
# INTELLIGENCE REPORT:

## HUGE FAN OF YOUR WORK:

### How TURBINE PANDA and China's Top Spies Enabled Beijing to Cut Corners on the C919 Passenger Jet

PUBLISHED OCTOBER 2019

**CROWDSTRIKE GLOBAL INTELLIGENCE TEAM**

web: WWW.CROWDSTRIKE.COM | twitter: @CROWDSTRIKE email: INTELLIGENCE@CROWDSTRIKE.COM

# FORWARD

Rarely in the infosec industry do cyber investigators get the luxury of knowing the full scope of their adversary's campaign—from tasking, to actual operations, all the way to completion. The oft-repeated mantra "Attribution is hard" largely stands true. Short of kicking down the door just as a cyber actor pushes *enter*, it is frustratingly hard to prove who is responsible for cyber attacks with 100% certainty. However, a series of recent U.S. Department of Justice (DoJ) indictments released over the course of two years, combined with CrowdStrike Intelligence's own research, has allowed for startling visibility into a facet of China's shadowy intelligence apparatus.

In this blog, we take a look at how Beijing used a mixture of cyber actors sourced from China's underground hacking scene, Ministry of State Security (MSS/国安部) officers, company insiders, and state directives to fill key technology and intelligence gaps in a bid to bolster dual-use turbine engines which could be used for both energy generation and to enable its narrow-body twinjet airliner, the C919, to compete against western aerospace firms. What follows is a remarkable tale of traditional espionage, cyber intrusions, and cover-ups, all of which overlap with activity CrowdStrike Intelligence has previously attributed to the China-based adversary TURBINE PANDA. These operations are ultimately traceable back to the MSS Jiangsu Bureau, the likely perpetrators of the infamous 2015 U.S. Office of Personnel Management (OPM) breach.


Figure 1. Leap Engine
Source: https://www.flightglobal.com/news/articles/cfm-delivers-first-leap-1c-to-comac-414924/

# PART I: THE TARGET

The story starts with a simple fact: Beijing accurately predicted that due to its rising economic status, China's middle class demand for air travel would far outpace its ability to supply aircraft and a domestic commercial aviation industry capable of supporting these logistics. Putting aside the obvious military-civil (军民融合) benefits[1] that turbine engines have for the energy and aviation sectors, much of China's strategic push into this industry is predicated by necessity. China is predicted[2] to succeed the U.S. as the world's largest aviation market by 2022, adding nearly 1 billion passengers by 2036. From China's 12th and 13th Five Year Plan to the increasingly scrutinized Made in China 2025 Plan,[3] numerous state strategic plans have named aerospace and aviation equipment as one of ten priority industries to focus on "leap-frog" developments.

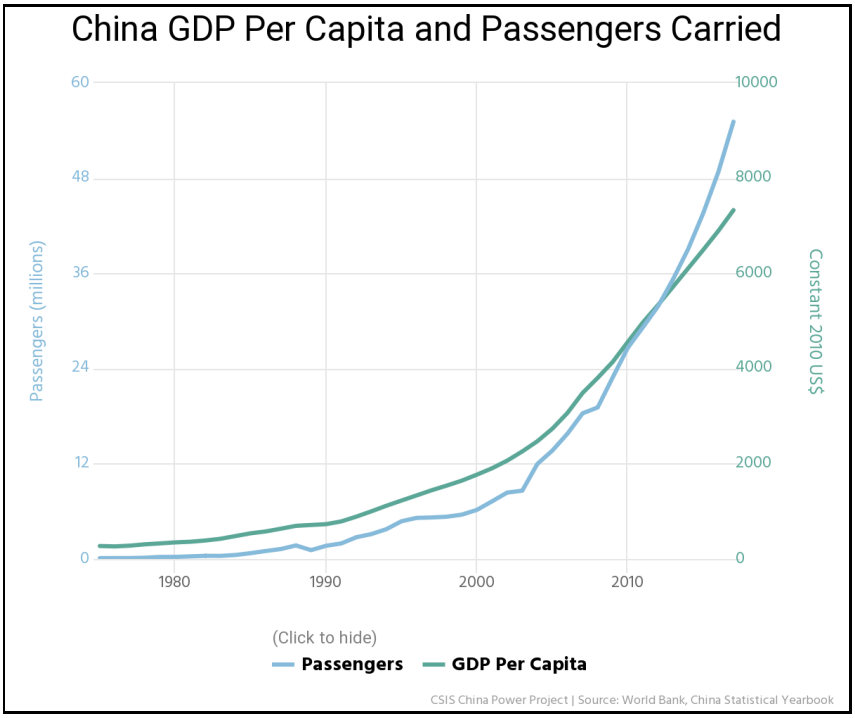


Figure 2. China's Exponential Growth in Air Travel Mirrored by Rise of China's Middle Class

