

Technology and Security: adapting to changing cyber security threats in North East Asia

French Institute of International Relations
Webinar

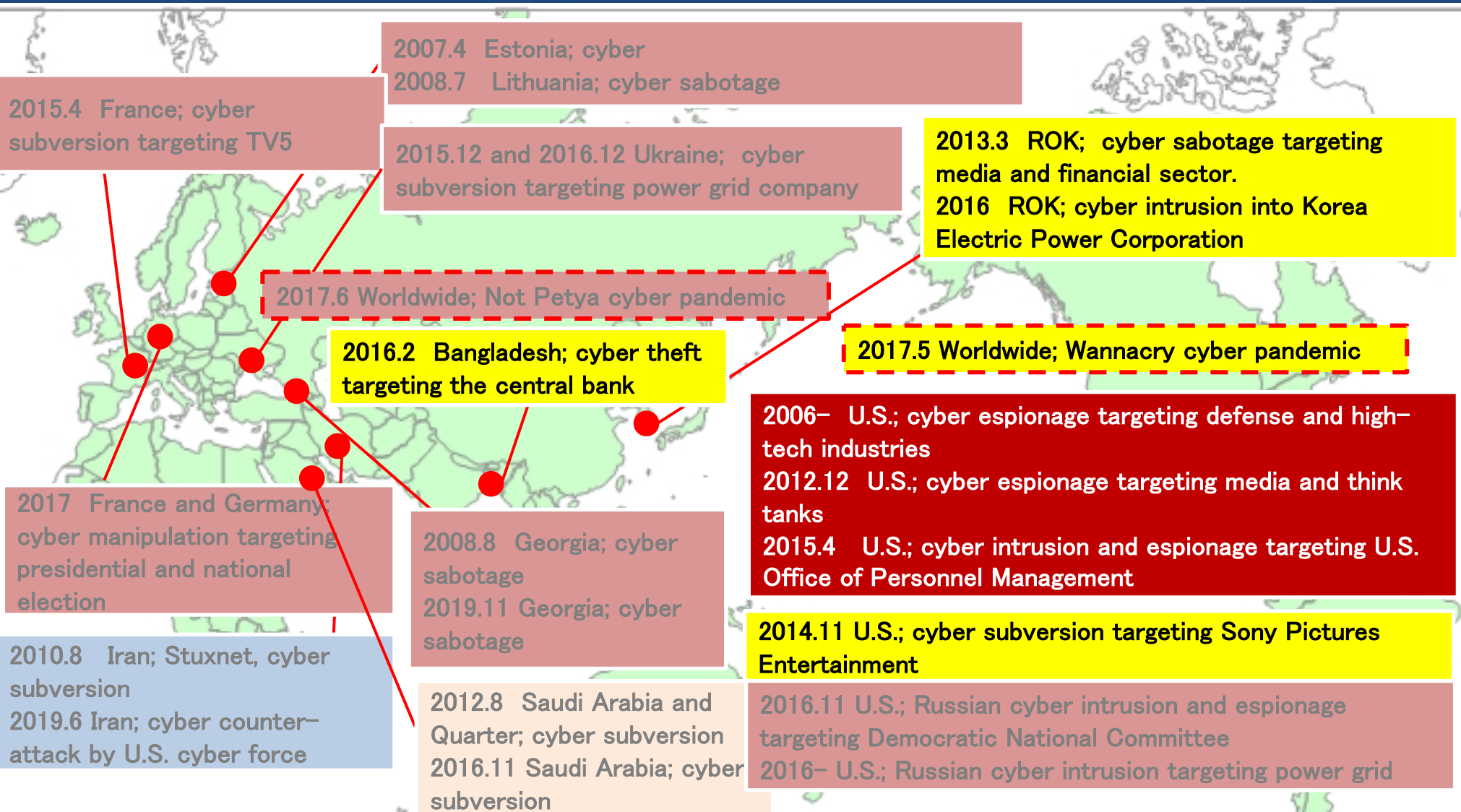
November 26, 2020

Jun OSAWA
Senior Research Fellow
Nakasone Peace Institute (NPI)/IIPS
Tokyo, Japan

Technology and Security: adapting to changing cyber security threats in North East Asia

- 1. Recognizing the Threat: What Kind of Cyber Attack does National Security Focus on?**
 - **State-sponsored cyber attacks on the rise**
 - **New serious challenge: cyber propaganda/manipulation of our democratic process (information warfare)**
- 2. Recognizing the emerging cyber threats in North East Asia : cyber espionage, cyber ransomware, and cyber manipulation (information warfare).**
 - **Cyber Espionage and Made in China 2025**
 - **DPRK cyber-attacks on financial institutions**
 - **Cyber Propaganda/Manipulation (Information Warfare)**
- 3. Contest for supremacy in digital arena**
- 4. How to Deter State-sponsored Cyber Attacks?**
 - **Comprehensive Cyber Deterrence and Countering against State-sponsored Cyber Attacks**
 - **Way of Future International Cooperation**

State-Sponsored Cyber Attacks on the Rise



2006– U.S., Europe, Japan, ASEAN, India; and etc. ; Chinese cyber espionage targeting governmental secret information, business secrets and intellectual properties

Recognizing the Threat: What Kind of Cyber Attack does National Security Focus on?

