FIREEYE iSIGHT INTELLIGENCE

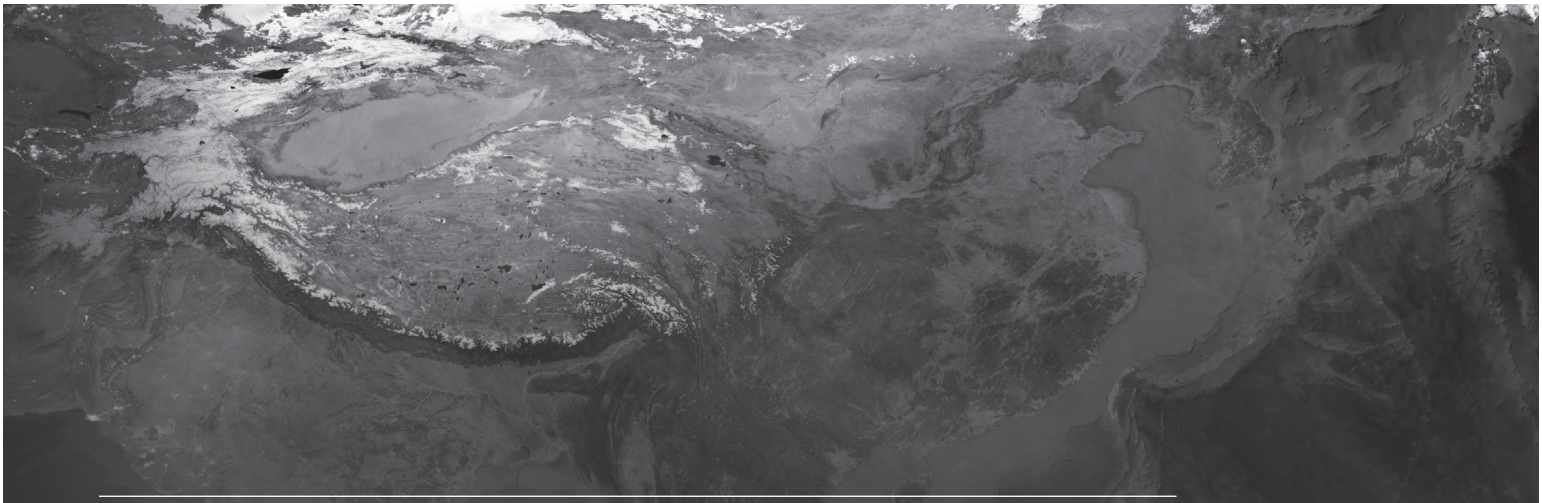
REDLINE DRAWN:

CHINA RECALCULATES ITS USE OF CYBER ESPIONAGE

FireEye

SPECIAL REPORT / JUNE 2016

CONTENTS



INTRODUCTION

On September 25, 2015, President Barack Obama and Chinese President Xi Jinping agreed that neither government would "conduct or knowingly support cyber-enabled theft of intellectual property"[1] for an economic advantage. Some observers hailed the agreement as a game changer for U.S. and Chinese relations, while skeptics saw this as little more than a diplomatic formality unlikely to stymie years of state-sponsored intellectual property theft.[2] [3] Since the agreement, there has been much discussion and speculation as to what impact, if any, it would have on Chinese cyber operations.

To investigate this question, FireEye iSIGHT Intelligence reviewed the activity of 72 groups that we suspect are operating in China or otherwise support Chinese state interests. Going back nearly three and a half years to early 2013, our analysis paints a complex picture, leading us to assess that a range of political, economic, and other forces were contributing to a shift in Chinese cyber operations more than a year prior to the Xi-Obama agreement.

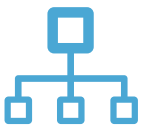
Between September 2015 and June 2016, we observed 13 active China-based groups conduct multiple instances of network compromise against corporations in the U.S., Europe, and Japan. During this same timeframe, other China-based groups targeted organizations in Russia and the Asia Pacific region. However, since mid-2014, we have observed an overall decrease in successful network compromises by China-based groups against organizations in the U.S. and 25 other countries. These shifts have coincided with ongoing political and military reforms in China, widespread exposure of Chinese cyber activity, and unprecedented action by the U.S. Government.

1 https://www.whitehouse.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states

2 http://www.cnn.com/2015/09/25/politics/us-china-cyber-theft-hack/

3 https://freedomhouse.org/blog/obama-xi-agreement-will-not-resolve-china-cybersecurity-threat

KEY FINDINGS

13	Between late-2015 and mid-2016, **13 suspected China-based groups have compromised corporate networks in the U.S., Europe, and Japan,** and targeted government, military, and commercial entities in the countries surrounding China.
25	Since mid-2014, we have seen a **notable decline in China-based groups' overall intrusion activity against entities in the U.S. and 25 other countries.** We suspect that this shift in operations reflects the influence of ongoing military reforms, widespread exposure of Chinese cyber operations, and actions taken by the U.S. government.
	Since taking power in late 2012, Chinese President Xi Jinping has implemented **significant military reforms intended to centralize China's cyber elements** and support a greater use of network operations.
	Public reports in recent years have **exposed Chinese cyber operations** and heightened public awareness of China's engagement in economic espionage. This likely provided the U.S. government with political support to **publicly confront China** over the issue.
	In 2014, the U.S. government began to take **unprecedented measures in response to claims of Beijing's cyber-enabled economic espionage.** Although many in the U.S. initially doubted that these actions would have any effect, they may have **prompted Beijing to reconsider the execution of its network operations.**
	**We have not seen evidence of a coordinated shift in the behavior of recently active China-based groups**—tactical changes appear to be specific to each group's mission and resources, and in response to public exposure of its cyber operations.