Source: CSIS China Power Project

A major focus of this strategy centered on building an indigenous Chinese-built commercial aircraft designed to compete with the duopoly of western aerospace. That aircraft would become the C919—an aircraft roughly half the cost of its competitors, and which completed its first maiden flight[4] in 2017 after years of delays due to design flaws. But the C919 can hardly be seen as a complete domestic triumph as

[1] https://www.rand.org/content/dam/rand/pubs/research_reports/RR200/RR245/RAND_RR245.pdf
[2] https://www.weforum.org/agenda/2018/08/these-five-charts-show-how-rapidly-china-s-aviation-industry-is-expanding/
[3] https://www.uschamber.com/sites/default/files/final_made_in_china_2025_report_full.pdf
[4] https://www.theguardian.com/world/2017/may/05/chinas-first-home-made-plane-makes-maiden-flight

it is reliant on a plethora of foreign-manufactured components (see Figure 3).[5] Likely in an effort to bridge those gaps, a Chinese state-aligned adversary CrowdStrike calls TURBINE PANDA conducted cyber intrusions from a period of roughly 2010 to 2015 against several of the companies that make the C919's various components.

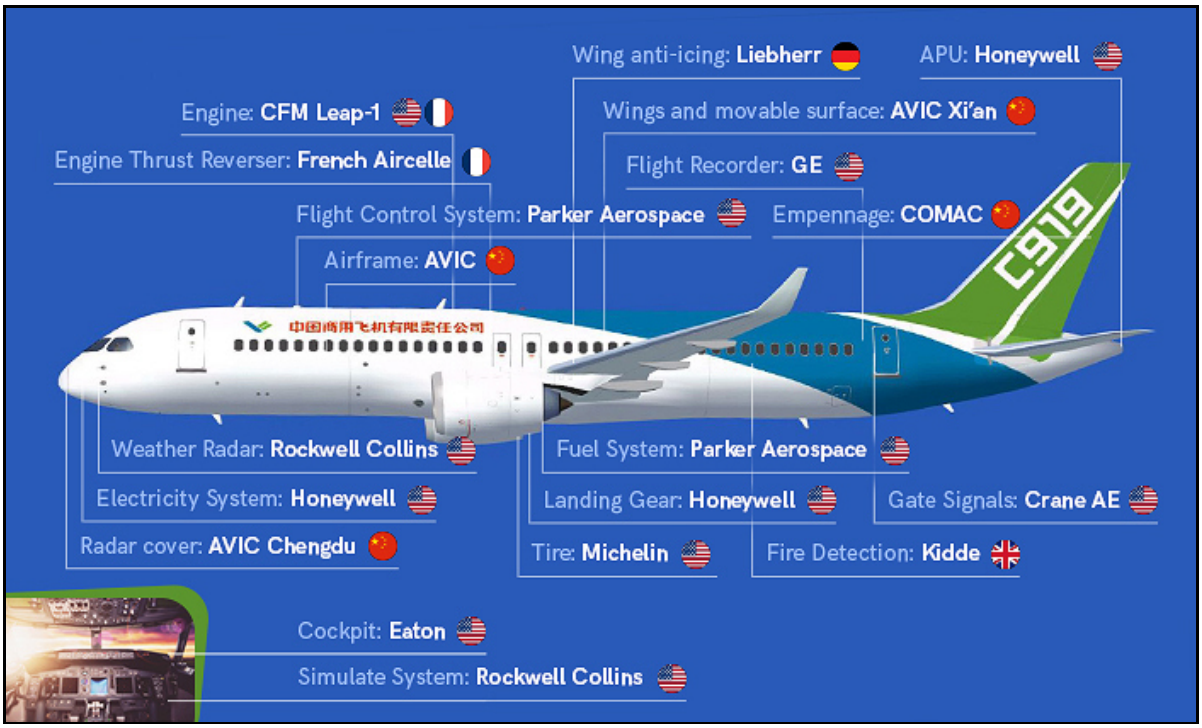


Figure 3. Components of C919
Source: https://www.aerotime.aero/aerotime.team/447-made-in-china-why-c919-can-hardly-be-called-chinese

Specifically, in December 2009, the state-owned enterprise (SOE) Commercial Aircraft Corporation of China (COMAC/中国商用飞机有限责任公司) announced it had chosen CFM International's (a joint venture between U.S.-based GE Aviation and French aerospace firm Safran, formerly Snecma) LEAP-X engine to provide a custom variant engine, the LEAP-1C, for the then-newly announced C919. The deal was reportedly signed in Beijing during a visit by then-French Prime Minister François Fillon.[6] Despite the early deal with CFM, both COMAC and fellow SOE the Aviation Industry Corporation of China (AVIC/中国航空工业集团公司) were believed[7] to be tasked by China's State-owned Assets Supervision and Administration Commission of the State Council (SASAC) with building an "indigenously created" turbofan engine that was comparable to the LEAP-X.[8]

In August 2016, both COMAC and AVIC became the main shareholders of the Aero Engine Corporation of China (AECC/中国航空发动机集团), which produced the CJ-1000AX engine. The CJ-1000AX bears

