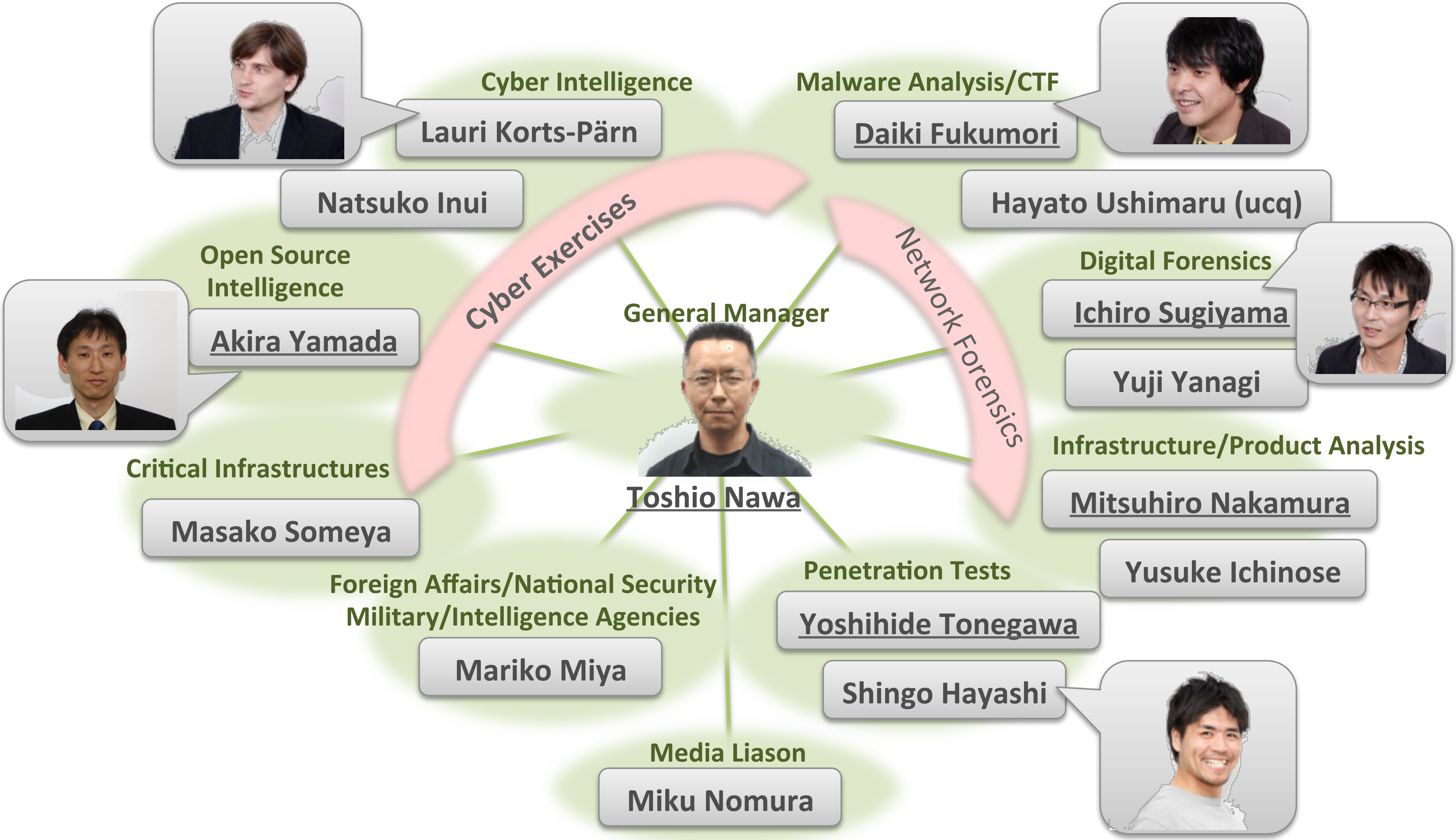
CyberDefense

Findings and Lessons Learned From Massive Cyber Attack Emergence Mechanisms in Japan

September 2013

Mariko MIYA
Cyber Defense Institute, Inc.

My Team - CDI-CIRT



General Manager

Toshio Nawa

Cyber Exercises

Network Forensics

Cyber Intelligence

Lauri Korts-Pärn

Natsuko Inui

Malware Analysis/CTF

Daiki Fukumori

Hayato Ushimaru (ucq)

