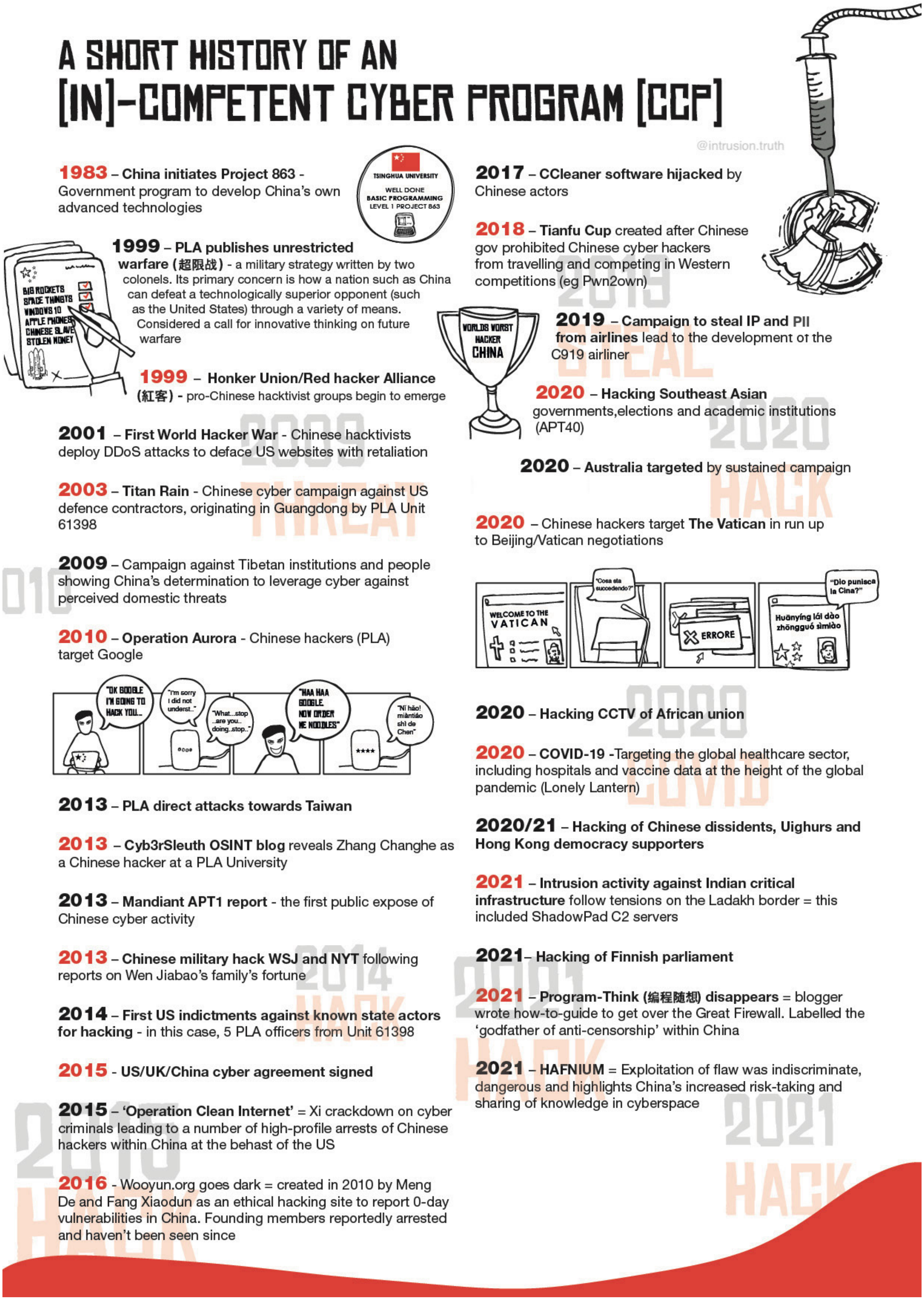
An (in)Competent Cyber Program – A brief cyber history of the ‘CCP’

intrusiontruth.wordpress.com/2021/07/29/an-incompetent-cyber-program-a-brief-cyber-history-of-the-ccp/

intrusiontruth July 29, 2021

Every so often, we like to take the opportunity to step back from our regular OSINT sleuthing and take stock about why we spend our time doing what we do.