[5] https://www.aerotime.aero/aerotime.team/447-made-in-china-why-c919-can-hardly-be-called-chinese
[6] https://www.flightglobal.com/news/articles/cfm-international-to-provide-engines-for-comacs-c919-336414/
[7] http://www.xinhuanet.com/english/2017-05/04/c_136257538.htm
[8] http://www.miit.gov.cn/n1146290/n1146397/c4244228/content.html

multiple similarities to the LEAP-1C,[9] including its dimensions[10] and turbofan blades. The AECC conducted its first test as recently as May 2018, having overcome significant difficulties in their first mockups. Though it is difficult to assess that the CJ-1000AX is a direct copy of the LEAP-X without direct access to technical engineering specifications, it is highly likely that its makers benefited significantly from the cyber espionage efforts of the MSS, detailed further in subsequent blog installments, knocking several years (and potentially billions of dollars) off of its development time.

The actual process by which the CCP and its SOEs provide China's intelligence services with key technology gaps for collection is relatively opaque, but what is known from CrowdStrike Intelligence reporting and corroborating U.S. government reporting[11] is that Beijing uses a multi-faceted system of forced technology transfer, joint ventures, physical theft of intellectual property from insiders, and cyber-enabled espionage to acquire the information it needs. Specifically, SOEs are believed to help identify major intelligence gaps in key projects of significance that China's intelligence services then are likely tasked with collecting. It is assessed with high confidence that the MSS was ultimately tasked with targeting firms that had technologies pertaining to the LEAP-X engine and other components of the C919, based on timing and the details revealed in the DoJ indictments. For example, the first preparatory activity in January 2010 believed to be associated with TURBINE PANDA targeted Los Angeles-based Capstone Turbine and began just a month after choosing CFM as its engine provider.

This brings us to our culprits: the Jiangsu Bureau of the MSS (JSSD/江苏省国家安全厅) located in Nanjing. In Part II, we will discuss the JSSD's location, and its joint operations between the JSSD's cyber operators and its human intelligence officers.

## PART II: THE CULPRITS

From August 2017 until October 2018, the DoJ released several separate, but related indictments against *Sakula* developer YU Pingan[12], JSSD Intelligence Officer XU Yanjun[13], GE Employee and insider ZHENG Xiaoqing[14], U.S. Army Reservist and assessor JI Chaoqun[15], and 10 JSSD-affiliated cyber operators in the ZHANG et. al. indictment[16]. What makes these DoJ cases so fascinating is that, when looked at as a whole, they illustrate the broad, but coordinated efforts the JSSD took to collect information from its aerospace targets. In particular, the operations connected to activity CrowdStrike Intelligence tracked as TURBINE PANDA showed both traditional human-intelligence (HUMINT) operators and its cyber operators working in parallel to pilfer the secrets of several international aerospace firms.

[9] https://www.flightglobal.com/news/articles/china-completes-assembly-of-first-high-bypass-turbof-444526/
[10] https://www.flightglobal.com/news/articles/c919s-local-engine-alternative-powered-up-448721/
[11] https://www.whitehouse.gov/wp-content/uploads/2018/06/FINAL-China-Technology-Report-6.18.18-PDF.pdf
[12] https://regmedia.co.uk/2017/08/24/yu.pdf
[13] https://www.justice.gov/opa/press-release/file/1099881/download
[14] https://www.justice.gov/opa/pr/new-york-man-charged-theft-trade-secrets
[15] https://www.justice.gov/opa/press-release/file/1096411/download
[16] https://www.justice.gov/opa/press-release/file/1106491/download