Open Source Intelligence

Akira Yamada

Digital Forensics

Ichiro Sugiyama

Yuji Yanagi

Critical Infrastructures

Masako Someya

Infrastructure/Product Analysis

Mitsuhiro Nakamura

Yusuke Ichinose

Foreign Affairs/National Security
Military/Intelligence Agencies

Mariko Miya

Penetration Tests

Yoshihide Tonegawa

Shingo Hayashi

Media Liason

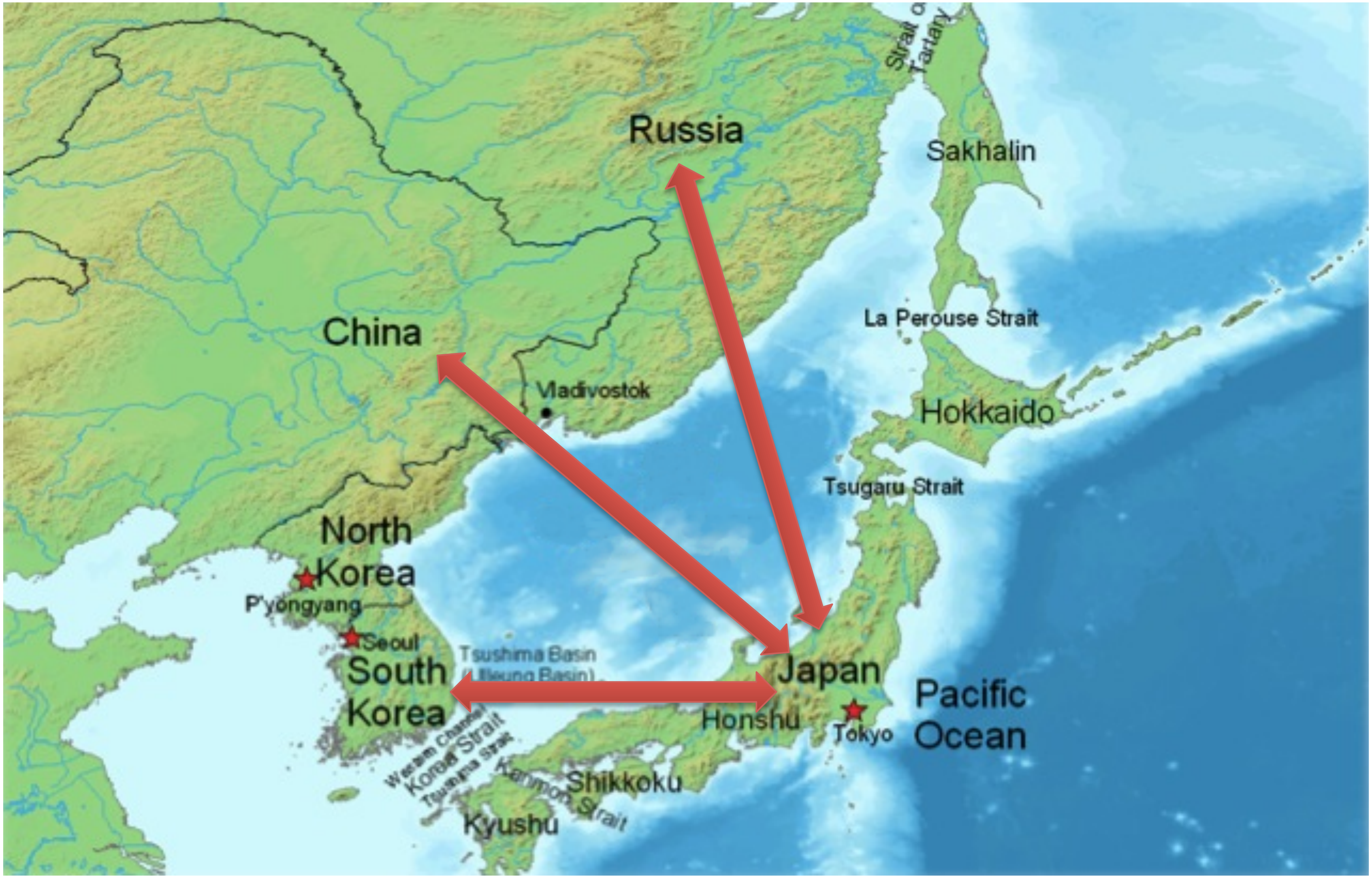
Miku Nomura

http://www.first.org/members/teams/cdi-cirt

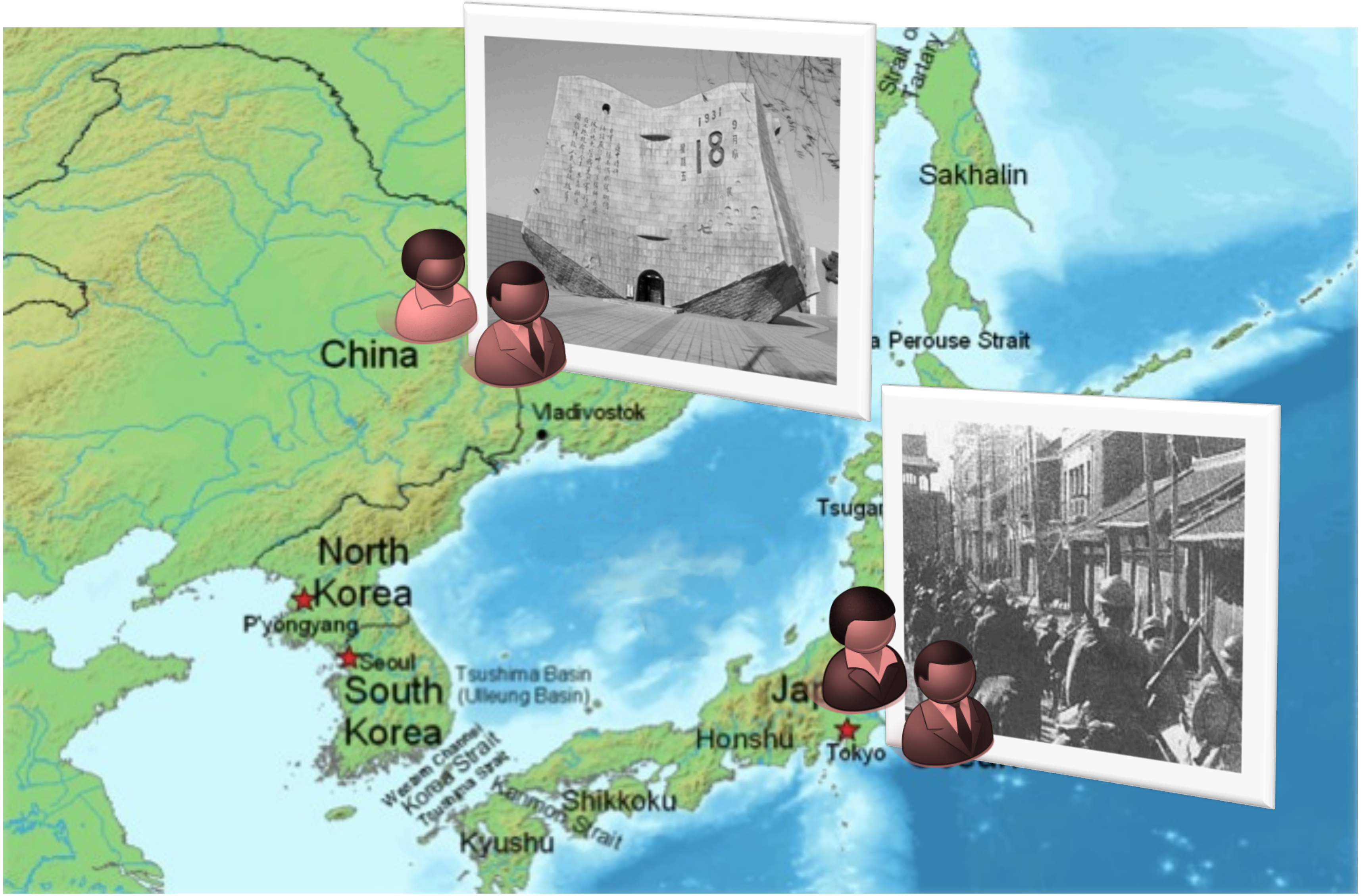
Agenda 1

FACTS – MASSIVE CYBER ATTACKS IN JAPAN

Geopolitical Issues Surrounding Japan

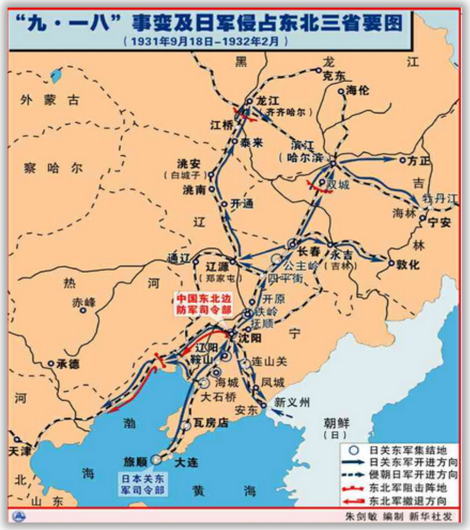


September 18 – Critical Day between China & Japan



“918 Incident” in China

- *What is the “918 Incident”?*
  - Otherwise known as: Mukden Incident, Shenyang Incident, Manchurian Incident (in Japan, it is mainly called the Manchurian Incident because it happened in an area of China called Manchuria)
  - **A military conflict /political incident that happened in northeastern China on September 18, 1931**
  - The disputing parties were the Northeast Army of China and Kwantung Army of Japan
  - After the outbreak of the 918 Incident, the Japanese Army became predominant and launched a full-scale invasion against Chinese territory
  - As result of the invasion, the Japanese Army seized three provinces in the Northeast region
  - **To the present day, September 18th is informally called China’s “National Shame Day”**



Map of the 918 Incident

Japanese troops entering Mukden

Events that happened September 2010 to 2013

Sep 2010

- The Chinese fishing boat collision incident off the Senkaku Islands between China and Japan