FACTORS INFLUENCING CHINESE CYBER OPERATIONS

CHINA IN TRANSITION: XI'S MILITARY AND DOMESTIC REFORMS CENTRALIZE CYBER OPERATIONS

Under Xi's leadership, the Chinese military began to implement many long-discussed strategies and concepts for conducting operations in cyberspace. These reforms have sought to centralize and emphasize military and government elements engaged in cyber activity. Combined with Xi's anti-corruption campaign cracking down on the illegitimate use of state resources, these reforms have begun materializing in what we believe is a more refined approach to cyber operations.

CHINESE DOMESTIC REFORMS

China has undergone significant changes under Xi's leadership, including a massive centralization of presidential power, reforms restructuring the country's military capabilities, and growing regional security concerns.[4] Xi's unrivaled authority has allowed him to advance a large-scale reorganization of the People's Liberation Army (PLA). The reforms aim to improve China's ability to conduct joint operations and win "informationized"[5] wars, deemphasizing the army in favor of a stronger focus on cyber and maritime capabilities and space assets.

Since 2012, Xi has also actively cracked down on government and military elements using state resources for their own agendas.[6]

DECEMBER 2013

Publication of the Science of Military Strategy describing "elite, specialized network warfare forces."[7]

JANUARY 22, 2013

Xi discusses plans to combat corruption, saying, "We must uphold the fighting of tigers and flies at the same time, resolutely investigating law-breaking cases of leading officials and also earnestly resolving the unhealthy tendencies and corruption problems which happen all around people," Xi said in a speech carried by the state news agency Xinhua.[8]

FEBRUARY 27, 2014

Xi establishes and heads the Central Internet Security and Informatization Leading Group.[9]

JUNE 26, 2014

Xi establishes the PLA Cyberspace Strategic Intelligence Research Center.[10]

MAY 2015

Chinese Ministry of National Defense publishes China's Military Strategy, which discusses use of cyber: "As cyberspace weighs more in military security, China will expedite the development of a cyber force, and enhance its capabilities of cyberspace situation awareness, cyber defense, support for the country's endeavors in cyberspace and participation in international cyber cooperation, so as to stem major cyber crises, ensure national network and information security, and maintain national security and social stability."[11]

JULY 6, 2015

Draft cyber security law submitted for comments.[12]

DECEMBER 31, 2015

Xi's PLA reorganization elevates cyber operations under the Strategic Support Force, placing cyber operations at the same level as other branches of the military.[13]

MARCH 26, 2016

Xi establishes the Cyber Security Association of China.[14]

APRIL 21, 2016

Xi establishes and leads the Joint Force Command to better promote integration of cyber capabilities into military operations.[15]

EXPECTED IMPACT ON CYBER OPERATIONS

- Greater coordination and fewer disparate government and military elements conducting cyber operations
- Deliberate integration of cyber operations with military activity
- More disciplined use of state resources to eliminate criminal and unauthorized use of state resources

4 https://www.foreignaffairs.com/articles/china/2014-10-20/chinas-imperial-president

5 http://eng.mod.gov.cn/Press/2015-05/26/content_4586805.htm

6 http://www.globaltimes.cn/content/902639.shtml

7 http://www.cnas.org/sites/default/files/publications-pdf/CNAS_WarringState_Chang_report_010615.pdf

8 https://www.theguardian.com/world/2013/jan/22/xi-jinping-tigers-flies-corruption

9 https://www.washingtonpost.com/world/chinese-president-takes-charge-of-new-cyber-effort/2014/02/27/a4bffaac-9fc9-11e3-b8d8-94577ff66b28_story.html

10 http://freebeacon.com/national-security/chinese-military-creates-high-level-cyber-intelligence-center/

11 https://news.usni.org/2015/05/26/document-chinas-military-strategy

12 http://www.jamestown.org/programs/chinabrief/single/?tx_ttnews%5Btt_news%5D=44924&cHash=db05078399a49339345c2957196d4073

13 http://blogs.cfr.org/cyber/2016/01/20/chinas-strategic-support-force-the-new-home-of-the-plas-cyber-operations/

14 http://timesofindia.indiatimes.com/tech/tech-news/China-launches-first-cybersecurity-organisation-Report/articleshow/51561355.cms

15 http://www.nytimes.com/2016/04/22/world/asia/china-xi-jinping-military-commander.html

CHINESE SECURITY CONCERNS

China is also facing pressing security concerns within the region, particularly from Taiwan, Japan, and claimants in the South China Sea dispute. Taiwan's recent election of the pro-independence Democratic People's Party has almost certainly prompted concern in Beijing. Despite the Taiwanese president's pledge to "maintain the status quo with China," Beijing almost certainly views the party's pro-independence mindset as a threat to its territorial sovereignty and future security. In addition, Japan's increased willingness to defend its regional interests, particularly through expanding the role of its Self-Defense Forces, may allow Japan to balance China more effectively, curbing Beijing's influence and regional ambitions. Lastly, territorial disputes in the South China Sea have intensified over the past few years, due in part to U.S. displays of military power and China's own island-building activities.