So, we thought we would honour the 100-year anniversary of the Chinese Communist Party (CCP) by pulling together a brief history of how the Chinese cyber programme developed into what it is today and our musings on this trajectory.



A SHORT HISTORY OF AN [IN]-COMPETENT CYBER PROGRAM [CCP]

@intrusion.truth

1983 – **China initiates Project 863** - Government program to develop China's own advanced technologies

1999 – **PLA publishes unrestricted warfare (超限战)** - a military strategy written by two colonels. Its primary concern is how a nation such as China can defeat a technologically superior opponent (such as the United States) through a variety of means. Considered a call for innovative thinking on future warfare

1999 – **Honker Union/Red hacker Alliance (紅客)** - pro-Chinese hacktivist groups begin to emerge

2001 – **First World Hacker War** - Chinese hacktivists deploy DDoS attacks to deface US websites with retaliation

2003 – **Titan Rain** - Chinese cyber campaign against US defence contractors, originating in Guangdong by PLA Unit 61398

2009 – Campaign against Tibetan institutions and people showing China's determination to leverage cyber against perceived domestic threats

2010 – **Operation Aurora** - Chinese hackers (PLA) target Google

"OK GOOGLE I'M GOING TO HACK YOU...
"I'm sorry I did not underst.."
"What...stop ..are you.. doing..stop.."
"HAA HAA GOOGLE. NOW ORDER ME NOODLES"
"Nǐ hǎo! miàntiáo shì de Chen"

2013 – **PLA direct attacks towards Taiwan**

2013 – **Cyb3rSleuth OSINT blog** reveals Zhang Changhe as a Chinese hacker at a PLA University

2013 – **Mandiant APT1 report** - the first public expose of Chinese cyber activity

2013 – **Chinese military hack WSJ and NYT** following reports on Wen Jiabao's family's fortune

2014 – **First US indictments against known state actors for hacking** - in this case, 5 PLA officers from Unit 61398

2015 - **US/UK/China cyber agreement signed**

2015 – **'Operation Clean Internet'** = Xi crackdown on cyber criminals leading to a number of high-profile arrests of Chinese hackers within China at the behast of the US

2016 - Wooyun.org goes dark = created in 2010 by Meng De and Fang Xiaodun as an ethical hacking site to report 0-day vulnerabilities in China. Founding members reportedly arrested and haven't been seen since

2017 – **CCleaner software hijacked** by Chinese actors

2018 – **Tianfu Cup** created after Chinese gov prohibited Chinese cyber hackers from travelling and competing in Western competitions (eg Pwn2own)

2019 – **Campaign to steal IP and PII from airlines** lead to the development of the C919 airliner

2020 – **Hacking Southeast Asian** governments,elections and academic institutions (APT40)

2020 – **Australia targeted** by sustained campaign

2020 – Chinese hackers target **The Vatican** in run up to Beijing/Vatican negotiations

2020 – **Hacking CCTV of African union**

2020 – **COVID-19** -Targeting the global healthcare sector, including hospitals and vaccine data at the height of the global pandemic (Lonely Lantern)

2020/21 – **Hacking of Chinese dissidents, Uighurs and Hong Kong democracy supporters**

2021 – **Intrusion activity against Indian critical infrastructure** follow tensions on the Ladakh border = this included ShadowPad C2 servers

2021– **Hacking of Finnish parliament**

2021 – **Program-Think (编程随想) disappears** = blogger wrote how-to-guide to get over the Great Firewall. Labelled the 'godfather of anti-censorship' within China

2021 – **HAFNIUM** = Exploitation of flaw was indiscriminate, dangerous and highlights China's increased risk-taking and sharing of knowledge in cyberspace