  - An incident between the Japanese Coast Guard and a Chinese fishing boat for operating near the Senkaku Islands

Sep 2011

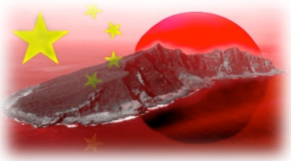
- "918 Incident" 80th Anniversary events in China
  - There were events to commemorate the 80th anniversary of the Liutiaohu Incident; one in particular was in Shenyang City, Liaoning Privince, co-hosted by 3 Northeastern Provinces

Sep 2012

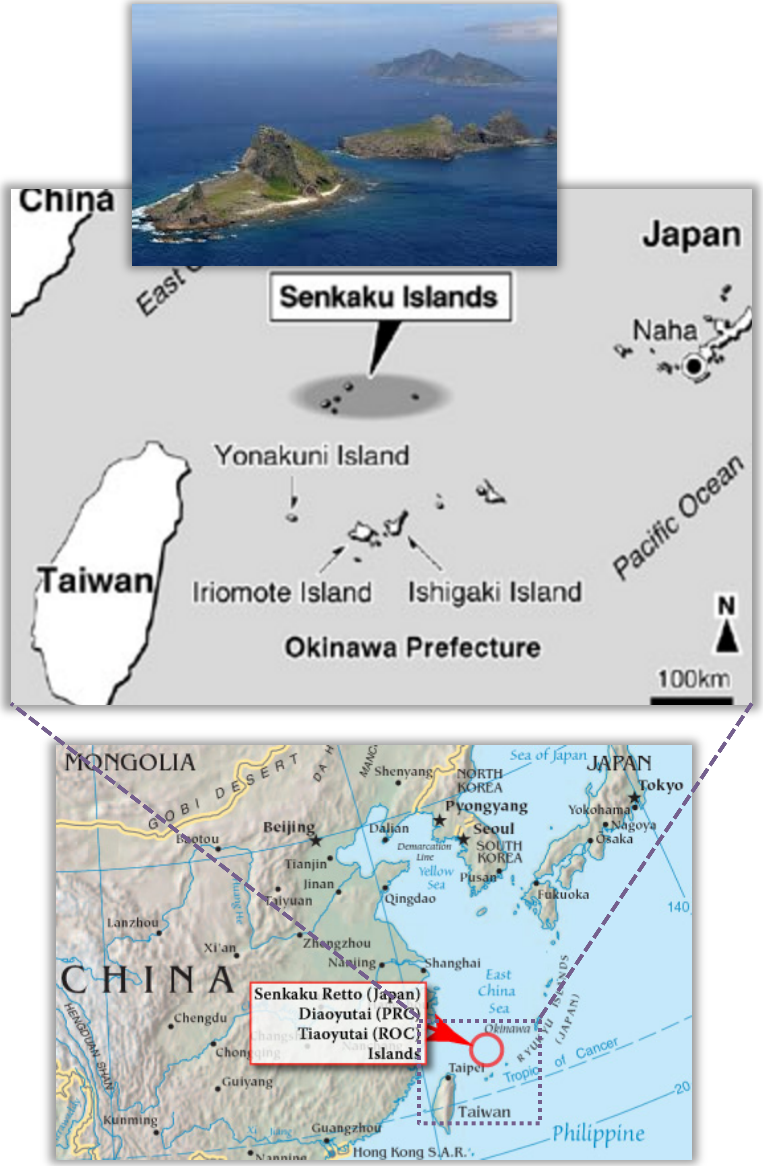
- Nationalization of the Senkaku Islands by Japan
  - 3 privately owned islands of the Senkaku Islands were bought for 2.05 billion Yen and nationalized by the Japanese government.

Sep 2013

- **Gap in historical perception** between China and Japan
  - China calls out to "set straight" historical perception of the Japanese, but this only narrows the gap between the two countries.



“918 Cyber Attacks” to Japan – Senkaku Islands



- *Names:* Senkaku Islands (Japan), Diaoyu Islands (China), Tiaoyutai Islands (Taiwan)
- *Location:* in the East China Sea between Japan, China, and Taiwan (shown in the map on the left)
- *Each country’s position on this issue:*
  - **China & Taiwan :** Claims sovereignty
  - **Japan :** “There is no territorial issue”
  - **US :** US Department of State states that it has no official position on who owns the island, but US government officials declare that Japan maintains effective administrative control on the islands
- *The cause of the 2012 anti-Japanese protests in China regarding this issue*
  - In **September 2012**, the Japanese government purchased the remaining 3 islands that they did not own to “nationalize” the disputed islands, which prompted a large scale Anti-Japanese protest in China.