State-sponsored Cyber Attacks

- Since around 2007, state-sponsored cyber attacks becomes not only a real threat to national security but also a threat to economic activities of private sector of our countries.
- Risks of state-sponsored cyber-attacks with the intent to steal classified information, disrupt critical infrastructure and obstruct military systems, are becoming more serious.

Cyber Espionage/Spying

- State-sponsored APT groups intend to make cyber espionage of stealing secret information or theft of intellectual properties becomes serious threat to national security.

Cyber attacks designed to paralyze the control systems

- There is a high incidence of country-level cyber attacks aimed at critical infrastructure in the last decade.

Cyber Propaganda/Manipulation

- New Phenomena of undermining or manipulating public opinion in democratic countries becomes serious. Attacker uses propaganda in cyber media, fake news spreaded by proxy actor or betraying secrets.

- Overviewing cyber-attacks trend in the last decade reveals that cyber-attacks frequently follow incidents of international discord or conflict. Risks of state-sponsored cyber-attacks with the intent to steal classified information, disrupt critical infrastructure and obstruct military systems, are becoming more serious.


- In addition to targeted attacks with the objective of stealing classified information, signs of attacks designed to paralyze the control systems of critical infrastructure have begun to appear in recent years.


- There are symptoms of new serious challenge that threaten our democratic process. New Phenomena of undermining or manipulating public opinion in democratic countries becomes serious. Attacker uses propaganda in cyber media, fake news or betraying secrets.

Serious Cyber Incidents in and from East Asia (2007-2020)


- 2007.4 Estonia; cyber sabotage targeting government, media, financial sector.
- 2009.7 ROK and U.S.; cyber sabotage targeting government.
- 2009.12 Google, cyber intrusion on its core system. ⇒ Google retreated from business in China.
- 2010.8 Iran; Stuxnet, cyber subversion targeting Iranian uranium-enrichment plant.
- 2011.9 Japan; cyber espionage targeting defense industry, including MHI and IHI.
- 2013.3 ROK; cyber sabotage targeting media and financial sector.
- 2014.11 U.S.; cyber subversion targeting Sony Pictures Entertainment. U.S. government identified the attacking group and blamed and sanctioned North Korea (first attributed state-sponsored attack).
- 2015.4 U.S.; cyber intrusion and espionage targeting U.S. Office of Personnel Management, resulted in the theft of sensitive information of 21.5 million individuals.
- 2015.5 Japan; cyber espionage targeting Pension Service, 1.25 million records breach.
- 2015.12 Ukraine; cyber subversion targeting power grid company. (first state-sponsored attack on CI)
- 2016.2 Bangladesh; cyber theft targeting the central bank, stolen \$81 million
- 2016.11 Saudi Arabia; cyber subversion targeting government and private sector. (Shamoon2.0)
- 2016.11 U.S.; Russian cyber intrusion and espionage targeting Democratic National Committee.
- 2016.12 Ukraine; cyber subversion targeting power grid company in Kiev.
- 2017.5 Europe; Wannacry cyber pandemic spread over the world from Europe.
- 2017.6 Ukraine: Not Petya cyber pandemic spread over the world from Ukraine.
- 2018.2 ROK; cyber sabotage targeting winter Olympic Game committee and its operation system.
- 2018.11 Taiwan; cyber manipulation (information warfare) in local election.
- 2019.6 Iran; cyber counter-attack by U.S. cyber force, targeting Islamic Revolutionary Guard Corps network
- 2019.11 Georgia; cyber sabotage targeting government sector.
- 2020.3 Japan; cyber reconnaissance targeting Olympic Game committee and sponsors.


Recognizing the Emerging Cyber Threats in North East Asia

 Cyber Espionage : steal confidential information, secrets or intellectual property, by using methods of advanced persistent threat (spear phishing, watering hole attack, etc.) or indiscriminate attacks.