Our take on the history of the Chinese Cyber Programme

Our take on the history of the Chinese Cyber Programme

The First World Hacker War

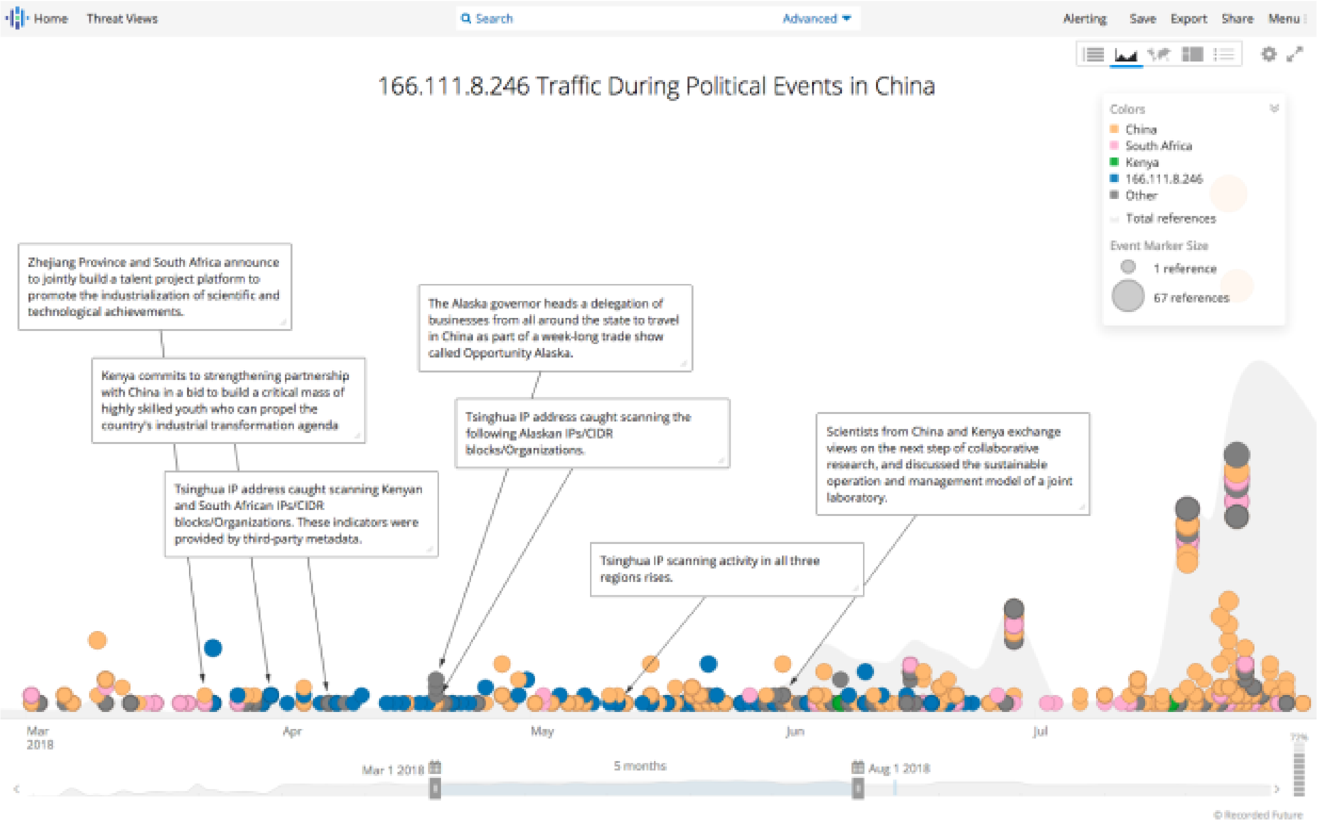
Cyber is entwined with the real-world. Not a particularly ground-breaking statement. But an important one to make. Real world tensions can spill into the cyber realm, and vice versa. Remember the 2001 China-US tension? To refresh your memory, a US EP-3 aircraft collided with the Chinese F-8 fighter jet and the Chinese pilot was killed. What followed was a sustained DDoS attack against US servers including defacement of the White House and military from Chinese hacktivists. US hacktivists retaliated and it became a cyber graffiti war of sorts. What we found interesting is that it wasn’t until the Chinese called out this behaviour as ‘web terrorism’ that the attacks stopped.

China: No longer hiding its strength

Former leader Deng Xiaoping touted the mantra of ‘*hide your strength and bide your time’ (*韬光隐晦*)*. Well, it seems that time has passed, and with Xi Jinping now at the helm, China is certainly showing its strength on the world stage. China is no longer hiding from the world.

China has aggressively and consistently built its national cyber program, prioritising education in computer science and technology and creating a recruitment pipeline of graduates from within its universities. Its focus seemingly being on offensive capabilities rather than security or intelligence analysis.