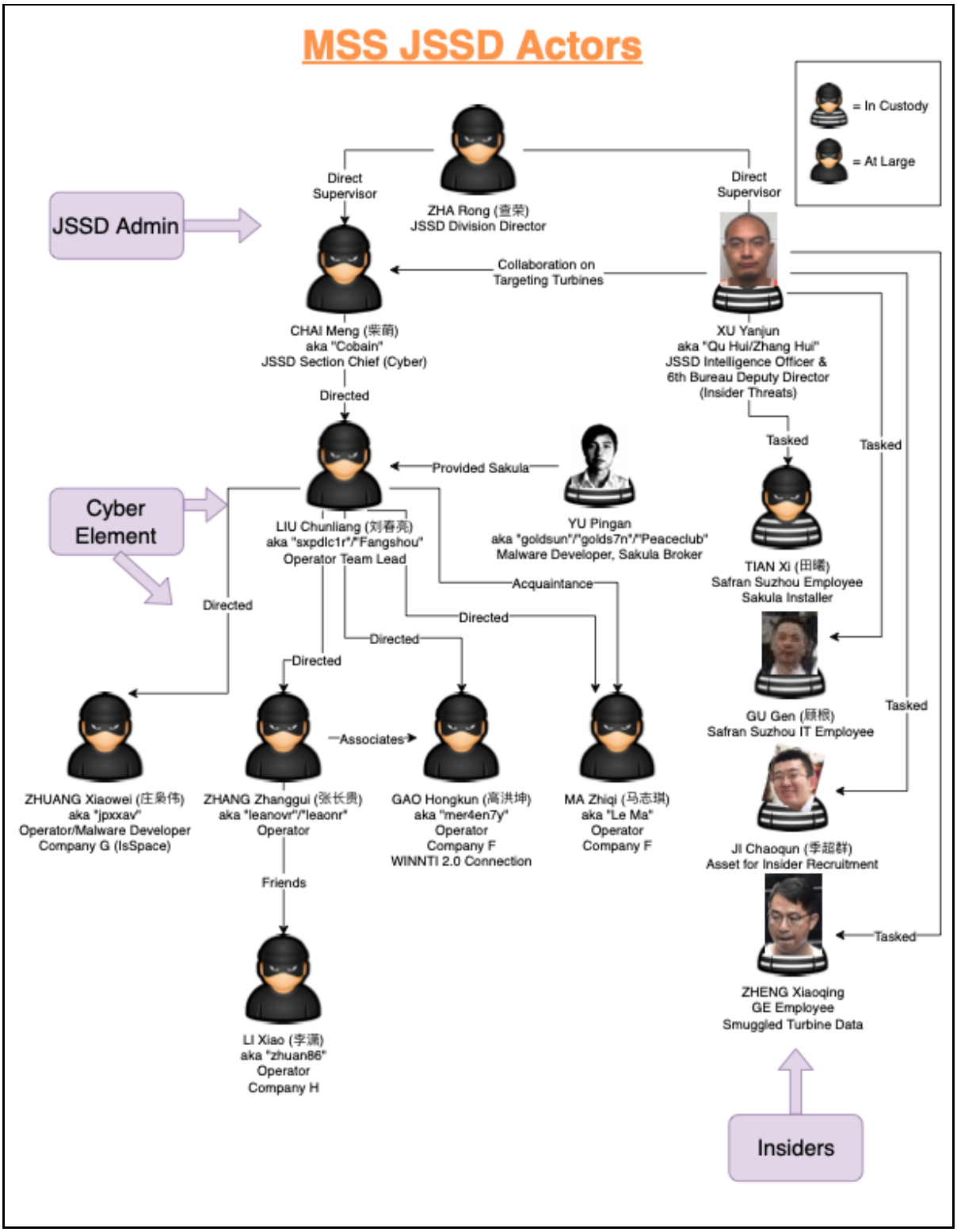


Figure 4. JSSD's Cyber Operations

As discussed in the previous section, it is believed that cyber targeting of aerospace firms by TURBINE PANDA cyber operators began in January 2010, almost immediately after the LEAP-X engine was chosen for the C919. The ZHANG indictment describes initial preparatory action that included compromising Los Angeles-based Capstone Turbine servers and later using a doppelganger site as a strategic web compromise (SWC) in combination with DNS hijacking (including a specific technique the indictment points out may have been borrowed from the Syrian Electronic Army/DEADEYE JACKAL[17]) to compromise other aerospace firms. From a period of 2010 to 2015, the linked JSSD operators are believed to have targeted a variety of aerospace-related targets—including Ametek, Honeywell, Safran, and several other firms[18, 19]—using two China-based APT favorites, *PlugX* and *Winnti*, and malware assessed to be unique to the group dubbed *Sakula*.

The same ZHANG indictment indicates that these operations were overseen by CHAI Meng (柴萌), who likely managed the JSSD's cyber operators as a pseudo Cyber Section Chief. Reporting to CHAI was the cyber operator team lead, LIU Chunliang (刘春亮/*sxpdlc1r/Fangshou*), who appeared to establish and maintain much of the infrastructure used in the attacks on various aerospace targets as well as organize the intrusions conducted by the operators ZHANG Zhanggui (张长贵/I*eanovr/Ieaonr*), GAO Hongkun (高洪坤/Mer4en7y), ZHUANG Xiaowei (庄枭伟/*jpxxav*), MA Zhiqi (马志琪/*Le Ma*), and LI Xiao (李潇/*zhuan86*). Many of these individuals are assessed to have storied histories in legacy underground hacking circles within China dating back to at least 2004.

Notably, LIU also appeared to broker the use of *Sakula* from its developer YU, as well as the malware *IsSpace* (associated with SAMURAI PANDA) from its likely developer ZHUANG.[20] LIU and YU's conversations about *Sakula* would be a critical factor in tying all of this disparate activity together as *Sakula* was believed to be unique to the JSSD operators and could be used to tie several aerospace intrusion operations into a single, long-running campaign.

## JSSD's HUMINT Efforts

Simultaneously, there was a HUMINT element to the JSSD's espionage operations against aerospace targets. XU Yanjun, was identified in his indictment[21] as the Deputy Division Director of the Sixth Bureau of the JSSD in charge of Insider Threats. XU affiliated himself with two cover organizations—Jiangsu Science and Technology Association (JAST) and the Nanjing Science & Technology Association (NAST)—when interacting with potential targets. XU also was reported as frequently associating with the Nanjing University of Aeronautics and Astronomics (NUAA), a significant national defense university controlled by China's Ministry of Industry and Information Technology (MIIT), that interfaces directly with many of China's top defense firms and state-owned enterprises. It is likely no coincidence that NUAA is a regular collaborator with state-owned enterprises (SOEs) COMAC and AVIC, the main shareholders of AECC, which went on to produce the LEAP-X inspired CJ1000-AX turbine engine for the C919.

