Influence of Cyber/Political Warfare by China upon Japan

M.S. Aoki Masao
Research fellow of SSRI

1. History of the Computer, the Internet Systems and Cyber/Political Warfare

In discussing Cyber/Political warfare from China, we need to consider the history of Computer and Internet circumstance not only in Japan and Taiwan, but also China. Furthermore, careful attention on geopolitical issues, their humanity background and technical background should be paid when we consider the circumstance.

As for a viewpoint of the technical background, in 1980’ era, computer and internet systems are used for interoperability network among academic fields like universities, academic institutes and so on. There were comercial computer operatiing system and opensource operating system such as 4.2 BSD, IPv4 and TCP/IP, SMTP, DNS and used to connect each other. Because the network infrastructures for the internet systems, some computer maniacs were creating BBS (Bulletin Board System) and connecting the personal computer to them, and exchanging technical information between computer maniacs.

A few of them were peeping other network systems, and creating malicious software, as is called ‘Computer Virus’. Some computer viruses were infected via internet, and called ‘Computer Worm’. In china, such malicious creators, as is called ‘hacker’, will be about 40 years old or 50 years old from now, I guess, and hackers were lived under the China’s Communist party, and deeply influenced by the Tiananmen Incident at their sensitive teen’s age.

In the late 1990s, China’s internet cafés were starting their services, and in early 2000, mobile internet systems were spread over China. At the same time, the use of the China’s communication infrastructure, so called QQ, began. Some old aged hackers were moving from BBS to QQ, and young peoples who adored them are gathered in the QQ community. Those young hackers seemed to be about 20 years old or 30 years old now.

And, the 2000s was the year when patriotism began to appear on the Internet, and it could be said that the beginning of the age of technology supported.

To consider Chinese cyber/political warfare, It will be necessary to consider not only the technical background but also the geopolitical events at the time of the attack and the age of the attacker against his historical background.

So, we have to tackle on these issues on computer system as follows:

Has the commander of Chinese cyber operation had 1980s computer geek era?

Has the operator of cyber operation infrastructure had 1990s the internet era?

Will cyber operator, who has deep knowledge of smartphone, social networks, cloud system engaged in future operations?

What kind of geopolitical issues will cause a cyber operation?

2. Cyber/Political Warefare against Japan

In the Internet Era at Japan, there were a lot of harmful incidents against the computer system and the network system. Some of such incidents were related to the other country by meaning of IOCs (the indicators of compromise) and TTPs (tactics techniques and procedure), such as IP address, C2 domain, malware type.

The type of incidents can be classified with many viewpoints.

In terms of awareness by the victim, the Incidents are classified as ‘noticeable’ and ‘unnoticeable’. In the former case, the destruction and tampering, such as DDoS attack to the web site, the ransomware to the computer system are noticeable easily. On the other hands, exploitation to computer system, such as cyber espionage is unnoticeable by the victim.

We experienced a lot of web site compromises and DDoS attack against th internet services from China in both early 2000s (00-03) and early 2010s (11-12).

Looking back on the historical background at that time, there were demonstrations driven by patriotism and false history perceptions, so some patriotic hackers were gathered in their domestic social network systems like BBS or blog site, and select the target, showed intentions of attack, done them, competed for results.

Behind those incidents, there were unnoticeable cyber operation with spear phishing email with remote access trojan against the stakeholders of some politics, national defense and so on.

Of course, there were a lot of spear phishing attacks against not only same bodies, but also scientists, engineers, company executives, secretaries and their private email have been observed from 2005 to now.

In terms of cyber operations, those incidents are classified as CNA and CNE. (Table.1)

In the viewpoint of CNE, there are multiple method to achieve the cyber espionage. At some stage, the adversaries chosen targets, selected cyber espionage tools and delivery method.

After those incidents were occurred and detected by victims or cyber security company or cyber security researcher, they created cyber intelligence report or blog post, presentation paper.

By collecting continuously such cyber intelligences and incidents, observed cyber operation, especially cyber espionage has been attributed china, and it turns out that there is state-sponsored activity

In addition, we are observing that the cyber espionage by china have been engaged in continuously around his country border with almost same IOCs, TTPs and intelligence requirements.

Table. 1 Type of Cyber/Political Warfare

Information Operation (IO)	
1	Psychological Operations (PSYOP)
2	Military Deception (MILDEC)
3	Operations Security (OPSEC)
4	Electronic Warfare (EW)
5	Computer Network Operations (CNO)

	Computer Network Attack (CNA)
	Computer Network Defense (CND)
	Computer Network Exploitation (CNE)

3. Conclusion

Chinese cyber/political warfare operations are increasing day by day. And to know those operations, we have to gather their footprint. To mitigate those operations, we use those evidences as a diplomatic card like ‘Naming and Shaming’ and an economic card or so on. But it is difficult to make the cyber situational awareness as is called the targeted cyber operation, because only the targeted person or organizations can only find them. Therefore, the omens of the malicious operation such are the not-opened targeted cyberespionage email, should be gathered to governmental authority, so called intelligence, military, police for the utilization.

In recent years, it is reported that Chinese cyber operations are used with the cognitive domain operations (认知域作战). So we must be careful about their psychological operation, such as Chinese “three warfares” (三战) which are consisting of public opinion warfare (舆论战), psychological warfare (心理战), and legal warfare (法律战).

At Taiwan, China conducted the election intervention on 1998, and distributing a message that inspires the public will via Taiwanese popular social networks.

Especially, incidents timings, IOCs and TTPs of the cyber espionage against Taiwan are mutually helpful to Japan.

So, to counter Chinese cyber domain operation and cognitive domain operation, we must start the cyber cooperation with Taiwan, such as not only the cyber intelligence sharing but also multi domain, multi-dimensional intelligences sharing, including such as the geoip, longitude latitude, satellite images, etc.

Table. 2 The information environment

Information Environment	
1	Physical Dimension
2	Information Dimension
3	Cognitive Dimension