As evidenced in our bottom-heavy timeline (seen above), the CCP have increased their scope for hacking and stealing. What is obvious to any observer is that they hack indiscriminately – friends and enemies are fair game. China’s BRI initiative is even considered a driver of cyber activity, which this graphic from Security Affairs neatly highlights.



166.111.8.246 Traffic During Political Events in China

Zhejiang Province and South Africa announce to jointly build a talent project platform to promote the industrialization of scientific and technological achievements.

Kenya commits to strengthening partnership with China in a bid to build a critical mass of highly skilled youth who can propel the country's industrial transformation agenda

Tsinghua IP address caught scanning Kenyan and South African IPs/CIDR blocks/Organizations. These indicators were provided by third-party metadata.

The Alaska governor heads a delegation of businesses from all around the state to travel in China as part of a week-long trade show called Opportunity Alaska.

Tsinghua IP address caught scanning the following Alaskan IPs/CIDR blocks/Organizations.

Tsinghua IP scanning activity in all three regions rises.

Scientists from China and Kenya exchange views on the next step of collaborative research, and discussed the sustainable operation and management model of a joint laboratory.

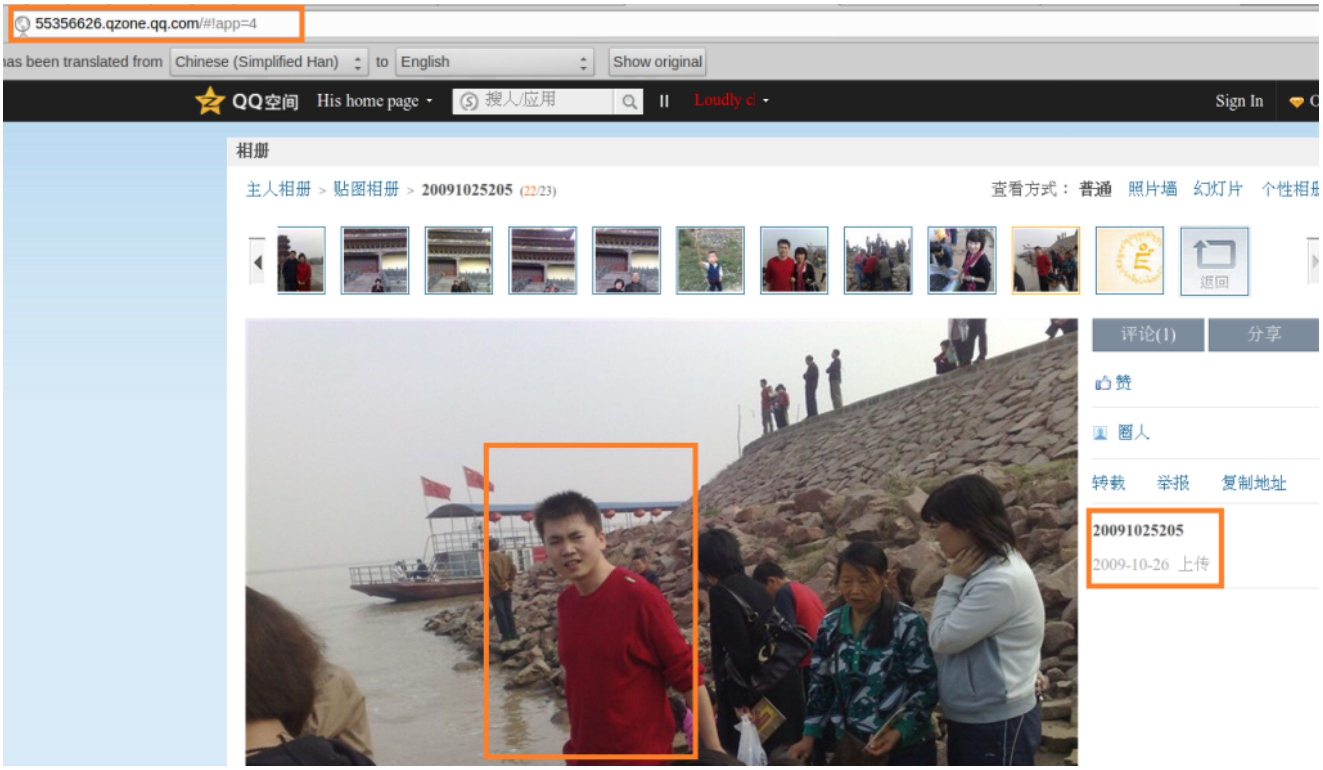
Tsinghua university IP traffic aligning with BRI initiatives

And their activity is at an industrial scale. This uptick reflects the CCP's priorities targeting intellectual property (IP) that have coincided with China's Five-Year Plans. It is now so common that barely a day goes by without another article reporting Chinese cyber theft. Provides us with lots of rich content though!