[17] https://www.forbes.com/sites/andygreenberg/2013/08/28/syrian-hack-of-nytimes-com-and-twitter-could-have-inflicted-much-more-than-mere-embarrassment/#3b3746944944
[18] https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-black-vine-cyberespionage-group.pdf
[19] https://cyberthreatintelligenceblog.wordpress.com/2018/11/16/c0ld-case-from-aerospace-to-chinas-interests/
[20] https://regmedia.co.uk/2017/08/24/yu.pdf
[21] https://www.justice.gov/opa/press-release/file/1099881/download

Figure 5. MSS Intelligence Officer and Deputy Division Director XU Yanjun

Over the course of several years, XU would recruit both an insider at LEAP-X manufacturer General Electric (GE), ZHENG Xiaoqing, and a Chinese-born Army reservist, JI Chaoqun (季超群). ZHENG's background appears to have made him uniquely qualified to accurately assess turbine engine schematics, and it was clear from his indictment that he had received coaching on which sensitive information on GE's turbine technology to access and how to use steganography in an attempt to exfiltrate the information. JI, who entered the U.S. on an F-1 student visa to study electrical engineering in Chicago, was approached by XU (initially undercover as an NUAA professor) in December 2013 and eventually recruited to provide assessments on other high-value individuals in the aerospace industry for potential recruitment by the MSS. JI's position in the U.S. Army Reserve program known as Military Accessions Vital to the National Interest (MAVNI) provided a perfect cover for JI's assessment activities, as the program focuses on potential recruitment of foreign citizens with skills pertinent to national interest and legally residing in the U.S. Had it been successful, JI would have been handing XU other foreign-born recruitment candidates as they were about to enter U.S. military service on potentially sensitive projects.

## HUMINT-Enabled Cyber Operations and the Role of CrowdStrike's Own Blog

In February 2014, one of our own blogs described the relationship between cyber activity in 2012 against Capstone Turbine and an SWC targeting Safran/Snecma carried out by TURBINE PANDA, potentially exposing the HUMINT-enabled cyber operations described in some of the indictments. As described in the ZHANG indictment, on 26 February 2014, one day after the release of our "French Connection" blog publicly exposed some of TURBINE PANDA's operations, intel officer XU texted his JSSD counterpart, cyber director CHAI, asking if the domain *ns24.dnsdojo.com* was related to their cyber operations. That domain was one of the few controlled by cyber operator lead LIU, and several hours after CHAI responded to XU's text that he would verify, the domain name was deleted.

According to the ZHANG indictment, The deletion was believed to be carried out by GU Gen (顾根), Safran's Suzhou Branch IT manager, when Safran began investigating beaconing from that domain following the blog post and notification from the Federal Bureau of Investigation (FBI). GU had been

previously recruited around January 2014 by XU, and was able to act as a fixer for LIU and his team's operations. The indictment also showed that XU had also previously recruited another Safran Suzhou insider named TIAN Xi (田曦) in November 2013, giving him a USB drive with *Sakula* on it. On 25 January 2014, TIAN communicated to XU that he had installed *Sakula* on Safran's networks, and XU in turn texted confirmation to CHAI, who's team subsequently began their operations on Safran's networks over the next month.

## Where is the JSSD?

Though not much is publicly known about the internal organizational structure of China's secretive national intelligence service, the MSS is known to operate a number of large municipal bureaus, normally located in the provincial capitals. Through a mixture of open-source research and confirmation from sensitive source reporting, CrowdStrike Intelligence confirmed two locations that the JSSD likely operates out of:

1. Approximately 32°3'34.25"N, 118°45'41.83"E in the Gulou District of Nanjing - 江苏省南京市鼓楼区扬州路 1 号. Co-located in the headquarters of the Jiangsu Ministry of Public Security (MPS/公安部)


Figure 6. Street View of a JSSD Location

*Left, the characters for the JSSD (江苏省国家安全厅). Right, the characters for the Jiangsu MPS. The same street view on Baidu Maps[22] currently has both the JSSD characters and the red emblem (poorly) blurred out.*

22 https://maps.baidu[.]cn/#panoid=09002500121709081338424411I&panotype=street&heading=182.45&pitch=13.76&l=21&tn=B_NORMAL_MAP&sc=0&newmap=1&shareurl=1&pid=09002500121709081338424411I

Tellingly, the listed address of the JSSD's kindergarten is 50 Ninghai road, Gulou District (江苏省南京市鼓楼区宁海路 50 号), a building very near to the Jiangsu MPS headquarters.[23] Furthermore, MSS facilities are believed to often be co-located in MPS buildings both to provide plausible cover and due to their overlapping work on domestic security.