“918 Cyber Attacks” - 2010

- September 7, 2010 **- “Chinese fishing boat collision incident off of the Senkaku Islands”** happened, leading to an extreme media circus

- **<u>Massive Cyber Attacks toward Japan around September 18th</u>** was excessive compared to past years

- *The Chinese fishing boat collision incident*
  - ➢ A Chinese fishing boat (Minjinyu 5179) was operating in the disputed waters off of the Senkaku Islands, and collided with a Japan Coast Guard patrol boat.
  - ➢ China repeatedly demanded to release the captain and crew members who were being detained, which resulted in a diplomatic dispute between China and Japan.
  - ➢ The captain and crew members were released without charge and returned to China on September 24.

"918 Cyber Attacks" – 2011 and 2012

2011

- September 18, 2011 was the 80th anniversary of the **Liutiaohu Incident**, and various events were held in China to commemorate this event.
- The Liutiaohu Incident – happened on September 18, 1931 in Northeastern China, which triggered the armed conflict between the Japanese Army and the Chinese Army otherwise known as the 918 (Manchurian) Incident.
- On September 18th at 9:18 am (Japan Time 10:18 am), an air raid alarm was rung for 3 minutes in Shenyang City, Liaoning Province, calling to the citizens to not forget the National Shame, strive for growth and development of China, and to always be ready for difficulties and dangers even in peacetime.
- China launched cyber attacks against several government agencies in Japan.

2012

- Anti-Japanese protests begin after the incident of Hong Kong activists landing on the Senkaku Islands on August 15, 2012.
- Especially after the purchase (nationalization) of the islands of Senkaku on September 11, the anti-Japanese protests in China escalated into the largest protest in history. Protesters became mobs and there were massive destructive behavior including robbery.
- From September 12 to September 19, there were large-scale cyber attacks from China to Japan, for the same reason as 2010.

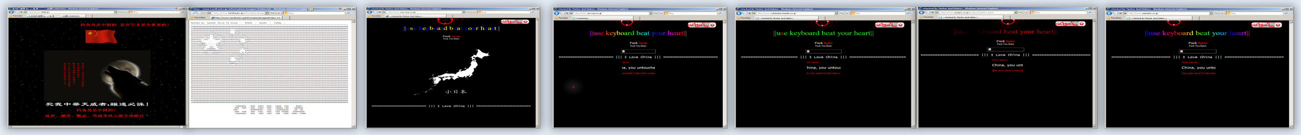
Flow of Events - 2012

Date	Events
September 10	• Posts on the Internet that seem to be excessively stirring anti-Japanese sentiment are being deleted • Accounts making statements leading to actual cyber attacks are deleted
September 11	• Cyber attack from China to the Philippines, attack tool is obtained
September 12	• Increase in the keyword “918” in Chinese microblogs
September 13	• Anti-Japanese protests, Chinese media criticizes Japan
September 14	• Honker Union of China announces attack, a joint statement is issued by PLA officials • Website defacement, DDoS attacks occur
September 15	• Eighth Army Corps announces attack, website defacement, DDoS attacks
September 16	• Website defacements increase, spreading information about successful attacks over internet
September 17	• Call-outs to attack on 9/18, spreading and sharing attack target lists online • Pictures from the 918 Incident shared in microblogs
September 18 (X-Day)	• Fueling anti-Japanese sentiment, active sharing of tools / tutorials for attack • Intensive website defacement, website intrusions, DDoS on Japanese government websites

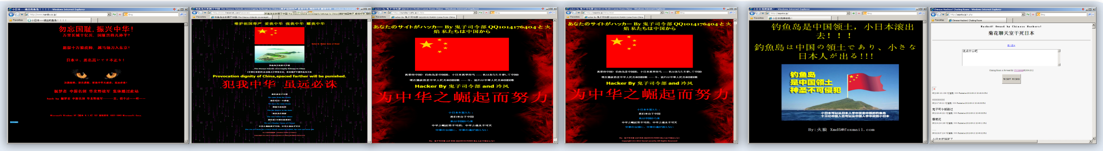
Defaced Websites (monitored by CDI-CIRT) - 2012