 Cyber Theft and Ransomware: targeted attacks, vulnerability exploits, etc., to penetrate the networks of certain government agencies, banks, companies, and individuals to make unauthorized money transfers or to encrypt data on a PC and demand a ransom for decryption

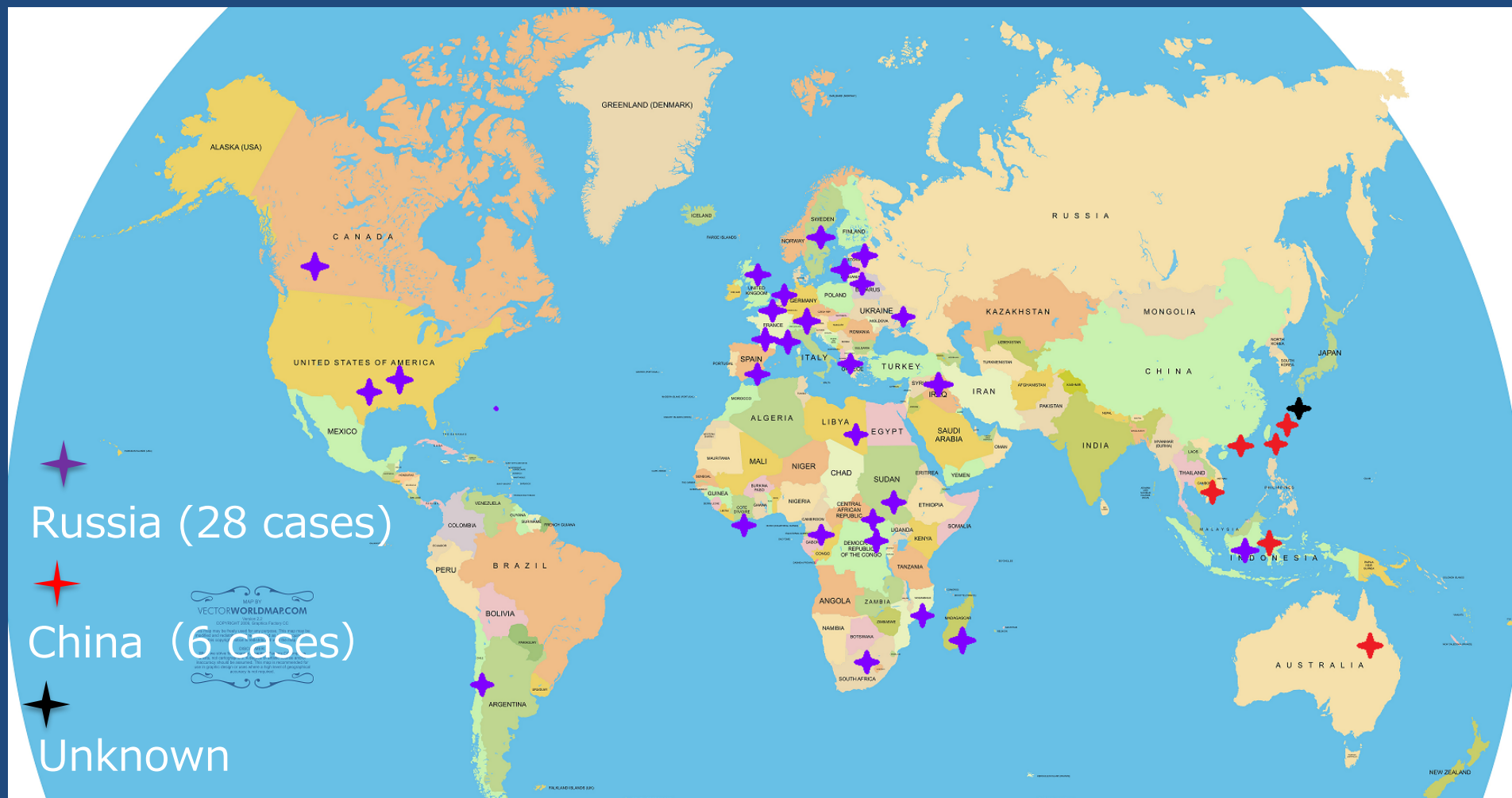
 Cyber Sabotage: paralyze servers or network service temporarily with overwhelming volume of data traffic, by using the method of distributed denial of service attacks.

 Cyber Subversion : disrupt or destroy function of computer network, including critical infrastructure , by means of deleting or manipulating digital data after intrusion of network by using methods of APT, indiscriminate attacks or Zero-Day vulnerabilities