NOVEMBER 23, 2013

China establishes an air defense zone near disputed Senkaku/Diaoyu islands in East China Sea."[17]

DECEMBER 17, 2013

Japan approves a new security strategy and increases defense spending. China says that it is "closely watching Japan's security strategy and policy direction. Japan's unreasonable criticism of China's normal maritime activities and its hyping up of the China threat has hidden political motives."[18]

Foreign Ministry spokesman Hong Lei

MARCH 31, 2014

The Philippines asks the UN Permanent Court of Arbitration to determine territorial sovereignty in the South China Sea[19] "It is about defending what is legitimately ours…it is about guaranteeing freedom of navigation for all nations [and will help] preserve regional peace, security, and stability."[20] Philippine Foreign Secretary Albert del Rosario. The Philippines should "stop going any further down the wrong track so as to avoid further damage to bilateral relations."[21]

Foreign Ministry spokesperson Hong Lei

AUGUST 5, 2014

During the ASEAN regional forum, the U.S. and the Philippines suggest a "freeze" on island-building in the South China Sea, which China rejects.[22]

SEPTEMBER 10, 2014

When describing its island building in the South China Sea "China's activities on relevant islands and reefs of the Nansha Islands fall entirely within China's sovereignty and are totally justifiable. [Construction is] mainly for the purpose of improving the working and living conditions of people stationed on these islands."[23]

Foreign Ministry spokesperson Hua Chunying

JANUARY 16, 2016

Taiwan elections bring the pro-independence Democratic People's Party to Power "We hope Tsai can lead the DPP out of the hallucinations of Taiwan independence, and contribute to the peaceful and common development between Taiwan and the mainland."[24]

Editorial published in the Global Times, state-run paper.

"There is only one China in the World, the mainland and Taiwan both belong to one China and China's sovereignty and territorial integrity will not brook being broken up. The results of the Taiwan region election does not change this basic fact and the consensus of the international community."[25]

Chinese Foreign Ministry Statement

EXPECTED IMPACT ON CYBER OPERATIONS

- Continued espionage operations in support of China's security interests
- Consistent targeting of regional government and military elements
- Renewed need for a military focus, likely supported by cyber operations, to boost regional security interests

16 http://bigstory.ap.org/article/7255da3434534074b870e8264fb7ac9e/pro-china-party-likely-lose-taiwans-election

17 http://www.bbc.com/news/world-asia-25062525

18 http://www.bbc.com/news/world-asia-25411653

19 http://www.bbc.com/news/world-asia-26781682

20 http://www.bbc.com/news/world-asia-26781682

21 http://www.bbc.com/news/world-asia-26781682

22 http://thediplomat.com/2014/08/china-rejects-proposed-freeze-on-provocative-south-china-sea-moves/

23 http://thediplomat.com/2014/09/why-is-china-building-islands-in-the-south-china-sea/

24 http://www.reuters.com/article/taiwan-election-idUSKCN0UV02I

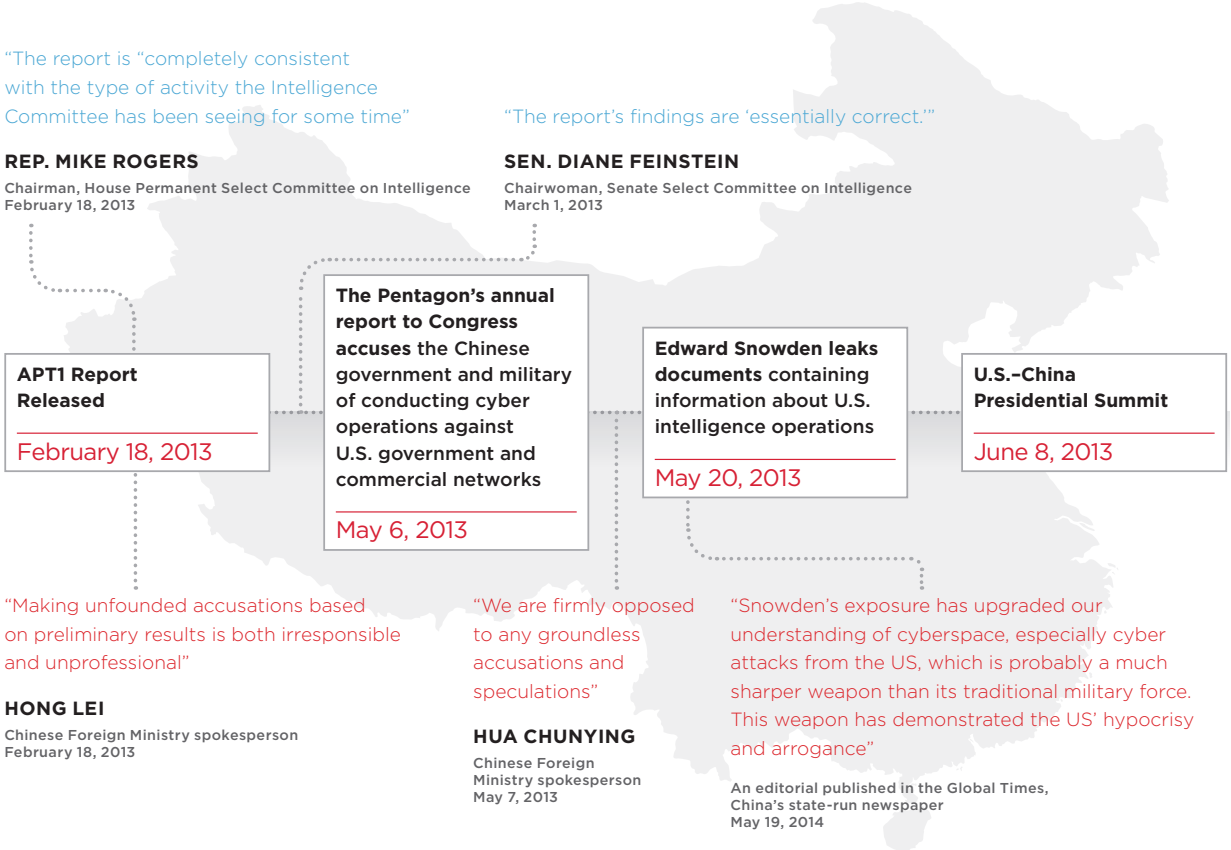
25 http://www.reuters.com/article/taiwan-election-idUSKCN0UV02I