2. Approximately 31°58'45.65"N, 118°46'32.93"E in the Yuhua District of Nanjing - 江苏省南京市雨花台区软件大道 33 号


Figure 7. Architectural Mockup of JSSD Compound

A particular Nanjing architectural firm appears fairly proud of the job it did on this JSSD compound (see above), and prominently features pictures of architectural mockups of the building's outside, atrium, and even its gym as splash pages on its main site.[24] Again, the JSSD hanzi (江苏省国家安全厅) are directly on the site along with indications that it was built in 2009. A comparison with the street view[25] (see Figure 8) and corroboration with sensitive source reporting gives us fairly high confidence that this building and location is affiliated with the JSSD. A satellite view shows an array of satellite dishes out front as well.

23 https://jiangsu.youbianku.com/%E5%90%8D%E5%BD%95/%E6%B1%9F%E8%8B%8F%E7%9C%81%E5%9B%BD%E5%AE%B6%E5%AE%89%E5%85%A8%E5%8E%85%E5%B9%BC%E5%84%BF%E5%9B%AD

24 https://web.archive.org/save/http:/dadda.cn/show-19-79-1.html

25 https://maps.baidu[.]cn/#panoid=09002500121709131120474746L&panotype=street&heading=353.22&pitch=3.8&l=21&tn=B_NORMAL_MAP&sc=0&newmap=1&shareurl=1&pid=09002500121709131120474746

Figure 8. Front Entrance of a JSSP Building in Yuhua Resembling Architectural Mockup

In the next section, we'll discuss the aftermath of these operations, their connection to other Chinese cyber campaigns, and how they fit into China's larger strategy of "leapfrog" development.

## PART III: THE AFTERMATH

The arrests of MSS officer XU Yanjun, his insiders (ZHENG Xiaoqing and JI Chaoqun), and *Sakula* developer YU Pingan will ultimately not deter Beijing from mounting other significant cyber campaigns designed to achieve leapfrog development in areas they perceive to be of strategic importance. Though XU's arrest in particular was likely a massive boon to U.S. intelligence given he was the first MSS officer (not simply an asset) known to be arrested, China has not ceased cyber operations even after incidents tying GOTHIC PANDA[26] and STONE PANDA[27] to the MSS were exposed publicly.

The reality is that many of the other cyber operators that made up TURBINE PANDA operations will likely never see a jail cell. YU was arrested in 2017 following his attendance at a U.S.-based security conference, and CrowdStrike Intelligence sensitive source reporting indicated that following his arrest, the MSS issued strict orders for China's security researchers to be barred from participating in overseas conferences or Capture the Flag competitions, likely fearing a repeat occurrence and more arrests of its offensive talents.

In years prior to that directive, Chinese teams—such as those from Qihoo 360, Tencent, and Baidu—had dominated overseas competitions and bug bounties including Pwn2Own and CanSecWest, earning thousands of dollars in cash rewards for their zero-day exploits for popular systems such as Android, iOS, Tesla, Microsoft, and Adobe. Instead, the companies these researchers work for were required to provide vulnerability information to the China Information Technical Security Evaluation Center

[26] https://intrusiontruth.wordpress.com/2017/05/09/apt3-is-boyusec-a-chinese-intelligence-contractor/
[27] https://www.crowdstrike.com/blog/two-birds-one-stone-panda/

(CNITSEC/中国信息安全测评中心). CNITSEC was previously identified by CrowdStrike Intelligence and other industry reporting[28] as being affiliated with the MSS Technical Bureau and it runs the Chinese National Information Security Vulnerability Database (CNNVD/中国国家信息安全漏洞库), which was outed for its role in providing the MSS with cutting-edge vulnerabilities likely for use in offensive operations.[29]

However, even before this directive, it is likely that many of the vulnerabilities used in offensive MSS operations came from these researchers. Many of the senior security researchers and executives at Chinese security firms got their start in legacy domestic hacking groups such as Xfocus and went on to turn their talents into successful careers—some whitehat, some blackhat, and the large majority probably falling somewhere in the grey area. The majority of these firms are listed partners of the CNNVD (see the image below). NSFOCUS, for example, was formed out of the remnants of the commercialized faction of China's patriotic hacking group the Green Army; its hanzi characters are actually still the same as the original group's name. Venustech and Topsec were both listed as known Chinese state-affiliated contractors in leaked U.S. government cable. Topsec was also linked to campaigns against the aerospace sector and Anthem breaches in public reporting.[30]


Figure 9. Prominent Chinese Tech Firms Partnering with the MSS-Affiliated CNNVD

What is notable about the use of certain vulnerabilities and strains of malware sourced from the Chinese underground is that they often uniquely indicate which actors are responsible for which campaigns. In this case, *Sakula* is described in the YU indictment as being relatively unique and was provided to JSSD

[28] https://www.recordedfuture.com/chinese-mss-behind-apt3/
[29] https://www.recordedfuture.com/chinese-mss-vulnerability-influence/
[30] https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-black-vine-cyberespionage-group.pdf

lead operator LIU Chunliang by YU along with multiple other vulnerabilities that were used against aerospace firms by LIU and other cyber operators that comprised TURBINE PANDA operations. The usage of *Sakula* across multiple victims and the arrest of its developer, YU, by the FBI would prove critical for several reasons.