14 Sep

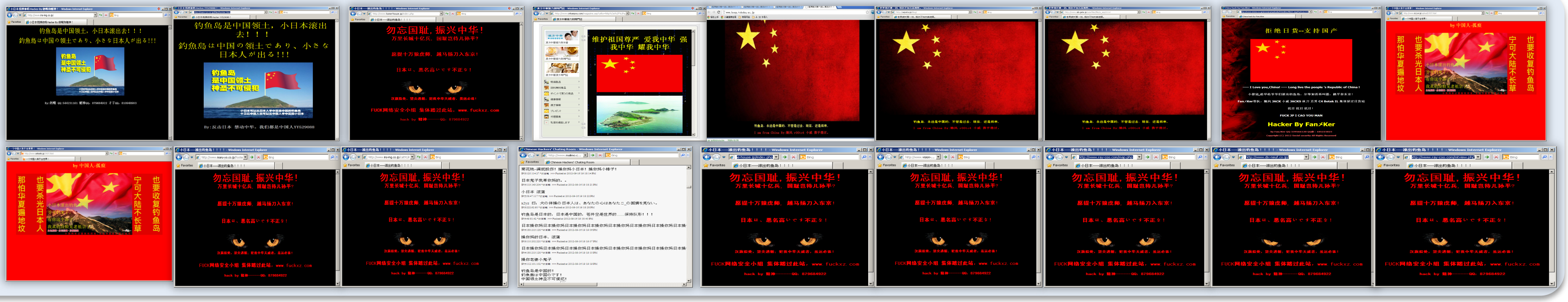
15 Sep



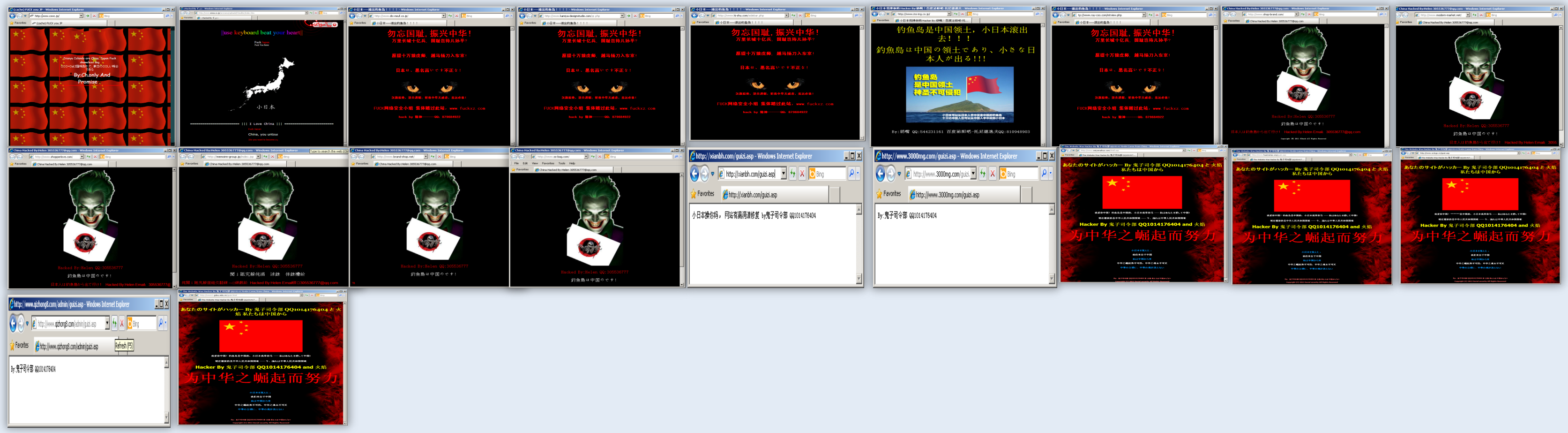
16 Sep


勿忘国耻，振兴中华！
犯我中华 虽远必诛
Hacker By 鬼子司令部 and 冷风
为中华之崛起而努力
钓鱼岛是中国领土，小日本滚出去！！！
釣魚島は中国の領土であり、小さな日本人が出る！！！
钓鱼岛是中国领土 神圣不可侵犯

17 Sep


钓鱼岛是中国领土，小日本滚出去！！！
釣魚島は中国の領土であり、小さな日本人が出る！！！
钓鱼岛是中国领土 神圣不可侵犯
勿忘国耻，振兴中华！
维护祖国尊严 爱我中华 耀我中华
拒绝日货—支持国产
Hacker By Fan Ker
by 中国人·孤瘦
那怕华夏遍地坟 也要杀光日本人
宁可大陆不长草 也要收复钓鱼岛

18 Sep

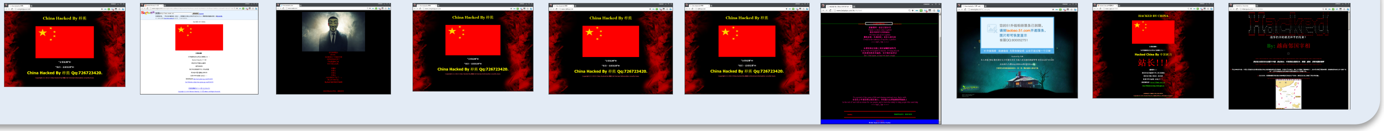

By:Only And Promise
[use keyboard beat your heart]
Fuck Japan
小日本
||| I Love China |||
勿忘国耻，振兴中华！
钓鱼岛是中国领土，小日本滚出去！！！
釣魚島は中国の領土であり、小さな日本人が出る！！！
钓鱼岛是中国领土 神圣不可侵犯
钓鱼岛是中国的！
http://xianbh.com/guizi.asp - Windows Internet Explorer
http://www.3000mg.com/guizi.asp - Windows Internet Explorer
http://www.qzhongli.com/admin/guizi.asp - Windows Internet Explorer
by:鬼子司令部 QQ1014176404
Hacker By 鬼子司令部 QQ1014176404 and 火焰
为中华之崛起而努力

Flow of Events –2013

Date	Events
September 10	• News that 8 vessels of the Chinese Security Bureau entered Japan's territorial waters is widely reported in China. • Movies and TV programs featuring Diaoyu Islands are being actively shared
September 11	• First anniversary since Japanese government's nationalization of Senkaku Islands
September 12	• NHK (Japan Broadcasting Corporation) reports about a Chinese hacker group BBS calling for attacks on 270 Japanese organizations
September 13	• Many texts and posts online expressing anti-Japanese sentiment in response to "National Shame Day"
September 14	• Chinese authority regulations (blocking results of particular word searches)
September 15	• An article about the Imperial Japanese Army bombing China during WWII is published, and is frequently discussed online
September 16	• Core members of Honker Union of China share information on smartphones • Massive number of tools shared in chat rooms
September 17	• Videos and logos of hacker communities and 918 spread in chats, micro blogs • 30 websites of Japanese organizations defaced • Defaced websites shown off and shared in micro blogs "Brothers act now!"
September 18 (X-Day)	• Count downs to attack launch time @ 20:00 (China time) • However, no cyber attacks on "major institutions" confirmed

Defaced Websites (monitored by CDI-CIRT) - 2013

before 14 Sep


China Hacked By

China Hacked By

China Hacked By

China Hacked By

15 & 16 Sep

You got H4ck3d By - B4tsc4r - I am from China!

YOU GOT H4CK3D BY - B4TSC4R - I AM FROM CHINA!

YOU GOT H4CK3D BY - B4TSC4R - I AM FROM CHINA!