CHINA EXPOSED: 2013 REPORTS AND DISCLOSURES JOLT GOVERNMENT CYBER OPERATIONS TO THE FOREFRONT OF THE U.S. SECURITY DIALOGUE

As Beijing embarked upon sweeping changes impacting its use of network operations, U.S. Government and defense officials wrestled with how to effectively confront China regarding its cyber espionage activity.[26] Although officials had discussed China's use of cyber espionage for years, the issue was not widely recognized in the public sphere. However, early 2013 saw multiple disclosures of breaches targeting media outlets, the release of our APT1 report, and additional reporting that attributed widespread corporate intellectual property theft to military units within China's People's Liberation Army (PLA). This exposure catapulted the issue of Chinese cyber espionage into the public consciousness, and likely provided the U.S. Government with increased momentum with which to confront Beijing - momentum that would quickly dissipate with Edward Snowden's disclosures of U.S. cyber activities.

In January 2013, the *New York Times* disclosed details of a network compromise targeting its reporters that was allegedly the work of the Chinese military.[27] Several weeks later, we released our APT1 report, attributing years of corporate intellectual property theft to Unit 61398 of the PLA. APT1 and the many other exposure reports that followed describe in detail the tools, tactics, and targets of Chinese cyber operations, laying bare evidence to support long-held suspicions of China's large-scale cyber espionage activity.

While the reports prompted outraged denials from the Chinese government, U.S. Government officials described the findings as "essentially correct" and "completely consistent with the type of activity [the U.S. government has] been seeing for some time."[28] [29] The threat posed by China's cyber operations emerged as a prominent theme in countless speeches, statements, and reports from U.S. leaders and federal agencies. In May 2013, the Pentagon's annual report to Congress directly accused China of using its military to conduct cyber operations against U.S. firms, and President Obama prepared to raise the issue at the U.S.–China Presidential Summit the following month.[30] However, Edward Snowden's coinciding disclosures of U.S. cyber activities diverted public attention to U.S. clandestine operations, complicating any leverage that the U.S. might have had to rebuke China over its economic espionage activities.[31]



26 http://www.reuters.com/article/us-usa-china-cyber-idUSTRE7934L2201111004

27 http://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html?_r=0

28 https://www.technologyreview.com/s/511981/unmasked-but-unfazed-chinese-hacking-group-is-still-active/

29 http://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html

30 http://www.bbc.com/news/world-asia-china-22798572

31 http://www.bbc.com/news/world-asia-china-22798572

INDICTMENTS AND SANCTIONS: U.S. UNDERTAKES MEASURES TO CONFRONT CHINESE ECONOMIC ESPIONAGE

In 2014, the U.S. Government began taking punitive measures against China, from indicting members of the PLA to raising the possibility of sanctions. These unprecedented measures, though met with skepticism in the U.S., have probably been taken much more seriously in Beijing.

In May 2014, the U.S. Department of Justice indicted five PLA officers, marking the first time that the U.S. Government has charged foreign government personnel with crimes related to commercial cyber espionage.[32] [33] Although China warned that the move "jeopardizes China-U.S. cooperation," the Department of Justice indicted another Chinese national, Su Bin, the following August for allegedly orchestrating a cyber-enabled economic espionage operation targeting U.S. defense companies.[34] [35] In 2015, President Obama authorized the sanctioning of individuals or entities involved in cyber activities that pose "a significant threat to the national security, foreign policy, or economic health or financial stability of the United States."[36] Later that year, news reports emerged claiming that the Obama administration had begun preparing a set of unprecedented economic sanctions against Chinese individuals and companies.[37]

32 http://www.wsj.com/articles/SB10001424052702304422704579571604060696532

33 http://www.nytimes.com/2014/05/20/us/us-to-charge-chinese-workers-with-cyberspying.html

34 http://www.nytimes.com/2014/05/20/us/us-to-charge-chinese-workers-with-cyberspying.html

35 https://www.fbi.gov/losangeles/press-releases/2014/los-angeles-grand-jury-indicts-chinese-national-in-computer-hacking-scheme-allegedly-involving-theft-of-trade-secrets