Industry reporting[31] outlined the overlapping similarities between activity at Ametek (one of TURBINE PANDA's victims) that exhibited certain Tactics, Techniques, and Procedures (TTPs) and the usage of *Sakula* in the Anthem breach publicly disclosed in 2015. As indicated by an FBI Flash Report[32] detailing the tools used in the U.S. Office of Personnel Management (OPM) intrusion, Sakula was named along with *FFRAT* and the *IsSpace* malware (tracked by CrowdStrike Intelligence as being used by SAMURAI PANDA and also connected to JSSD operators in the ZHANG indictment via cyber operator ZHUANG Xiaowei) in the OPM case, likely indicating the JSSD was also behind these operations.

Public reporting has long theorized that the same operators were behind the Anthem and OPM incidents, and that both operations were likely perpetrated by actors affiliated with the MSS. Further reporting tied a breach at United Airlines to the same group that perpetrated Anthem and OPM, reaffirming that those actors had interests in aviation as well.[33] It is likely that the DoJ indictments provided yet another piece to this complicated puzzle that saw the pilfering of the data of millions of cleared U.S. government workers funneled to China, a veritable intelligence gold-mine for recruiting potential future spies.

## The Bigger Picture

Even with the arrest of a senior MSS intelligence officer and a valuable malware developer, the potential benefits of cyber-enabled espionage to China's key strategic goals has seemingly outweighed the consequences to date. Beijing still has a long way to go before it has a completely independent domestic commercial aviation industry, as evidenced by the $45 billion USD deal to purchase 300 Airbus planes during President XI Jinping's recent visit to France.[34] XI inked a similar purchase agreement for 300 Boeing planes during a November 2017 visit to the U.S. Yet China still seeks to decrease its dependency on this duopoly and eventually compete on an even footing with them. Notably, China was the first country to ground Boeing's 737 MAX and tout its own air safety records, following a second deadly 737 MAX crash this year.[35]

In May 2017, weeks after the C919's successful maiden flight in China, AECC and Russia's United Aircraft Corp (UAC) announced a 50-50 joint venture (JV) called China-Russia Commercial Aircraft International Corp (CRAIC) to fund and design a new aircraft dubbed CR929 (see Figure 10), a wide-body jet designed to compete with the Airbus 350 and Boeing 787.[36] Though both countries will design much of the

[31] Ibid.
[32] https://info.publicintelligence.net/FBI-HackToolsOPM.pdf
[33] https://www.bloomberg.com/news/articles/2015-07-29/china-tied-hackers-that-hit-u-s-said-to-breach-united-airlines
[34] https://www.scmp.com/news/china/diplomacy/article/3003384/china-france-sign-us45-billion-deals-including-airbus-order?utm_medium=email&utm_source=mailchimp&utm_campaign=enlz-scmp_china&utm_content=20190327&MCUID=f85aea33ab&MCCampaignID=ea970c4480&MCAccountID=3775521f5f542047246d9c827&tc=5
[35] https://www.nytimes.com/2019/03/13/business/china-boeing.html
[36] https://www.reuters.com/article/us-china-comac-russia-idUSKBN18I0KZ

aircraft, the CR929's engines, onboard electrical systems, and other components will still likely need to be supplied by foreign suppliers.[37]


Figure 10. CR929 Airliner

Source: Reuters

Similar to the procedure for developing the C919, the JV is currently taking bids for an aircraft engine that will be used until a Chinese-Russian substitute can take its place; this appears likely to be the CJ-2000, an upgraded version of the CJ-1000AX used in the C919. Finalists in the bidding process may face additional targeting from China-based adversaries that have demonstrated the capability and intent to engage in such intellectual property theft for economic gain. It is unclear whether Russia, a state that also has experienced cyber operators at its disposal, would also engage in cyber-enabled theft of intellectual property related to the CR929.

The C919 still faces significant barriers to entry—namely, international certification and the current Sino-U.S. trade war. COMAC aims to have the C919 pass grueling certification standards by the end of 2020.

Notably, public reporting in February 2019 detailed a potential cover-up involving a November 2016 cyber intrusion at the Canada-based International Civil Aviation Organization (ICAO), the United Nations (UN) body that sets global civil aviation standards.[38] The documents indicate that the intrusion at ICAO was likely designed to facilitate a strategic web compromise (SWC) attack (similar to what TURBINE

[37] https://chinapower.csis.org/china-commercial-aviation/

[38] https://www.cbc.ca/news/canada/montreal/montreal-based-un-aviation-agency-tried-to-cover-up-2016-cyberattack-documents-show-1.5033733

PANDA did with Capstone Turbine and described in Part II of this series) that would easily provide a springboard to target a plethora of other aerospace-related as well as foreign government victims. Upon being alerted to the breach by the Aviation Information Sharing and Analysis Center (AISAC), the ICAO internal IT investigation staff was reportedly grossly negligent, and the cyber intruders may have had direct access to one of their superuser accounts. In addition, a file containing a list of all the potential organizations who were compromised by the incident mysteriously disappeared during further investigations.