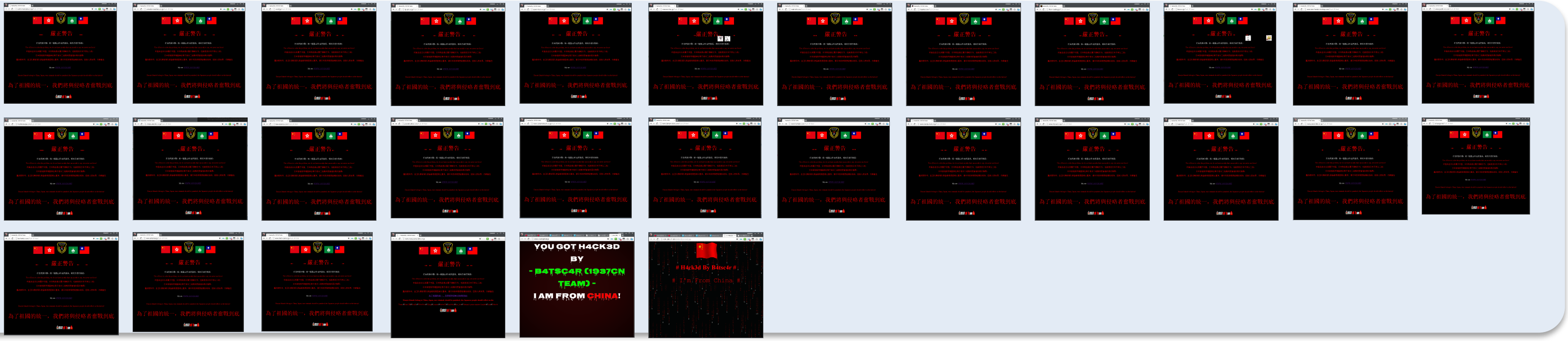
YOU GOT H4CK3D BY - B4TSC4R - I AM FROM CHINA!

YOU GOT H4CK3D BY - B4TSC4R - I AM FROM CHINA!

YOU GOT H4CK3D BY - B4TSC4R - I AM FROM CHINA!

HACKED BY CHINA

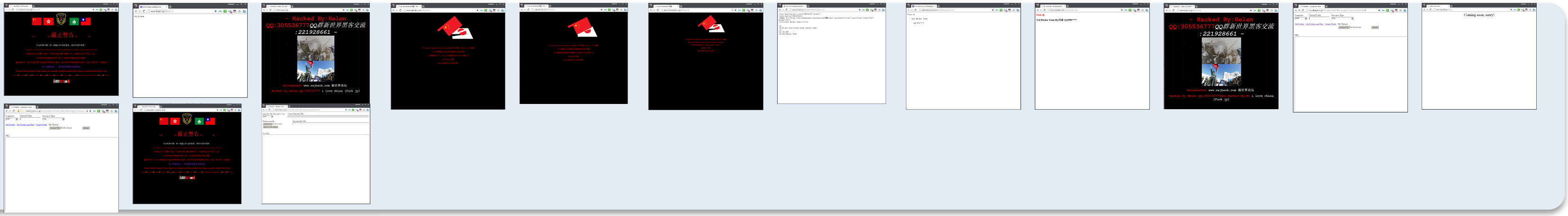
17 Sep


YOU GOT H4CK3D BY - B4TSC4R (1937CN TEAM) - I AM FROM CHINA!

H4ck3d By B4tsc4r

I'm From China

18 Sep


Hacked By:Ba1en

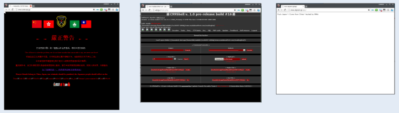
QQ:305534777 :221928661

Hacked By:Ba1en

QQ:305534777 :221928661

Coming soon, sorry!

19 Sep



Agenda 2

FINDINGS & ANALYSIS

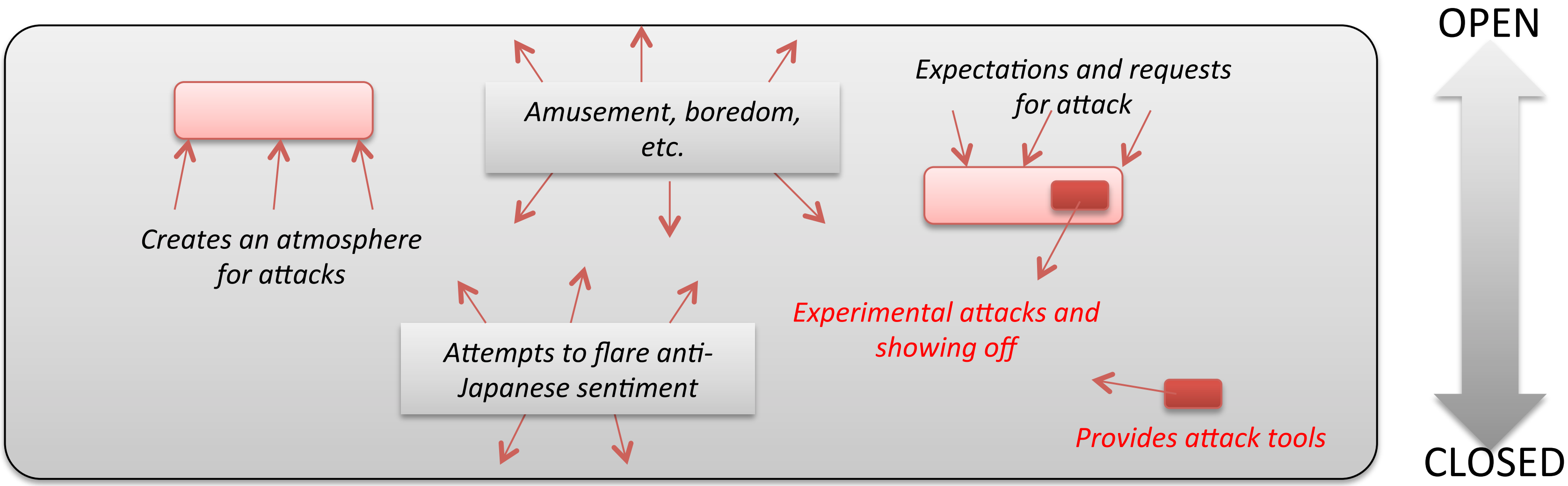
Findings From Monitoring & Analysis

- *[Finding] There are various types of "persons involved in cyber attacks toward Japan"*
  - [Analysis] Major categories are the following:

⬜ Shows strong willingness to attack, and also emphasizes reasons for attack or anti-Japanese sentiment, but relies on other for attack because they have no skills themselves. These types of Internet users are greatly affected by the media and online information. (MAJORITY)

▭ Feels that attacks are necessary, and has the knowledge and techniques to attack, and knows the target's systems well enough to be cautious at all times. (MINORITY)

■ Has no noticeable motivation to attack, yet is particular about the significance and purpose of attack, and defaces websites etc. with trial and error. They usually do not release information in open places on the Internet. (VERY RARE)


OPEN
Expectations and requests for attack
Amusement, boredom, etc.
Creates an atmosphere for attacks
Experimental attacks and showing off
Attempts to flare anti-Japanese sentiment
Provides attack tools
CLOSED

Findings From Monitoring & Analysis

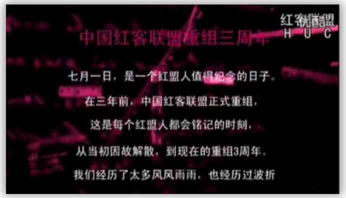
- [Finding] To share and distribute information, pictures and video data were actively shared in addition to using the traditional BBS, micro blogs, SNS
  - [Analysis] Visual images give a person far more information at one time compared to text data, therefore the impact to the reader is very large.