36 https://www.whitehouse.gov/the-press-office/2015/04/01/executive-order-blocking-property-certain-persons-engaging-significant-m

37 https://www.washingtonpost.com/world/national-security/administration-developing-sanctions-against-china-over-cyberespionage/2015/08/30/9b2910aa-480b-11e5-8ab4-c73967a143d3_story.html

U.S. GOVERNMENT ACTIONS IN RESPONSE TO CHINA'S CONTINUED ECONOMIC ESPIONAGE

U.S. Department of Justice Indicts Five PLA Officers for Their Alleged Roles in Supporting China's Cyber Economic Espionage

May 19, 2014

"This is a case alleging economic espionage by members of the Chinese military and represents the first ever charges against a state actor for this type of hacking. The range of trade secrets and other sensitive business information stolen in this case is significant and demands an aggressive response. This Administration will not tolerate actions by any nation that seeks to illegally sabotage American companies and undermine the integrity of fair competition in the operation of the free market."

ERIC HOLDER
U.S. Attorney General
announcing the indictment of five PLA officers

U.S. Department of Justice Charges Chinese Businessman Su Bin for his Alleged Role in Stealing Proprietary Technology Related to Boeing's C-17, and Lockheed's F-22 and F-35

August 18, 2014

"This plea sends a strong message that stealing from the United States and our companies has a significant cost; we can and will find these criminals and bring them to justice."

JOHN P. CARLIN
Assistant U.S. Attorney General for National Security
remarking on Su Bin's guilty plea, March 23, 2016

Executive Order Allows for the Freezing of Property of Individuals Engaged in Significant Malicious Cyber-Enabled Activity Posing Threats to the National Security, Foreign Policy, and Economy of the U.S.

April 1, 2015

"Starting today, we're giving notice to those who pose significant threats to our security or economy by damaging our critical infrastructure, disrupting or hijacking our computer networks, or stealing the trade secrets of American companies or the personal information of American citizens for profit."

PRESIDENT BARACK OBAMA
announcing the executive order

Widespread Reports of U.S. Government Considering Sanctions Against China Due to Cyber Economic Espionage

September 17, 2015

"We are preparing a number of measures that will indicate to the Chinese that this is not just a matter of us being mildly upset, but is something that will put significant strains on the bilateral relationship if not resolved"

PRESIDENT BARACK OBAMA
while speaking at a quarterly roundtable with U.S. business leaders a week prior to Xi's visit to the U.S.

