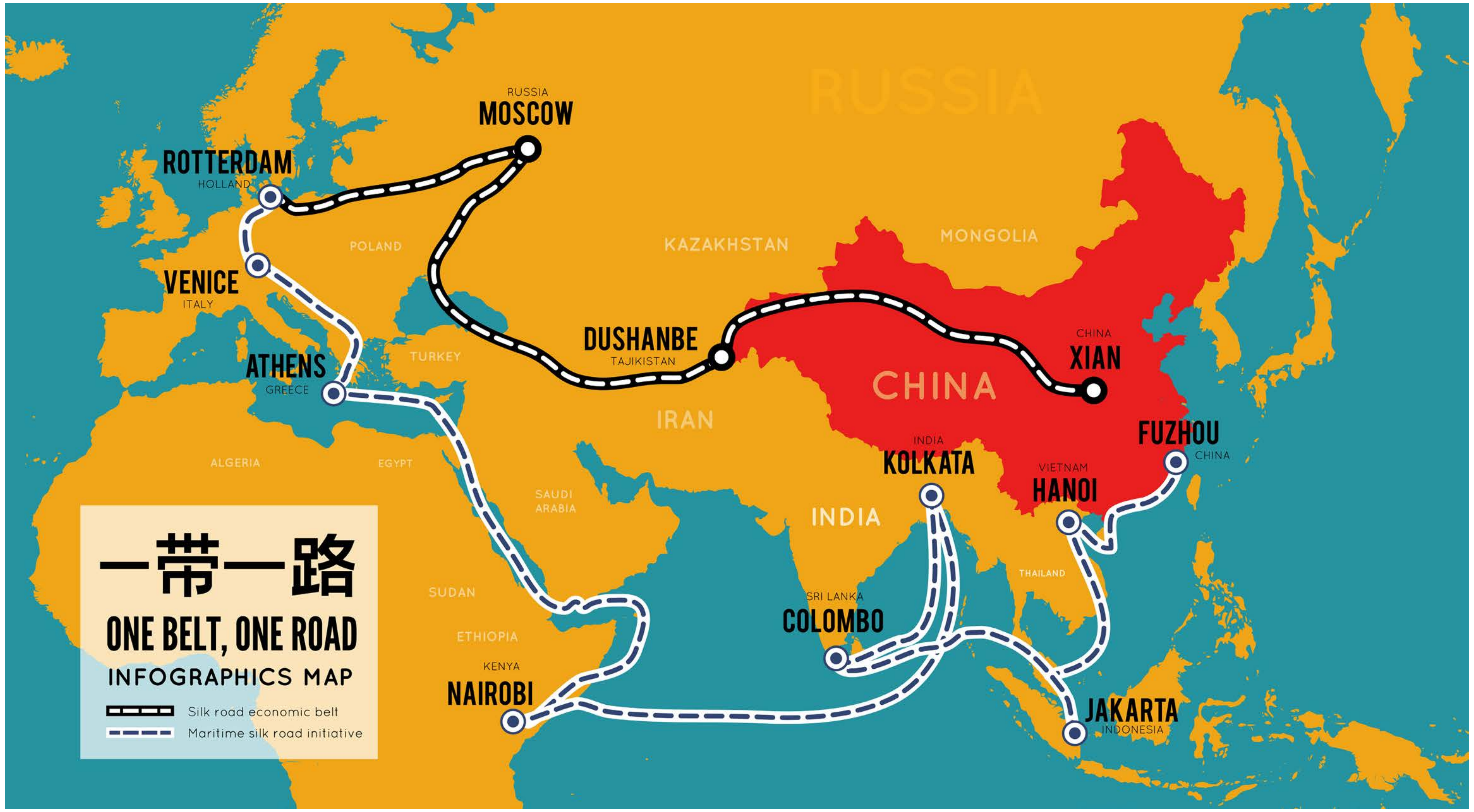
Pro-democracy protests in Hong Kong

“Indigenous innovation”: harvesting intellectual property and controlling the supply chain

Judging by the Plenum discussion, the language of the 5 Year Plan is likely to revolve around words like ‘entrepreneurship’ and ‘innovation’. However, the signs are again pointing to increased CCP control over business and commerce, whilst simultaneously rejecting external influence. For domestic businesses, innovation will not be fostered by foreign investment and expertise. Instead, it will be likely derived from the theft of intellectual property and business intelligence through numerous means, including cyber espionage, mergers & acquisitions, and legal measures.