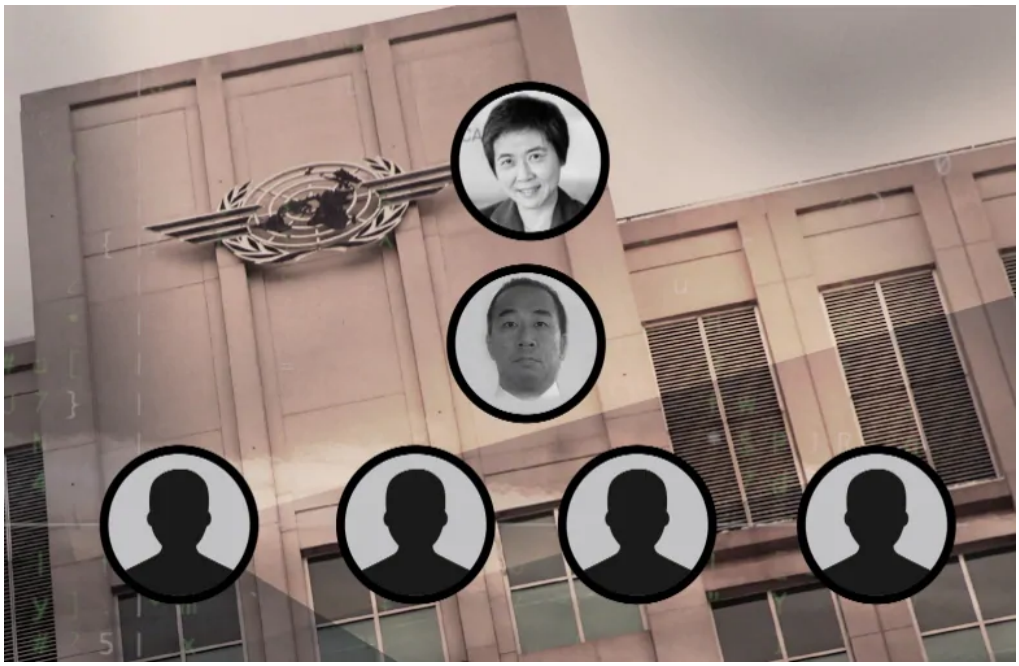

Figure 11. ICAO's Secretary General Gang LIU and IT Deputy Director James WAN Suspected of Having Mishandled Investigation of Breach

Source: Canadian Broadcasting Corporation (CBC)

Outside, third-party investigations point to China-based EMISSARY PANDA as the culprit. CrowdStrike Intelligence is unable to independently confirm this; however, EMISSARY PANDA has been previously observed targeting the aviation industry as well. Both the ICAO IT supervisor in charge of the mishandled internal investigation, James WAN, and Fang LIU, the ICAO's secretary general who shelved recommendations to investigate WAN and his four team members, were both found by CrowdStrike to have ties to China's aviation industry. LIU previously was a major figure at the Civil Aviation Administration of China (CAAC), one of several prominent Chinese state-owned enterprises (SOEs) tasked with advancing China's aviation industry.[39] WAN was previously connected to the Civil Aviation University of China (CUAC), another prominent institution in China's aviation industry research that is administered by CAAC. Though CrowdStrike Intelligence cannot make any high confidence determinations about the breach, the timing in 2016, the techniques (such as attempting an upstream SWC to target other industry victims), and the nature of the intrusion into ICAO is an eerily similar situation to GU Gen, the MSS-recruited IT manager at Safran's Suzhou branch who sought to cover up

[39] https://www.icao.int/DownloadDocs/liu_biography_en.pdf

TURBINE PANDA operations (see the previous blog post). LIU, WAN, and the four employees are all still employed at ICAO.

A major facet of the current Sino-U.S. trade war is forced technology transfer, which Beijing has used to great effect by siphoning intellectual property from foreign firms in exchange for providing joint ventures (JVs) and granting access to China's lucrative market, only to be forced out later by domestic rivals as they grow competitive with state subsidies and support. Under current laws, the C919's foreign suppliers (many of whom were targets of TURBINE PANDA operations) are required to physically assemble components in China through a JV with COMAC.[40]

It remains to be seen whether the high-level Sino-U.S. trade negotiations will result in limiting Beijing's ability to speed its aviation development through JVs, forced technology transfer, HUMINT operations, or cyber-enabled theft of IP. But the unprecedented visibility into how the MSS and its cyber operators enhance China's leapfrog development coming at this time is more than just a coincidence.

[40] https://apex.aero/2019/01/23/comac-aims-high