Disgruntled Hackers and ties to Academia

Back in 2013, a disgruntled hacker from the PLA (given the name Wang) wrote about his time in the PLA hacking for his country. "My only mistake was that I sold myself out to the country for some minor benefits and put myself in this embarrassing situation," he wrote on his blog. Few incentives and minimal benefits can lead some to defect and leave. Who knew. We wonder if conditions have changed in China since.

What hasn't changed however are the links between Chinese hackers and academia. Wang himself co-authored two academic papers whilst at the PLA university. And interestingly, it was this same year that Cyb3rSleuth outed Zhang Changhe. His 9-5 job was as an assistant professor at the PLA Engineering University. Cyb3rSleuth was one of the first public uses of OSINT to attribute Chinese cyber-attacks to named individuals within the Chinese system (having named 10 Chinese hackers in total). Kudos – an inspiration to our platform.



Cyb3rSleuth identifying Zhang Changhe from Chinese social media as a PLA hacker

Further, it was a Tsinghua university (清华大学) IP (self-proclaimed state-owned technological institution) that engaged in network reconnaissance targeting a number of countries actively working with China on their Belt and Road Initiative (BRI) – see image above.

The PLA led the way with cyber hacking back in the 90's and early 00's. However, in 2015 there appeared to be a shift within the Chinese government, with the PLA transferring the bulk of cyber operations over to the MSS. After all, when the PLA hack – it's very clear the direction of activity is coming from within the Party itself. This transfer (at least in the mind of the CCP) enabled plausible deniability following the public indictments of PLA unit 61398 a year earlier. After all, signing cyber agreements with a number for Western countries meant the Chinese military needed to 'hide their strength' and fade into the shadows.

Enter the MSS

As dedicated readers will know by now, it is the MSS that we at Intrusion Truth have focussed on for some time. And we do so given their continued support and engagement with criminal hackers. The MSS get something out of this relationship: deniability on the world stage (supposedly). But what do the criminal hackers get out of this? I'm sure some would say 'security'. After all, the relationship between citizen and the state is deliberately murky. In recent years, there is evidence that China will not prosecute hackers within its borders unless they attack China. However, as indictments have shown, the Chinese state cannot, and do not, protect their own.

China is a vast surveillance state. They monitor everything and everyone. Thus, one could say that their continued denial of Chinese APTs, or cries of rouge actors… is laughable. Chinese APTs leave traces of their activity on the internet. Whether this is due to their naivety, thinking the state will cover their activities, or their inability to understand that the Great Firewall does not actually prevent others connecting to Chinese infrastructure and seeing their mistakes – only they know. Perhaps they have started believing their own propaganda: '*We are world-leading, stealthy, and advanced threat actors'*. Or perhaps they simply do not care? What *is* evident though is their sloppiness, which is something we are more than willing to highlight, evidence and make public.

State-sponsored theft

Chinese IP theft represents one of the largest transfers of wealth in human history. And their targeting is indiscriminate – from innovation and R&D (rice and corn seeds, software for wind turbines, naval engineering and medical research), to personally identifiable information (PII) and sensitive government documents. Ultimately, anything that provides China an edge is fair game. The methods China uses rely less on physically stealing data, and more on MSS contract hackers being tasked to steal it from within China's borders.

There is a distinction made between a hacker and a criminal. Some might say one man's hacker is another's freedom fighter. Yet there are ethical and moral boundaries which the Chinese continue to violate. Utilising criminals to hack for the state's bidding, and to do so to steal IP from hard-working companies provides an unfair advantage to prop up Chinese businesses. They can't be pioneering or forerunners in their own right and seem to have concluded that they need to steal to gain a competitive advantage. And this is theft condoned and actively encouraged by the Chinese state. A state which is rapidly emerging into a global superpower. It is a powerful message to be sending the world.