There are numerous examples of this approach to business and commerce. One recent example being the cancellation of Ant Group’s (owned by Alibaba) IPO in November 2020, which was almost certainly caused by pressure from the CCP.[3] It provides a good example of the current reluctance to allow any foreign control over key businesses in mainland China. Other examples of this approach include: the CCP’s attempt to extricate its own financial services sector from the SWIFT network;[4] and leveraging the National Security Act to pressurise international financial institutions operating in Hong Kong. China also released its draft of the Personal Information Protection Law (PIPL), which is likely to be passed into law in early 2021.[5] Similar to GDPR, it sets out how organisations in the PRC must handle PII, and stipulates that an individual located in the PRC must be a point of contact for matters involving PII. Not only does this grant the individual with oversight into the internal functions of an organisation, but also enables the collection and transference of PII and likely other forms of data to the PRC.

Fundamentally, the BRI is an ambitious push to exert Chinese influence over the global supply chain, investing heavily in national infrastructure which can be controlled and leveraged depending on the CCP’s economic and geopolitical objectives.



China's proposed Belt and Road Initiative

A cornerstone policy that underpins the non-reciprocal approach to investment is the Belt and Road Initiative (BRI). The BRI is part of the wider strategy to reduce China's reliance on foreign goods and services, instead opting to establish its own supply chain, often in developing nations. The trade disputes especially between China and the US in 2020 is likely to have reinforced the CCP's policy to continue reducing their reliance on foreign trade, and thus the ability for rival nations to use trade as geopolitical tool against them.

Implications for the Cyber Threat Landscape

The factors listed above signal a more overt and aggressive push by Xi Jinping to project Chinese interests abroad, whilst rejecting foreign influence and investment. As such, it is almost certain that offensive cyber threat activity will be deployed to match this increase in aggression. The theft of various forms of information, information operations, and potentially disruptive attacks will likely be adopted to realise this strategy.

Tiananmen Gate, Beijing

The New York Stock Exchange

Likely targets of Chinese Cyber and conventional Espionage

The above covers the why behind the China's motivations.
The following sections cover our assessments into:

Who will be targeted?

How they will be targeted?

What will these attacks look like?

When will this activity take place?

WHO is most likely to be targeted?

When the details of the 5 year plan are released there is likely to be a good indication of what sectors will be a priority for the CCP. Nevertheless, assessments can be made based on previous 5 year plans and recent targeting behaviour.

High Tech

Sectors involved in the research, development, and production of advanced technology, including aerospace, artificial intelligence, biotechnology, information technology, semiconductors, quantum computing, robotics, advanced machinery and rail, deep sea and space technologies, and new materials, are likely to be targeted.

Government and Military

International and regional tensions involving China is highly likely to lead to ongoing targeting of political and military institutions in key rival countries. This will also likely include aerospace, defense and security contractors. Economic, and geopolitical rivalry will mean heavy targeting of the US; military posturing in the South China Seas and with Taiwan will mean targeting of South East Asian sectors; disputes with India are likely to lead to continued targeting of government and military sectors; tensions over Hong Kong will also lead to the heightened risk of targeting of government entities in Europe, especially the UK.

Financial Services

As such, areas relating digital currencies, interbank payments (akin to SWIFT), and e-commerce will be a focus. It is likely therefore that espionage operations will be directed towards core financial entities (large banks and Central Banks) and financial technology (FinTech) in order to collect information on the implementation of these emerging technologies.