- [Finding] Attacker communities who actually have the ability to attack user closed SNS.
  - [Analysis] It is difficult to grasp activity trends using automatic or mechanical monitoring, so responders need to earn personal trust from the attacker communities when monitoring their activities.

- [Finding] Malicious codes being inserted into defaced websites is becoming more common.
  - [Analysis] This is not just to get a message across, but an attempt to spread malware to Chinese Internet users visiting the defaced website.

- [Finding] Sharing attack tools are extremely common.
  - [Analysis] By attack tools spreading via SNS, the impact of simultaneous attack by Internet users without knowledge or skills about cyber attacks has become larger.

BBS



中国红客联盟重组三周年

七月一日，是一个红盟人值得纪念的日子。

在三年前，中国红客联盟正式重组，

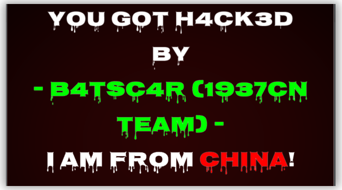
这是每个红盟人都会铭记的时刻，

从当初因故解散，到现在的重组3周年。

我们经历了太多风风雨雨，也经历过波折

Movie

Portal Site

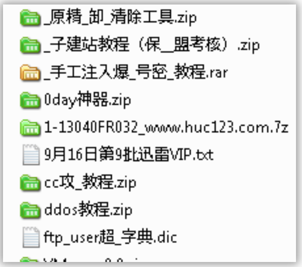

YOU GOT H4CK3D

BY

- B4TSC4R (1937CN TEAM) -

I AM FROM CHINA!

Defaced Site


_原精_卸_清除工具.zip

_子建站教程（保_盟考核）.zip

_手工注入爆_号密_教程.rar

0day神器.zip

1-13040FR032_www.huc123.com.7z

9月16日第9批迅雷VIP.txt

cc攻_教程.zip

ddos教程.zip

ftp_user超_字典.dic

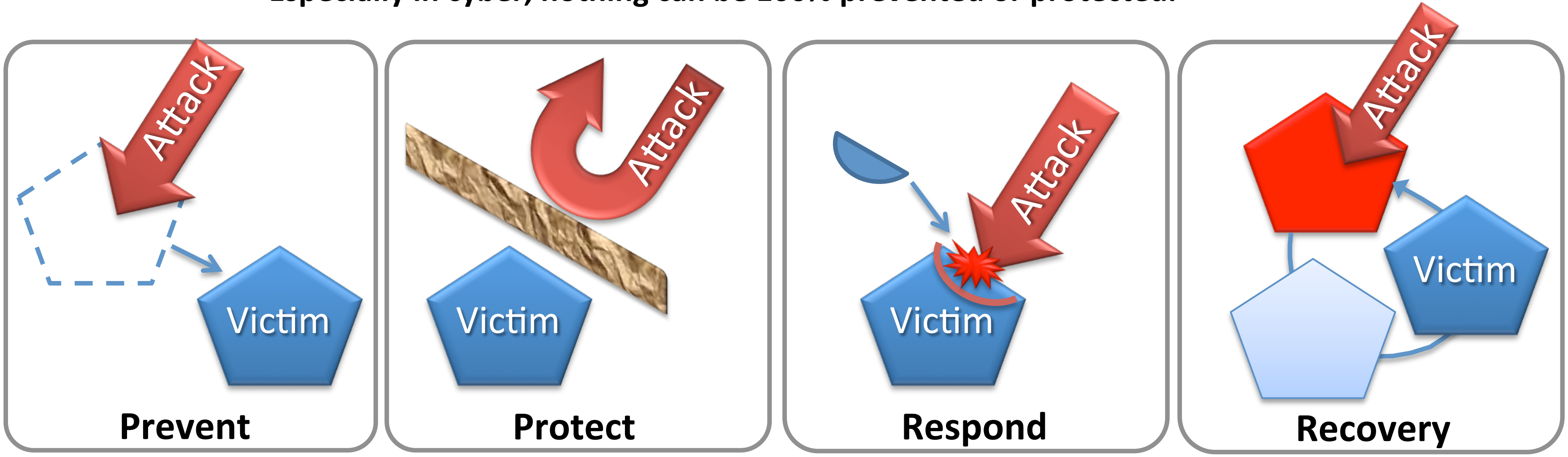
Attack tools

Agenda 3

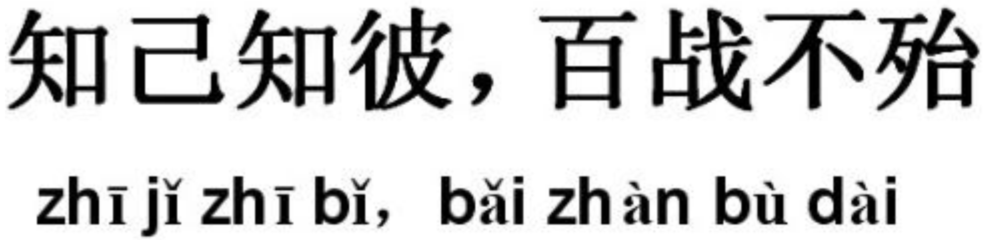
LESSONS LEARNED

The Need to Improve Capabilities - **Concept**

- *The need to conduct cyber exercises*
  - Western countries are more focused on building capabilities, whereas Japan is focused on building framework and strengthening the system
    - Japan is focused on strengthening and building a strong system, because they are not under the assumption of a crisis, emergencies are to be “avoided” or “prevented”
      - Japan focuses on the “Protect” rather than the “Respond,” so they are not ready to respond when something happens (i.e. the Fukushima nuclear plant after 3.11 Great East Japan Earthquake)
    - Multi-national multi-cultural western countries are focused on responding when in an emergency situation
      - The western countries conduct very realistic exercises to become aware and ready to respond smoothly when something happens
    - **Especially in cyber, nothing can be 100% prevented or protected.**