Home-grown hēikè

The Wooyun.org shutdown appears to be one of the first events which highlights the CCP's direction of travel to essentially hoard offensive cyber capabilities by restricting the publication of 0-day vulnerabilities. In a statement on Sina, founder of Qihoo 360 Zhou

Hongyi (周鸿祎) stated that it was only ‘imaginary success’ when competing in overseas competitions. Rather, Chinese hackers and their knowledge should ‘stay within China’ so they could recognize the true importance and “strategic value” of the software vulnerabilities. Following this, China restricted travel for Chinese hackers, instead inviting them to compete in the home-grown Tianfu competition. The very same event where the winning vulnerability (Chaos) has been aggressively used to target Uyghurs.

The APT side hustle

An increasing number of reports highlight activity from Chinese APTs deploying ransomware on their victims and hacking for-profit, using the same tactics, tools and occasionally time as their MSS campaigns to conduct this side business. This has included the repurposing of state-sponsored malware in the gaming industry, stealing virtual currencies and selling malicious apps.

A really interesting article on China’s Sina Games portal details an interview with a Chinese hacker. He comments that online games are the most valuable part of the Chinese hacking industry. His reasoning? That China’s internet’s security consciousness is weak. Granted this article is old. But what is interesting is the openness to which a Chinese hacker talks of hacking Chinese netizens for profit. Yet it seems this focus might have changed over the years, with China’s hackers now focusing outside of the Firewall.

The Chinese government is permitting cyber criminals to conduct this activity within its borders. We have evidenced direct involvement of criminal hackers with the MSS, whilst others in the InfoSec community have proven clear Chinese state links to APT intrusion activity.

So, is it tactical toleration on behalf of the MSS to allow these hackers to conduct cybercrime outside of its borders for self-profit? Do the MSS pay their hackers so poorly that they have to let them make money on the side to keep them sweet? Or have the MSS lost control of the criminals it employs to do its dirty work?

We are also seeing greater sharing of tools, techniques and knowledge across Chinese APT groups. This is most evident with Hafnium, where a large number of Chinese APT groups were concurrently and recklessly using the MES vulnerability. Increased crossover in malware and TTPs points to greater knowledge sharing and a higher level of organisation than what China would have us believe.

Chain of command

As we know, Chinese APTs take direction from the Chinese state. This is a pattern starting with front companies, leading back to MSS contract hackers and ultimately to local and regional MSS bureaus. It is becoming increasingly obvious that there is something more at play here. A cyber campaign of sorts; coordinated, run and tasked by seniors within the MSS?

We have evidenced multiple Chinese APTs which have relationships with MSS officers and are behind global campaigns of cyber hacking. Yet China keeps denying responsibility, crying that claims of their APT activity is '*baseless with no evidence'*… we would recommend our blog as some light reading in this regard.

So, who is leading the Chinese Cyber Programme?

Let's look upwards. Someone is leading the coordination of China's cyber campaign. The multiple APTs, appearing across various provinces within China, are all linked by the MSS bureaus sitting behind these groups. And there is one person in charge of the MSS.

One person giving the direction.

One person overseeing the Chinese cyber programme.

That person?

Chen Wenqing (陈文清).

Cyber karma

Beijing come across as powerful within the offensive cyber space. After all, their state is actively, aggressively and successfully sponsoring malign cyber activity against fellow states, private companies, industry and individual people. Yet Beijing also see themselves as vulnerable.

The Cyberspace Administration of China (CAC) is the country's internet regulator and official body for enacting censorship. Recently, it stepped into the controversy around Didi (the ride-hailing app), ordering it to undergo a cybersecurity review ahead of its IPO in New York. The CAC later released a security-review revision in which it said companies holding personal data on at least one million users must apply for a cybersecurity review before any foreign listings.

Are China's actions causing reactions? It's almost as if the Chinese government know that their bulk collection of data on Chinese citizens is contentious. They lead the way in stealing PII from foreign governments and organisations – and the CAC know how powerful this data can be. Did they read our article outing APT10 using Uber receipts and are understandably worried about the vast data personal data holdings Didi might reveal on some of their senior officials?

Cyber karma – It is the guilty party that assumes everyone else is doing the same thing as them.