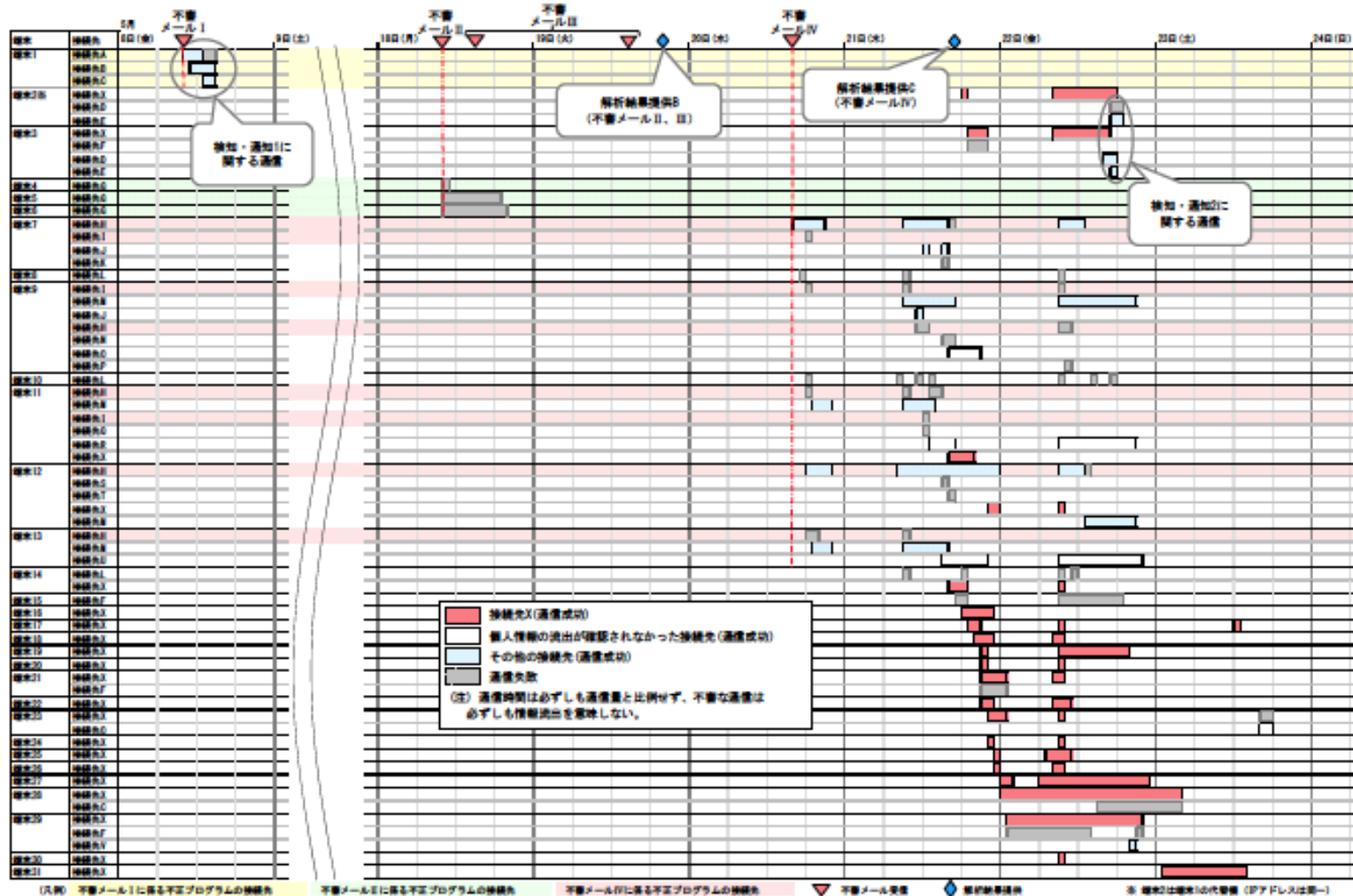
 Cyber Propaganda/Manipulation : undermine or manipulate public opinion in western allies by means of propaganda in cyber media or fake news spreaded by proxy actor to cover or hide real purpose.

 Military Cyber Attack: disrupt or destroy adversary's military cyber-based C4ISR assets or critical infrastructure along with military operation.

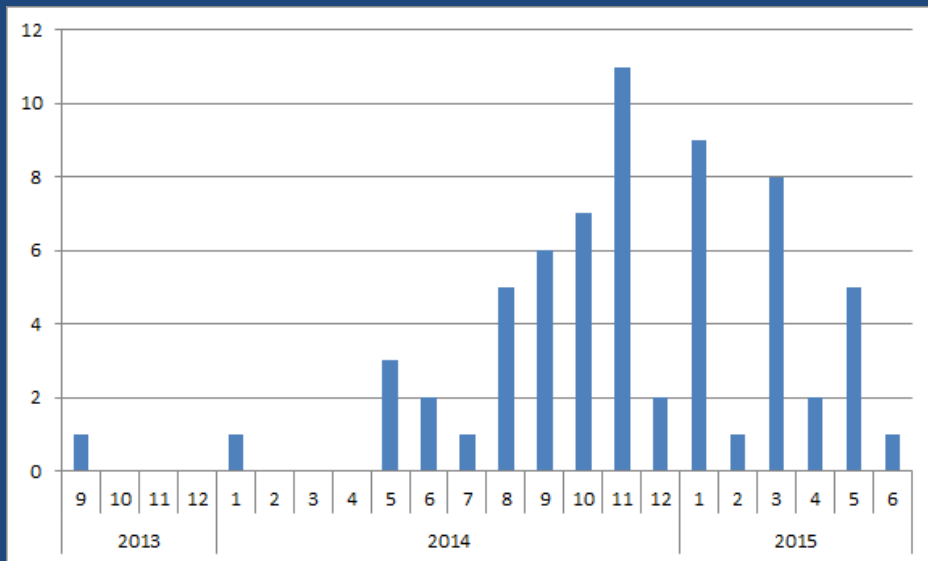
Cyber Propaganda/Manipulation (Information Warfare)