The Need to Improve Capabilities – **Cyber Intelligence**



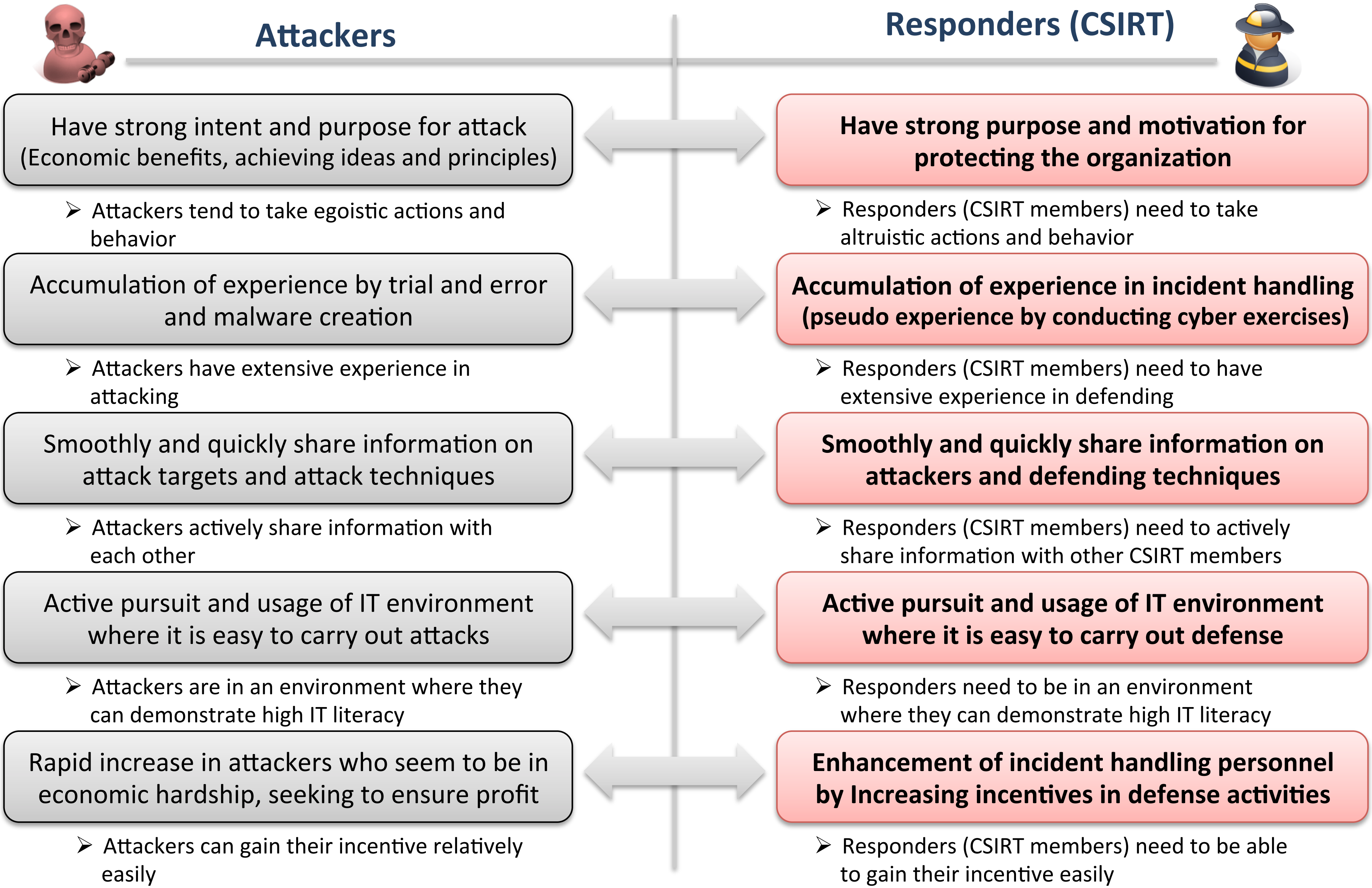
知己知彼，百战不殆

zhī jĭ zhī bĭ，băi zhàn bù dài

“Know your enemy and know yourself and you can fight a hundred battles without disaster.”

- Sun Tzu

The Need to Improve Capabilities - **Embodiment**



Attackers	Responders (CSIRT)
Have strong intent and purpose for attack (Economic benefits, achieving ideas and principles)	**Have strong purpose and motivation for protecting the organization**
➢ Attackers tend to take egoistic actions and behavior	➢ Responders (CSIRT members) need to take altruistic actions and behavior
Accumulation of experience by trial and error and malware creation	**Accumulation of experience in incident handling (pseudo experience by conducting cyber exercises)**
➢ Attackers have extensive experience in attacking	➢ Responders (CSIRT members) need to have extensive experience in defending
Smoothly and quickly share information on attack targets and attack techniques	**Smoothly and quickly share information on attackers and defending techniques**
➢ Attackers actively share information with each other	➢ Responders (CSIRT members) need to actively share information with other CSIRT members
Active pursuit and usage of IT environment where it is easy to carry out attacks	**Active pursuit and usage of IT environment where it is easy to carry out defense**
➢ Attackers are in an environment where they can demonstrate high IT literacy	➢ Responders need to be in an environment where they can demonstrate high IT literacy
Rapid increase in attackers who seem to be in economic hardship, seeking to ensure profit	**Enhancement of incident handling personnel by Increasing incentives in defense activities**
➢ Attackers can gain their incentive relatively easily	➢ Responders (CSIRT members) need to be able to gain their incentive easily

Contact Information

Mariko MIYA

Cyber Defense Institute, Inc.
Data Analysis Department
(Foreign Affairs / National Security)

Email: miya@cyberdefense.jp
Tel: 03-3242-8700

Office: www.cyberdefense.jp/en/
Response Team: www.cirt.jp