Conclusion

There has been 100 years of the CCP but only 38 years of the MSS. Yet there are a number of questions which remain unanswered (ie, we'd like more evidence to help answer, might we say):

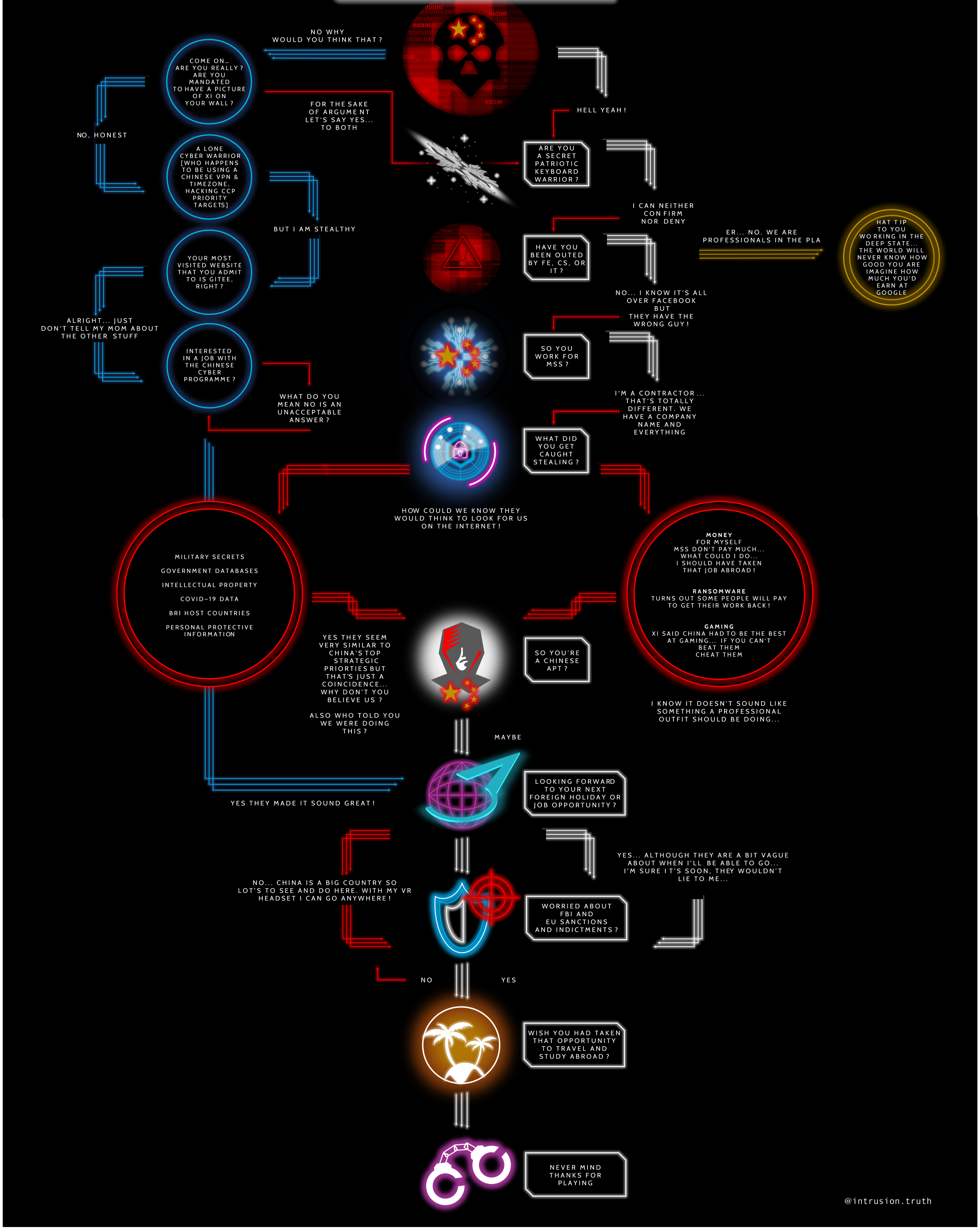
1. Does Xi know what the MSS are doing in cyber space?
2. Do the CCP understand how their actions undermine the positive narrative China would like the world to believe?
3. Does the benefit of the Chinese cyber programme outweigh the costs to the Chinese leadership?