Critical National Infrastructure

Finally, critical national infrastructure will likely be a priority sector for many Chinese actors. The targeting of India’s energy sector is an example of how geopolitical disputes lead to an increased risk[6] The telecommunications sector is highly likely to be of interest to Chinese actors. The banning of Huawei will likely mean that a new, cheap 5G communications equipment will be produced and sold worldwide under a different name. Additionally, Chinese actors will continue to see the telco sector as a valuable collection area to monitor and track individuals of interest to the CCP.

HOW will Chinese actors look to target organisations?

The Supply Chain

Targeting of the supply chain is highly likely to continue in the medium to long term. Chinese actors especially have proven how vulnerable and indeed how valuable the supply chain can be. Techniques whereby suspected Chinese actors have been able to 'trojanise' legitimate software, such as NetSarang (2017),[7] CCleaner (2017),[8] and ASUS (2019),[9] will likely be used again. Managed service providers (MSPs) will almost certainly continue to face intrusions by Chinese actors such as APT10 who will use the partner network to access a range of networks belonging to countries and sectors of interest to them and aligned with the 5 year plan.

Exploitation of External Facing Systems

While spear-phishing will remain a popular intrusion mechanism, Chinese actors have only very recently demonstrated their capability and willingness to deploy zero-day vulnerabilities to compromise valuable external systems. The use of a series of zero-days against Microsoft Exchange servers in March 2021 is a reminder that it can be very difficult to prevent exploitation by Chinese actors when they have capabilities to hand.[10]

Physical Access

New laws and measures brought in by the CCP allude towards a drive to embed more individuals sympathetic to the CCP into businesses. The aforementioned PIPL law is likely to part of the strategy to place employees that can act as malicious insiders for Chinese intelligence.

It is likely that alongside growing isolation, the Chinese intelligence services will use insiders more in the medium to long term.

Collaboration with Russia

With the CCP inclined to reduce reliance on Western-aligned systems and countries, particularly the US, it is likely that China will turn to geopolitical rivals. There is evidence for example of burgeoning co-operation in the technology space between the PRC and Russia. In March 2020, Huawei developed a joint research lab at the Moscow Institute of Physics and Technology with sponsorship from Huawei. The lab focuses on artificial intelligence and deep learning. It is a realistic possibility that this co-operation will go beyond these areas and into offensive cyber operations, involving the sharing of capabilities, tooling, exploits, etc.[11]

Chinese City of Shenzhen, a centre of Chinese innovation

WHAT are the likely objectives of these attacks?

Theft of R&D and Intellectual Property

To be self-sufficient and to advance the development of these previously mentioned key sectors, China will need a plentiful supply of intellectual property. Recent operations attributed to Chinese actors have seen them search and pivot to systems and repositories that are likely contain intellectual property. Documentation, source code, technical specifications, even some email correspondence will be considered valuable by Chinese actors.

Mergers & Acquisition Data

Targeting M&A data enables China to achieve several strategic goals that underpin the 5 year plan. Key insights into M&A allow China to commit to strategic purchases of organisations. Acquiring organisations is in itself another method to obtain intellectual property. Proposed mergers and acquisitions that undermine or go against the CCP's strategy outlined above will likely face heightened threat from M&A focused espionage activity. Law firms and financial services are likely to face an increased risk from this type of espionage given the amount of aggregated relevant data they are likely to hold.

Long Term Persistence And Prepositioning

One key characteristic of Chinese threat activity is the focus on achieving widespread persistence on compromised networks. Very rarely do their threat actors rely on just one entry point into the network, in case their presence is detected and/or the C2 connection broken. Linked to this is the concept of prepositioning, which is essentially maintaining persistence to priority systems, and potentially acting on them in the future depending on objectives. It is highly likely therefore, that Chinese actors will look to acquire this persistent access on networks that relate to priority sectors mentioned previously. Prepositioning on critical national infrastructure especially is a tactic likely to be employed by Chinese actors in the same way Russian actors do.