Japan Pension Service data breach (2015.5)



Japan Pension Service data breach: digital forensics

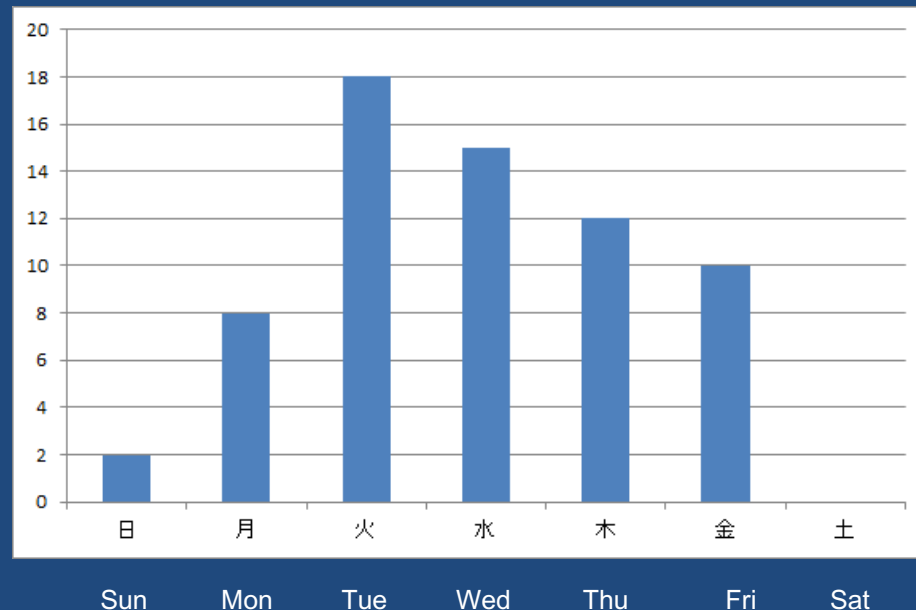


Malware “Emdivi” was compiled since summer 2014.

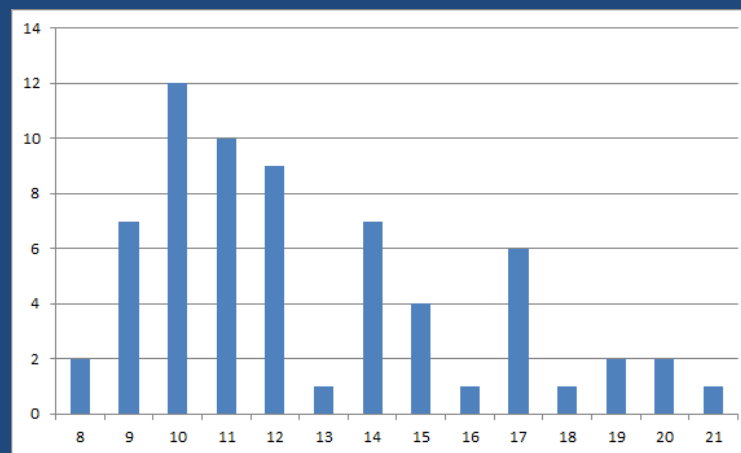
Programmers might get a Chinese New Year Holiday in Feb.

Programmers who complied “Emdivi” worked nine-to-five in Beijing Standard Time.

Source: Macnica Networks



Programmers who complied “Emdivi” worked on weekdays.