Happy Birthday CCP

生日快乐. As our present to you for reaching this auspicious milestone, we promise to stick with you and keep a close eye on what the MSS cyber programme is up to. We will continue to pen more attribution pieces as long as you support your APTs and deny they are working for you.

Psst. Chinese cyber hackers: If you are reading this, please do enjoy our fun quiz we put together. We feel the flowchart neatly leads to the right outcome.

SO YOU'RE A CHINA BASED CYBER HACKER ?



NO WHY WOULD YOU THINK THAT ?

COME ON… ARE YOU REALLY ? ARE YOU MANDATED TO HAVE A PICTURE OF XI ON YOUR WALL ?

NO, HONEST

A LONE CYBER WARRIOR [WHO HAPPENS TO BE USING A CHINESE VPN & TIMEZONE, HACKING CCP PRIORITY TARGETS]

BUT I AM STEALTHY

YOUR MOST VISITED WEBSITE THAT YOU ADMIT TO IS GITEE, RIGHT ?

ALRIGHT... JUST DON'T TELL MY MOM ABOUT THE OTHER STUFF

INTERESTED IN A JOB WITH THE CHINESE CYBER PROGRAMME ?

WHAT DO YOU MEAN NO IS AN UNACCEPTABLE ANSWER ?

FOR THE SAKE OF ARGUMENT LET'S SAY YES... TO BOTH

HELL YEAH !

ARE YOU A SECRET PATRIOTIC KEYBOARD WARRIOR ?

I CAN NEITHER CONFIRM NOR DENY

HAVE YOU BEEN OUTED BY FE, CS, OR IT ?

ER... NO. WE ARE PROFESSIONALS IN THE PLA

HAT TIP TO YOU WORKING IN THE DEEP STATE... THE WORLD WILL NEVER KNOW HOW GOOD YOU ARE IMAGINE HOW MUCH YOU'D EARN AT GOOGLE

NO... I KNOW IT'S ALL OVER FACEBOOK BUT THEY HAVE THE WRONG GUY !

SO YOU WORK FOR MSS ?

I'M A CONTRACTOR ... THAT'S TOTALLY DIFFERENT. WE HAVE A COMPANY NAME AND EVERYTHING

WHAT DID YOU GET CAUGHT STEALING ?

HOW COULD WE KNOW THEY WOULD THINK TO LOOK FOR US ON THE INTERNET !

MILITARY SECRETS

GOVERNMENT DATABASES

INTELLECTUAL PROPERTY

COVID–19 DATA

BRI HOST COUNTRIES

PERSONAL PROTECTIVE INFORMATION

MONEY
FOR MYSELF
MSS DON'T PAY MUCH... WHAT COULD I DO... I SHOULD HAVE TAKEN THAT JOB ABROAD !

RANSOMWARE
TURNS OUT SOME PEOPLE WILL PAY TO GET THEIR WORK BACK !

GAMING
XI SAID CHINA HAD TO BE THE BEST AT GAMING... IF YOU CAN'T BEAT THEM CHEAT THEM

YES THEY SEEM VERY SIMILAR TO CHINA'S TOP STRATEGIC PRIORTIES BUT THAT'S JUST A COINCIDENCE... WHY DON'T YOU BELIEVE US ?

ALSO WHO TOLD YOU WE WERE DOING THIS ?

SO YOU'RE A CHINESE APT ?

I KNOW IT DOESN'T SOUND LIKE SOMETHING A PROFESSIONAL OUTFIT SHOULD BE DOING...

MAYBE

YES THEY MADE IT SOUND GREAT !

LOOKING FORWARD TO YOUR NEXT FOREIGN HOLIDAY OR JOB OPPORTUNITY ?

YES... ALTHOUGH THEY ARE A BIT VAGUE ABOUT WHEN I'LL BE ABLE TO GO... I'M SURE IT'S SOON, THEY WOULDN'T LIE TO ME...

NO... CHINA IS A BIG COUNTRY SO LOT'S TO SEE AND DO HERE. WITH MY VR HEADSET I CAN GO ANYWHERE !

WORRIED ABOUT FBI AND EU SANCTIONS AND INDICTMENTS ?

NO

YES

WISH YOU HAD TAKEN THAT OPPORTUNITY TO TRAVEL AND STUDY ABROAD ?

NEVER MIND THANKS FOR PLAYING

@intrusion.truth