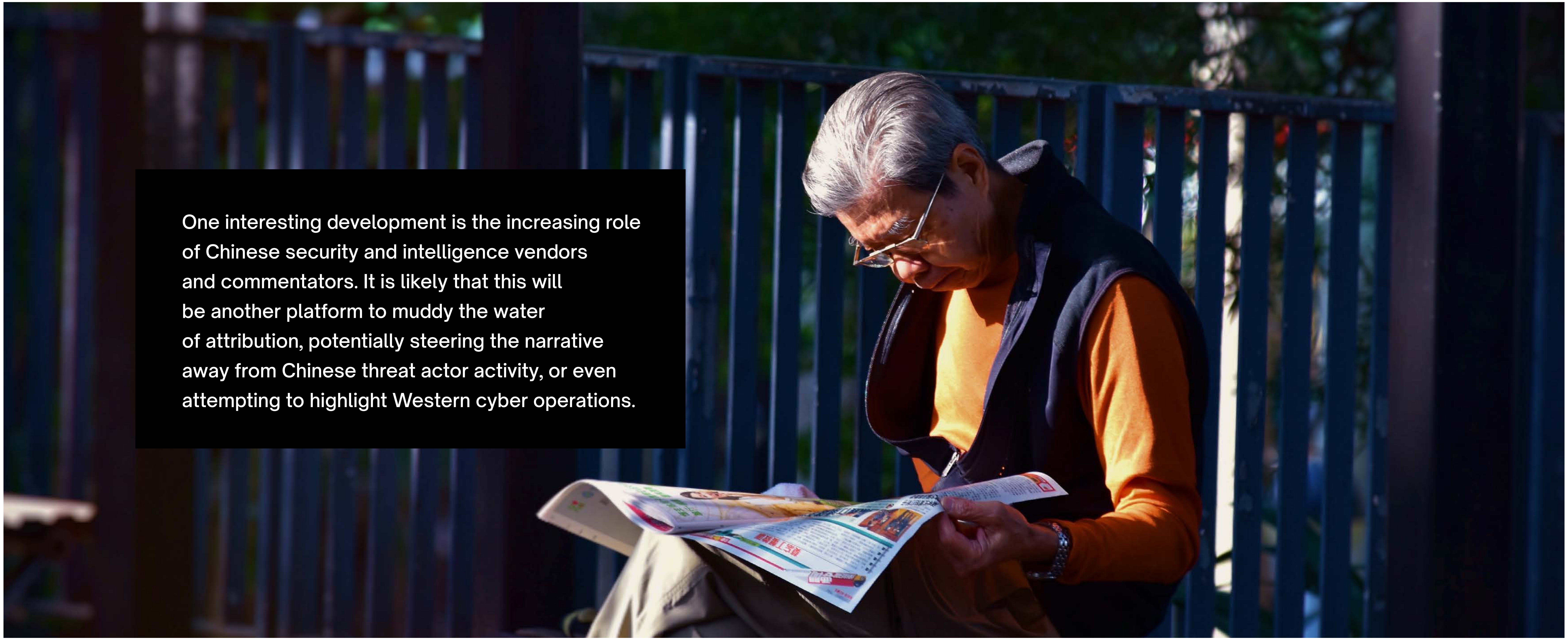
Information Operations

China's political isolation, domestic social clampdown, and commitment to tackling their 5 poisons, means that information operations and 'controlling the narrative' has become increasingly important space. Russian actors have demonstrated effectively how cyber operations can facilitate information operations to sway socio-cultural discourse, sow seeds of doubt, and influence major political events. It is highly likely that Chinese actors will adopt this approach more and more. Exfiltrating sensitive information and leaking it strategically is not something Chinese actors have been observed doing. Instead information is consumed solely by the CCP's intelligence apparatus. However, it is assessed as likely that with the impetus to control and influence the narrative, information operations like this will be adopted by Chinese groups.

Theft Of PII, Tracking & Monitoring Individuals

In addition to the exfiltration of IP and sensitive information, the collection of aggregated forms of PII will continue to be a priority for the CCP, who will use it to identify political, economic, or military individuals of interest. This ties into the concept of tracking individuals, both domestic and abroad. China has created organisations that act as a legal front for espionage activities, such as Chengdu 404. A big data product, "SonarX" was developed and described as an "Information Risk Assessment System".[12] However, this was a repository of searchable social media data used to monitor individuals. While any organisation that has large repositories of PII will be of interest, it is likely that telecommunications organisations will be targeted heavily, given their potential to track targets, collect phone numbers, call data, etc.