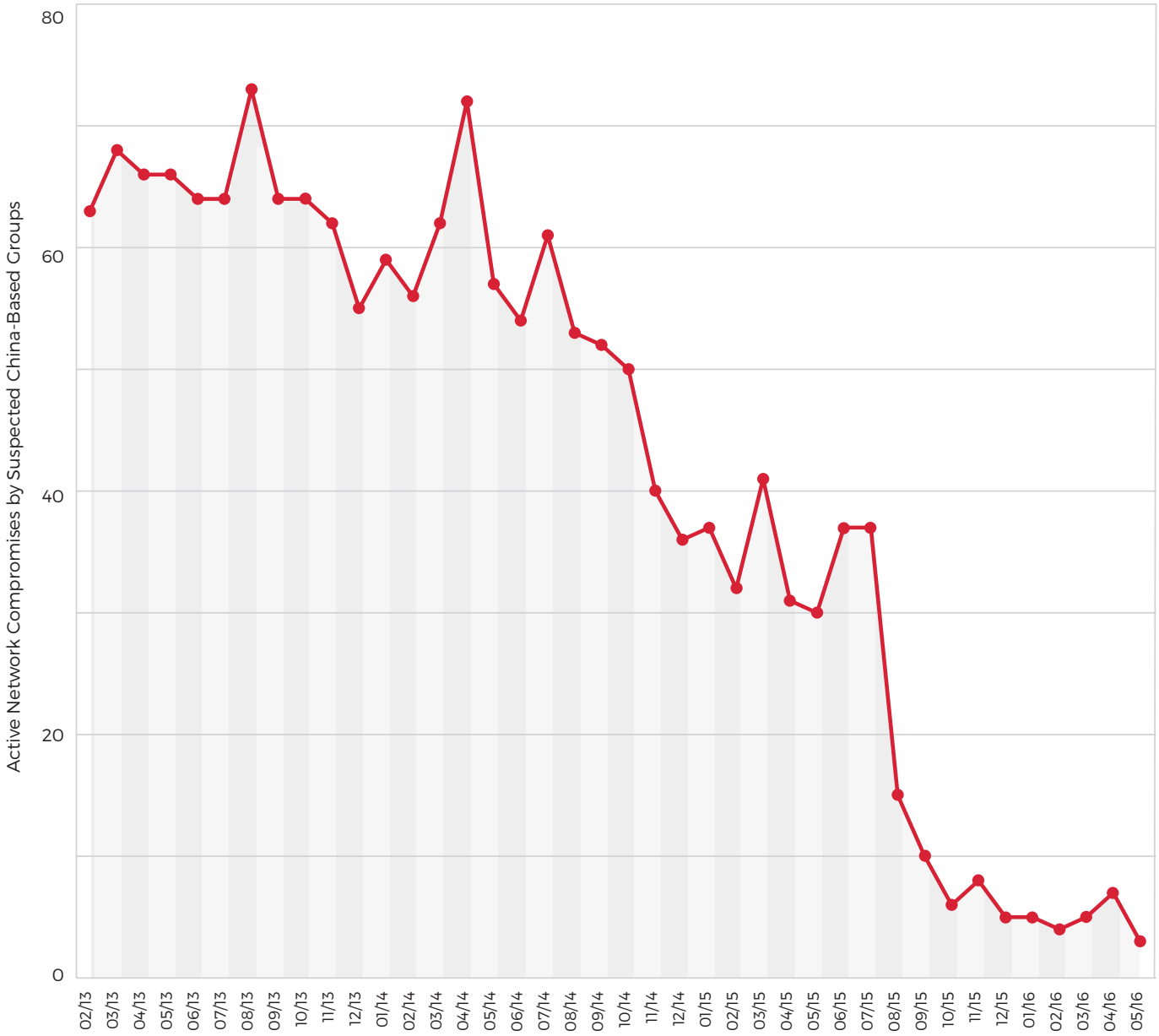
OBSERVED CHANGES IN CHINESE CYBER OPERATIONS

NETWORK COMPROMISES CONTINUE; MID-2014 DECLINE IN OVERALL ACTIVITY FROM SUSPECTED CHINA-BASED GROUPS

We examined the incidence of network compromises by suspected China-based actors dating back nearly three and a half years, to early 2013. Our data is based on our visibility, which includes a combination of sources (Mandiant Services engagements, FireEye as a Service, and FireEye's Dynamic Threat Intelligence data) that provide us with both a breadth and depth of coverage. While our visibility may vary from region to region depending on our customer base, we believe it provides a reasonable representation of Chinese cyber activity.

As shown in *Active Network Compromises Conducted by 72 Suspected China-Based Groups by Month* (in the following graph) a decline in activity began in mid-2014. During that time period we identified 262 network compromises (where a network compromise is defined as successful remote entry into a victim's network) conducted by 72 suspected China-based groups. Our data analysis reveals an overall decline in China-based intrusion activity against private and public sector organizations since mid-2014.

ACTIVE NETWORK COMPROMISES CONDUCTED BY 72 SUSPECTED CHINA-BASED GROUPS BY MONTH



262
total compromises

182 incidents occurred on U.S entities' networks

80 incidents affected entities in the following countries

Of the 262 compromises, 182 affected U.S. entities' networks while 80 affected entities outside of the U.S. This includes one instance where a suspected China-based group stole information from a privately held Chinese conglomerate. These compromises affected a total of 25 other countries in Europe, Asia, South America, the Middle East, and Africa. Following are the specific countries, listed by frequency of incident:

Great Britain
Japan
Canada
Italy
Switzerland
Germany
Netherlands
India
Australia
Denmark
Philippines
Sweden
Taiwan
Brazil
China
Colombia
Egypt
France
Hong Kong
Israel
Korea
Norway
Saudi Arabia
Singapore
Tunisia

Although we have continued to see suspected China-based groups compromise corporations' networks in the U.S., Europe, and Japan and target entities in the countries surrounding China through late 2015 and into 2016, our data shows an overall decline in compromises that began in earnest in mid-2014 – more than a year before the Xi-Obama agreement. While there was a subsequent drop-off in activity leading up to President Xi's September 2015 visit to the U.S., possibly orchestrated to avoid any negative publicity during the meeting, it occurred during what was already an ongoing decline in network intrusions.

THE BASIS FOR 'CHINA-BASED'

Attributing cyber activity to a geographic location is a complex process. We are never fortunate enough to be presented with a "smoking gun"; instead we rely on the careful accumulation of multiple pieces of evidence in sufficient quantity over time. Inevitably, as we discover more about specific sets of activity, we frequently find links that show us commonalities between these sets, and allow us to assess that the same actors are behind two formerly distinct groups.

Some of the factors we consider when assessing a group's location and potential sponsorship include, but are not limited to, the following:

- **Operations:** The scope or scale of the group's operations and their level of sophistication (e.g., adaptability, stealth, or access to advanced tools or exploits). What type of group would have the resources (personnel, funding, length of operations) to conduct this activity?
- **Tactics, Techniques, and Procedures (TTPs):** Does the group use tools and methodologies that are generic, publicly available, or widely known, or ones that are unique, novel, or not typically seen? Such TTPs may make a group more or less distinctive, and potentially act as a "fingerprint" allowing us to link together disparate incidents.
- **Operational Details:** Groups operate with varying levels of stealth and anonymity. At one end are actors who make no attempt to hide their tools or operations, and instead rely on victims' inability to respond effectively for their success. At the other end are actors who take great pains to appear innocuous and limit or delete evidence of their presence. However, even the most careful operators make mistakes that can expose key details. Clues such as language settings within malware, observed hours of operation, build paths within binaries, or the use of infrastructure or services in particular geographic locations may point to a particular locale. While such indicators could be used deliberately for "false flag" purposes, human error often introduces anomalies that would expose such an operation. When combined with other types of evidence, these indicators can help support attribution.
- **Motivation:** We identify likely motivations based on the individuals, organizations, or data the group targets, and the themes present in any communications (spear-phishing messages, attachment contents, web sites leveraged as part of an attack) with the targets.