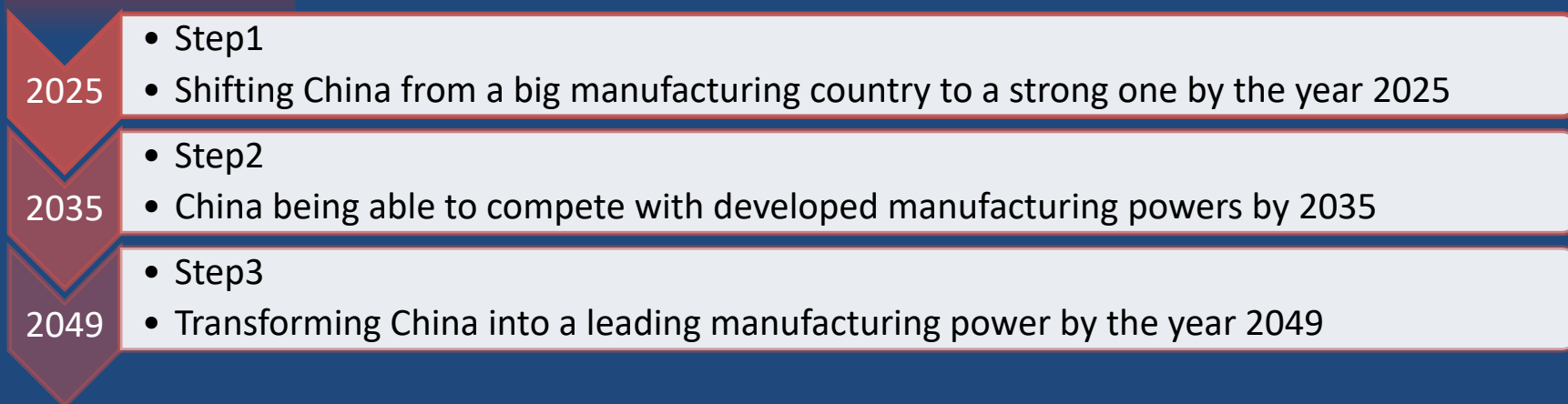
APT Group and Cyber Espionage Operation

Name of APT Group	Targets
APT1	English-speaking Countries : Government, Information Tech , Financial, Energy , etc.
APT4	Asia-Pacific Countries (Japan and South Korea): Aerospace and Defense Industry
APT5	South-east Asian Countries, now World-wide Telecom, Information Tech, High-Tech and Defense Industry
APT9 (Nightshade Panda)	US, Japan, Taiwan, Singapore, India, South Korea and Thailand: Aerospace, Agriculture, Construction, Energy, Medical, Transportation
APT10 (Cloud Hopper)	World-wide (2016- esp. Japan) Government, Think Tank, Media, Aerospace, Defense Industry, Medical and Healthcare
Cloudy Omega/ Blue Termite	Japan: Government, Academia, Financial, Energy, Chemical, Heavy Industry, Media, ITC etc.
APT12 (Numbered Panda)	Asia-Pacific Countries (-2011), Taiwan and Japan (2011-): Defense Industry (Satellite, Encryption and Aerospace)
APT16	Taiwan and Japan: Government, Media, Financial and High-Tech
APT17 (Hidden Lynx)	World-wide (2016- esp. Japan) : Government, Information Tech, Aviation and Law Firm
Dragon OK	Japan : Academia (Science and Technology)
Tick	Japan : High Tech, Chemical, Heavy Industry (Shipbuilder) and Media
Winnti	Japan : High Tech, Chemical, E-Commerce, Financial, Electronics, Tele-com and Gaming Industry
Black Tech (PLEAD)	Taiwan and Japan : Private Sector
LODEINFO	Japan: Media, Think Tanks

Made in China 2025 and Ten Key Sectors



On May 2015, China's State Council its first 10-years national plan for transforming China's manufacturing, entitled "Made in China 2025".



Ten Key Sectors





DPRK cyber-attacks on financial institutions

Suspected DPRK cyber-attacks on financial institutions

Date	Location	Damage
Dec 2015	Guatemala	16 mil USD
Dec 2015	Vietnam	1.1 mil Euro
Feb 2016	Bangladesh	951 mil USD
May 2016	South Africa/ Japan	18 mil USD
Jul 2016	India	166 mil USD
Jul 2016	Nigeria	100 mil USD
Oct 2016	Tunisia	60 mil USD
Oct 2017	Taiwan	60 mil USD
Jan 2018	Mexico	110 mil USD
Jan 2018	Costa Rica	19 mil USD
Feb 2018	India	17 mil USD
Mar 2018	Malaysia	390 mil USD
May 2018	Chili	10 mil USD
Jun 2018	Liberia	32 mil USD
Aug 2018	India	12 mil USD
Feb 2019	Malta	14.5 mil USD
Feb 2019	Spain	10.8 mil USD
Mar 2019	Gambia	12.2 mil USD
Mar 2019	Nigeria	9.3 mil USD
Mar 2019	Kuwait	49 mil USD





DPRK cyber-attacks on financial institutions

Suspected DPRK cyber-attacks on crypt currency		
Date	Location	Damage
Feb 2017	ROK (Bithumb)	7M USD
Apr 2017	ROK (Youbit)	4.8MUSD(3618Bitcoin)
May 2017	(Wannacry)	144,000USD(52Bitcoin)
Jul 2017	ROK(Bithumb)	7MUSD(Bitcoin/Ethereum)
Summer 2017	ROK	25,000USD(70Monero)
Sep 2017	ROK (Coinis)	2.19MUSD(Bitcoin)
Dec 2017	ROK (Youbit)	Theft of 17 percent of Youbit assets
Dec 2017	Slovenia (NiceHash)	70M USD(Bitcoin)
Jun 2018	ROK (Bithumb)	3.1M USD
Aug 2018	India	13M USD
Oct 2018	Bangladesh	2.6M USD
Mar 2019	China, Hong Kong, Singapore and Thailand	9M USD
Mar 2019	ROK (Bithub)	20M USD (in total)

Source: UN Security Council, "Report of the Panel of Experts established pursuant to resolution 1874 (2009) ", 30 August 2019.