Tracking dissidents, journalists and activists will certainly play into the efforts to control the narrative around controversial domestic and international activity.



One interesting development is the increasing role of Chinese security and intelligence vendors and commentators. It is likely that this will be another platform to muddy the water of attribution, potentially steering the narrative away from Chinese threat actor activity, or even attempting to highlight Western cyber operations.

WHEN will this activity take place?

The underlying motivation, strategy, and targeting focus hasn't changed drastically since the last 5 year plan, nevertheless the changes that have been made will be felt by many. The current targeting activity and overtures by the CCP alludes to how the threat picture will look in the short-to-medium.

It is likely that the current activity and priorities will continue, however the future CTI outlook is that Beijing is finally becoming more overt, aggressive and confident in its operations. This will mark a change from the more delicate approach taken by the Xi Jinping's CCP up until this point.

The next 5 year plan will illustrate China's increasing ambition and assertiveness, which will in turn bring about a heightened threat from Chinese cyber activity in the medium to long term.

Great Hall of the People, in Beijing, China. Home of the CCP

About SecAlliance

SecAlliance is a threat intelligence product and services company, formed in 2007. We are a fully qualified and accredited security consultancy, as well as an intelligence portal vendor.

We deal in real intelligence, gathered, analysed and curated by true intelligence experts with real-world experience. We pride ourselves on the quality of our intelligence product and services, and the strong relationships built with our clients and partners.

It is our objective to help clients manage and reduce business risks, and build relevant intelligence-led security strategies, on a continuous basis. We help our clients understand their greatest threats, and develop their own intelligence capabilities.

Clients

SecAlliance is trusted by the most critical, most targeted organisations in the world including:

Financial Services: Central Banks, Retail Banks, Clearing Houses, Exchanges, Insurance Providers

Critical National Infrastructure: Energy Providers, Transportation, Infrastructure builders, Government Departments

Multi-national technology conglomerates: Manufacturing, Defence, Telecommunications

Experience

Our cyber intelligence team is made up of seasoned intelligence professionals with diverse backgrounds, ranging from conventional intelligence, law enforcement and consulting, to research and academia.

Intelligence-Led Red Team Assessments: Dedicated team used to deliver intelligence-led red team engagements since the inception of the CBEST initiative.

Intelligence Framework Creation: SecAlliance has been central in the creation and ongoing steering of core industry frameworks and professional bodies for threat intelligence-led red teaming. This includes CBEST and TIBER-EU.

Intelligence Sharing Communities: Designed, implemented and manage world-leading intelligence sharing communities for central banks across Europe.

References

[1] www.nytimes.com/2021/02/24/world/asia/hong-kong-national-security-law-education.html

[2] www.bbc.com/news/world-asia-china-56030340

[3] www.nytimes.com/2020/11/06/technology/china-ant-group-ipo.html

[4] www.reuters.com/article/us-china-banks-usa-sanctions-idUSKCN24U0SN

[5] www.lexology.com/library/detail.aspx?g=db4592e2-53c1-4cb6-91a9-94da1ee14b26

[6] www.recordedfuture.com/redecho-targeting-indian-power-sector/

[7] www.kaspersky.com/about/press-releases/2017_shadowpad-how-attackers-hide-backdoor-in-software-used-by-hundreds-of-large-companies-around-the-world

[8] https://www.vice.com/en/article/7xkxba/researchers-link-ccleaner-hack-to-cyberespionage-group

[9] www.kaspersky.com/about/press-releases/2019_operation-shadowhammer-new-supply-chain-attack

[10] www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/

[11] tass.com/world/1110991

[12] www.wsj.com/articles/justice-department-unseals-indictments-alleging-chinese-hacking-against-u-s-international-firms-11600269024

SecAlliance

☎ +44 (0) 20 7148 7475

✉ enquiries@secalliance.com

🌐 secalliance.com