SUSPECTED CHINA-BASED ACTIVITY AGAINST CORPORATE VICTIMS, LATE 2015 TO MID-2016:

Despite the decline, China-based threat groups continue to operate. Through late 2015 and 2016, we saw suspected China-based groups compromise corporations' networks in the U.S., Europe, and Japan, while also targeting government, military, and commercial entities in the countries surrounding China.

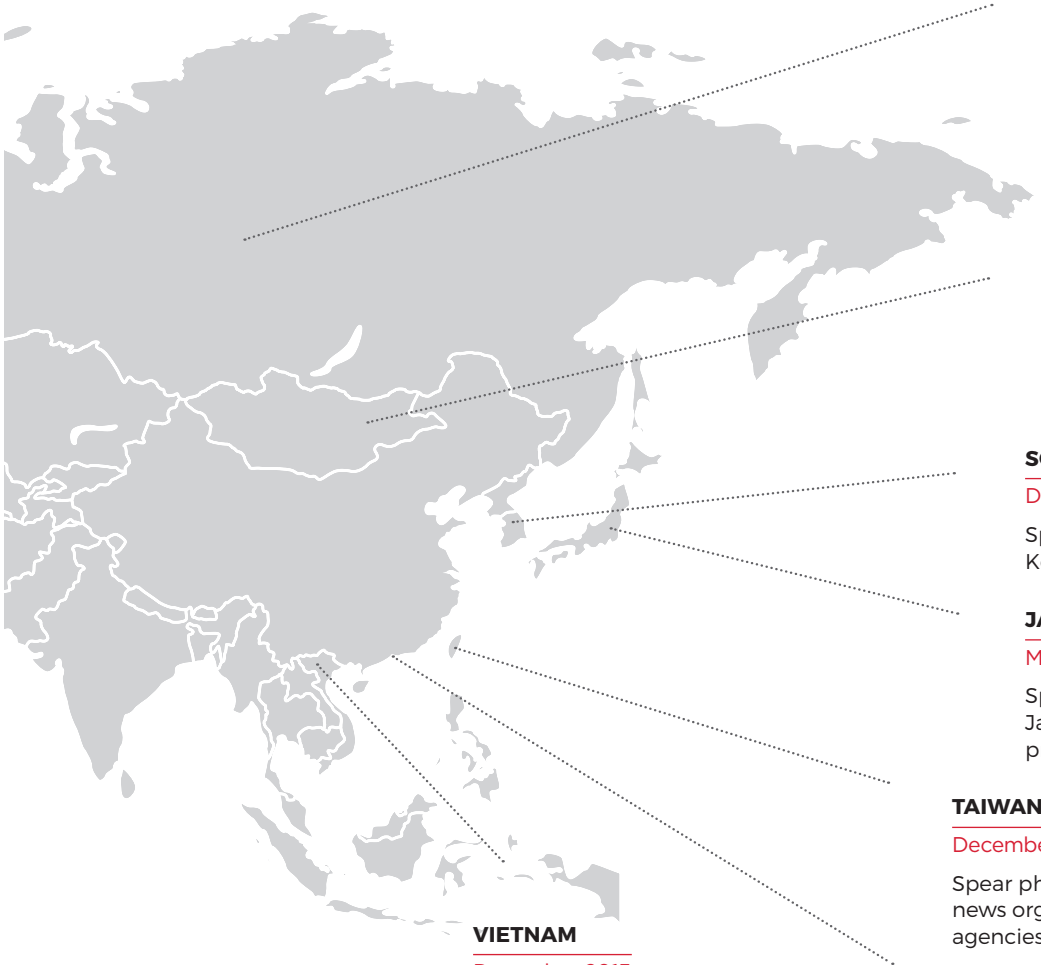
April – May 2016		Three groups compromised the networks of four firms headquartered in the U.S., Europe, and Asia that are involved in the manufacturing of semiconductors and chemical components used in the production of semiconductors. We did not observe data theft in any of these instances. However, in 2012, we saw one of these same groups compromise a semiconductor firm and target the workstation of a key individual active in research and development. Other China-based groups have also compromised and stolen data from semiconductor firms in the past, including as recently as July 2015.
April – May 2016		After compromising a network, the group moved laterally, harvested credentials, and deployed backdoors on systems at a U.S. high-tech corporation.
March – May 2016		In what appeared to be an attempt to obtain information related to U.S. military projects, a group deployed backdoors to a victim's web servers and harvested credentials at a U.S. government services company.
August 2015 – March 2016		After compromising the network of a U.S. high-tech corporation, the group began collecting data about navigational software in RAR files, likely in preparation for transferring the data from the environment.
March 2016		A group compromised a U.S. healthcare organization and deployed a backdoor providing continued access to the network.
December 2012-March 2016		In December 2012 a group breached the network of a U.S. software company. In 2014, they returned to the network, packaged data on navigational projects in likely preparation for removing it from the network. The same group returned again in early 2016 and viewed files related to the same project, but they did not transfer any data out of the network.
October 2015 – February 2016		In early 2016, a group prepared to transfer files out of the network of a European consulting company. The files were related to technology used in U.S. military projects.
January 2016		At a European logistics company a group collected user credentials during an intrusion into the network.
October – November 2015		After a group breached the network of a major media company, they stole user credentials, probably with the intent to expand their access within the network.
September – October 2015		At a U.S. aerospace company, a group deployed a backdoor, conducted network reconnaissance, and harvested user credentials, likely in preparation for continued activity. We did not observe the group transferring data from the network.