Contest for Supremacy in Digital Arena

Supremacy in Digital Arena

Economic
Predominance

Tech Predominance

R&D
+
Tech Transfer by Cyber
Espionage

Digital
Dominance
(Digital
SilkRoad)

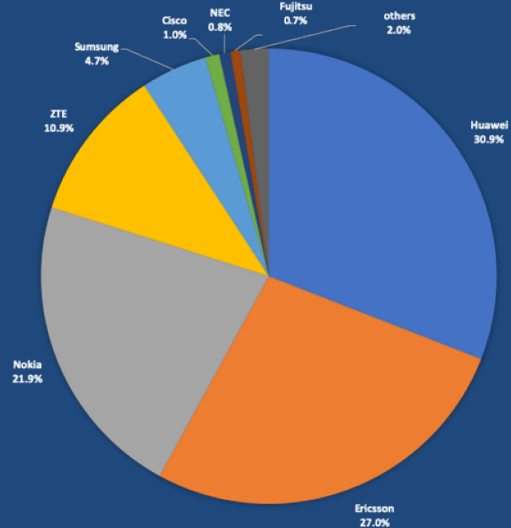
Software
Dominance
IoT Platform
Predominance
(EC, Electronic
Payment, Digital
Surveillance, SNS,
etc.)

Hardware Dominance
Information and
Communication Infrastructure
Predominance
(Submarine Cables and 5G)

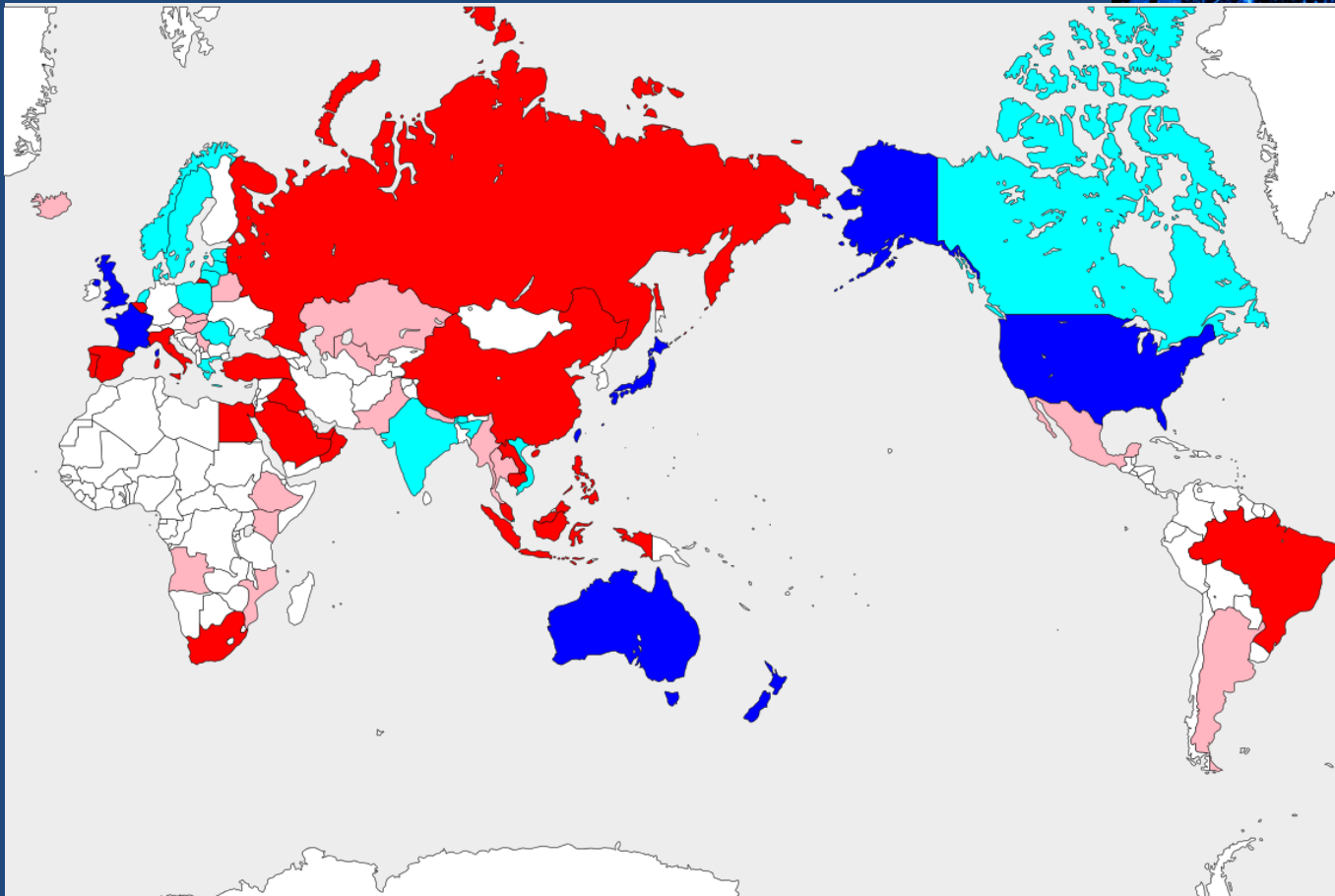
Digital SilkRoad: China-led Submarine Cable AAE-1



MARKET SHARE OF MOBILE COMMUNICATION BASE STATION (2018)



5G Clean Path VS Digital Silk Road



Source: various open information as of September 2020

How to Deter State-sponsored Cyber Attacks?

- - In order to stop potential state adversaries conducting cyber attacks on our national interests, like minded countries have to employ new strategy that is based on comprehensive cyber deterrence, as U.S. DoD 2015 Cyber Strategy describes.
- - It seems to me that U.S. government seeks to establish the cyber deterrence strategy through a trial and error process in these years. E.g. sanction North Korea in 2014, prosecute 5 PLA officers in 2014, Obama's diplomatic pressure on Chinese president Xi in September 2015 not to engage in economic cyber espionage, NATO's declaration of cyber collective defense in 2014, Cybersecurity Information Sharing Act of 2015, Cybersecurity National Action Plan of 2016, etc.

Countering against State-sponsored Cyber Attacks

- 2011-2017 U.S.; Cyber espionage targeting Siemens , Moody's and Trimble (GPS maker).
-> **U.S. charged three Chinese nationals** working for Chinese internet security firm, 2017.11
- 2013.12- 2018 U.S.; cyber espionage targeting US turboprop engine companies.
-> **U.S. charged Yanjun Xu**, identified as an agent of the **Ministry of State Security**, 2018.10
- 2010- 2015 U.S.; cyber espionage targeting US and EU turboprop engine companies.
-> **U.S. charged Zha Rong and Chai Meng**, identified as high rank officers of **the Ministry of State Security**, 2018.10
- 2014.11 U.S.; cyber subversion targeting Sony Pictures Entertainment.
U.S. government identified the attacking group and blamed and sanctioned North Korea (first attributed state-sponsored attack).
-> **U.S. financial sanction against NK**, 2015.1
-> **U.S. criminal complaint against North Korean Park Jin Hyok**, 2018.9
- 2016.2 Bangladesh; cyber theft targeting the central bank, stolen \$81 million
-> **U.S. criminal complaint against North Korean Park Jin Hyok** and state-sponsored "Lazarus" Group, 2018.9
- 2016.11 U.S.; Russian cyber intrusion and espionage targeting Democratic National Committee.
-> **U.S. charged 13 Russian individuals and three Russian entities**, 2018.2
-> **U.S. sanctioned Russian five entities and 19 individuals**, 2018.3
-> **U.S. charged twelve Russian intelligence officers**, 2018.7
-> **U.S. sanctioned 33 Russian individuals and entities**, 2018.9
-> **U.S. charged Russian national**, Elena Alekseevna Khusyaynova, with interfering in U.S. political system, 2018.10
- 2017.5 Europe: Wannacry cyber pandemic spread over the world from Europe.
-> **US, UK, Australia, NZ, Canada and Japan condemn NK on the attack**, 2017.12
-> **U.S. criminal complaint against North Korean Park Jin Hyok**, 2018.9
- 2017.6 Ukraine: Not Petya cyber pandemic spread over the world from Ukraine.
-> **US, UK, Denmark, Lithuania, Estonia, Canada, and Australia jointly attributed and condemn Russia** on the Attack , 2018.2
-> **U.S. sanctioned three Russian individuals and 7 Russian entities**, 2018.6

Way of Future International Cooperation

- To make good use of diplomatic pressure, international society has to promote norms of state behavior in cyberspace, such as to refrain from cyber-enabled theft of intellectual property for commercial gain, not to attack critical infrastructure and not to interfere in internal affairs by means of cyber manipulation.
- In order to protect cyberspace, early detection of cyber attacks is essential and warnings must be shared without delay among like-minded countries. Like-minded partners should make effective use of classified meeting for exchange views on cyber threat situation awareness and potential cyber adversaries.
- Immediate introduction of a joint database of cyber-attacks or automated cyber indicator sharing system is desirable, but is still years away from realization.