2015-2016 REGIONAL SPEAR-PHISHING ACTIVITY REFLECTS SECURITY CONCERNS

In addition to the confirmed network compromises described above, our research identified suspected China-based groups spear phishing governments and commercial organizations headquartered in countries surrounding China. Much of this activity appears to be traditional espionage, primarily motivated by political and security concerns amid ongoing diplomatic tensions in the region.

We have strong indications that China-based groups have been conducting espionage activity in the region for more than a decade as shown, for example, by our profile of a group likely backed by the Chinese government whom we refer to as APT30. The Chinese Government's use of cyber operations to conduct espionage in support of state security objectives parallels similar efforts by other nation states to pursue state secrets through network means. The targeting and data taken during traditional espionage activity typically allows us to distinguish it from corporate intellectual property theft. However, we frequently see compromises where a group targets or steals data that could equally serve military, security, and economic ends—such as navigational technology. This gray area between espionage that would support state economic ends and that, which would support state security, makes it difficult to definitively characterize espionage activity without visibility into the data's end use.

On the following map we identify several instances of 2015 and 2016 activity that indicate interest by China-based groups in regional political and security targets.



RUSSIA

Mid to Late 2015

Spear phishing against possible Russian defense organizations and a Russian engineering corporation that serves the energy sector.

MONGOLIA

Late 2015

Spear phishing against Mongolian government targets.

SOUTH KOREA

December 2015

Spear phishing against Korean IT service provider.

JAPAN

March 2016

Spear phishing against Japanese government and private sector.

TAIWAN

December 2015 & February 2016

Spear phishing against Taiwanese news organizations, government agencies, and commercial entities.

HONG KONG

February 2016

Spear phishing against Chinese dissidents in Hong Kong.

VIETNAM

December 2015

Spear phishing targeting Vietnamese government and commercial organizations.

THE MYTH OF THE MONOLITH:

SOME GROUPS REVAMP OPERATIONS WHILE OTHERS CARRY ON

We have strong indications that the 72 groups we have observed are based in China or otherwise support Chinese interests, although we question whether there is much consistency in the level of state direction or support that each of these groups may receive from the Chinese Government. The Chinese landscape, frequently characterized as monolithic and rigidly state-directed, is composed of a wide range of groups, including government and military actors, contractors, patriotic hackers, and even criminal elements. Occasionally, aligned interests between two types of groups may drive activity that blurs the lines between direct government sponsorship and independent action. For example, during territorial disputes, patriotic hackers may conduct targeting activity that is indistinguishable from that of government forces. As a result, it is often difficult to determine the extent to which activity is directed by the Chinese Government.

The variety of changes (or lack of change) observed in recent years across the groups we track demonstrates the range of state direction and support that they most likely receive. While this report discusses the likely impact of political, economic, and other forces on Chinese cyber activity as a whole, the extent to which specific groups altered their activity in response to certain factors, such as the Chinese Government's efforts to restructure its cyber forces, likely varies depending on how directly the groups are aligned with the Chinese Government.

Despite an overall decline in China-based threat activity, multiple groups actively conduct network intrusions, while others continue to compromise servers to use as infrastructure in preparation for future network intrusion operations. We have noted some changes in tactics among the groups that we track, but have not seen evidence of coordinated, widespread shifts in how these groups operate. Changes in operations are more likely to be driven by individual groups' specific circumstances, resources, and needs. For example:

- From mid-2014 through June 2016, a group did not make any changes to the tools and infrastructure that it used to compromise chemical companies in Germany, Japan, and the U.S.
- From 2009 until 2014, a group relied heavily on the same set of tools to compromise victims in multiple industries. Then in late 2014, a report exposing one of its most commonly used tools likely prompted the group to develop and use replacements, including those that incorporated anti-detection techniques. While the group replaced many of its tools, the actors still use some of those that had been exposed.
- A group that breached multiple victims in the U.S. through 2014 appears to have discontinued operations against organizations in the U.S., while continuing to compromise U.S.-based servers, presumably for use as infrastructure in carrying out other operations. Between 2015 and March 2016, the group has compromised organizations in in Taiwan, India, and Japan.

CONCLUSION

In 2013, when we released the APT1 report exposing a PLA cyber espionage operation, it seemed like a quixotic effort to impede a persistent, well-resourced military operation targeting global corporations. Three years later, we see a threat that is less voluminous but more focused, calculated, and still successful in compromising corporate networks. Rather than viewing the Xi-Obama agreement as a watershed moment, we conclude that the agreement was one point amongst dramatic changes that had been taking place for years. We attribute the changes we have observed among China-based groups to factors including President Xi's military and political initiatives, the widespread exposure of Chinese cyber operations, and mounting pressure from the U.S. Government.

Yet China is not the only actor in transition: we've observed multiple state-backed and other well-resourced groups develop and hone their operations against corporate and government networks. The landscape we confront today is far more complex and diverse, less dominated by Chinese activity, and increasingly populated by a range of other criminal and state actors.

To download this or other
FireEye iSight Intelligence reports,
visit: **www.fireeye.com/reports.html**

FireEye, Inc.
1440 McCarthy Blvd. Milpitas, CA 95035
408.321.6300 / 877.FIREEYE (347.3393) / info@FireEye.com

www.FireEye.com

FireEye