SOCIAL MEDIA IN JAPAN:

AN INVESTIGATION OF THE IMPACT SOCIAL MEDIA HAS ON CYBER-SECURITY AND POLITICS IN JAPAN

By

Wynton El

A Thesis Submitted to The Honors College

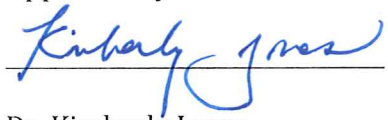
In Partial Fulfillment of the Bachelors degree
With Honors in

East Asian Studies

THE UNIVERSITY OF ARIZONA

DECEMBER 2014

Approved by:



Dr. Kimberly Jones
East Asian Studies

Acknowledgment

The author wishes to acknowledge and thank the many individuals who contributed to the research: Dr. Kimberly Jones, Department of East Asian Studies, University of Arizona.

Abstract

The advancement of technology and social media in East Asia, although innovative, has created an avenue for cyber-criminals to access information from individuals and corporations. Three of the most technologically and economically advanced nations in the world lie in East Asia and have a substantial amount of data in cyberspace. A large volume of sensitive and inadequately protected data is in this continuously growing cloud. This suggests the need for governments in the region to establish increased cyber-security legislation in order to protect national security interests.

The purpose of this research is to investigate the impact social media has on cyber-security and politics in East Asia with an emphasis on Japan. Research suggests that China and South Korea lead Japan in cyber-security; however, Japan is making great strides in effectively securing its cyberspace. With assistance from the United States and other NATO allies, Japan has the ability and means to create an optimal cyber-defense infrastructure that matches its technology innovations.

Key terms: *cyber-attack, cyber-security, cyber-defense, cyber-threats, cyberspace, cyber-crime*

Introduction

East Asia consists of three economically advanced nations: China, Japan and South Korea. Home to the world's top electronic industry and an intelligent workforce, this region is also the largest consumer and producer of social media, largely due to its home-based software messaging applications and networking websites. Thus, this region's governments and civilian populations have a very large volume of sensitive, yet inadequately protected, data sitting on a revolutionary cloud. This sensitive data has been breached many times. Therefore, regional groups like ASEAN+3, NATO, and the Japan US Security Consulting Committee (SCC) are scrambling to develop ways of protecting it (Japan's New Secrecy Law Revives Prewar Memories, 2014). The purpose of this research is to investigate the impact social media has on cyber-security and politics in East Asia with an emphasis on Japan.

Cyber-attacks appear rapidly, without warning, from various places in many forms, so much so that there are thousands of these attacks every day (Security Incidents Continue to Rise in Cost and Frequency while Budgets Decrease, 2014). Securing cyberspace is challenging because of the difficulty in identifying the perpetrators, who have neither fingerprints nor borders. In the past decade, cyber-attacks have been on the rise, but Japan has not followed the rest of the world in implementing security strategies against these attacks. Western media ridiculed Japan after it needed the FBI to help find a lone hacker who spent months taunting the media and local police through email (Alabaster, 2013). Japan's Chief Cabinet Secretary, Yoshihide Suga, said there is a cyber-attack on government sites every two minutes (Kelly and Kubo, 2014). Furthermore, Japan has acknowledged that its cyber-security is not adequate as it prepares for the 2020 Olympics (Kelly and Kubo, 2014).

Even in the East Asian region, the United States is the leader in cyber-security. It is a resident power with over 70,000 troops in Japan and on the Korean Peninsula (Kurtenburch, 2014). However, China and South Korea have strong cyber-defense networks as well, with Japan lagging behind. As allies of the U.S. with mutual concerns, South Korea and Japan partner with the U.S. to combat cyber-threats. On the other hand, due to a 62% increase in cyber-attacks in China, this country is making efforts to become a "cyber-power" (Epstein, 2014). Furthermore, China's president, Xi Jinping, even said, "no internet safety means no national security" (Barboza, 2014).

In 2005, ASEAN+3 (10 countries in Southeast Asia and 3 in East Asia: Japan, Korea and China) formed a national computer emergency team to address cyber-crimes and cyber-terrorism. In 2007, South Korea hosted a Cyber Terrorism Summit to strengthen information sharing and establish a program where Interpol would train regional police: the regional crime database would be linked to that of Interpol which is the world's largest crime information database. In Japan, from 2008 to 2012, attacks had doubled, making cyber-attacks the second most common crime. Ironically, China, which is a member of ASEAN+3, was responsible for 29% of all global bot attacks in 2006. These attacks allowed the perpetrators to gain complete control of the attacked computers (Thomas, 2009).

Social Media

Social media, although convenient and a fairly new and innovative way to communicate with friends, relatives and co-workers, is also an open door for cyber-criminals: specifically, the cyber warriors out of China, as they make up the majority of these attacks (Corrin, 2014). Cyber warriors defend or attack computers and information technology like messaging applications and

online networking websites (Figure 1). As one of the fastest growing mobile phone markets, East Asia has a vast amount of social messaging applications and networks.

Facebook is the worldwide leader in social media networking (Espinosa, 2014) and is also the leading networking website in Korea and Japan, overtaking homegrown networks like Japan's Mixi and South Korea's Cyworld (McKenzie, 2013). However, China's homegrown site, Ozone, dominates its online networking market. China also dominates its social messaging application market with its homegrown WeChat created by the 5th largest Internet Company worldwide, Tencent. Likewise, South Korea's Kakao Talk and Japan's Line dominate their respective social messaging application industries (Tang, 2014) (Figure 2).

As the world's most populace region, East Asia's social media consumption is rapidly growing. In Japan and Korea alone, there are more mobile phone subscriptions than the total population, which means that many mobile phone users have more than one phone. This region's home-grown messaging applications or online networks can access bank accounts, order drinks from vending machines, make video calls, and send animated stickers (popular features in this region). Fifty-eight percent of the Japanese population, 74% of the South Korean population, and 42% of over 1 billion people in China use social media (Tang, 2014).

Social media consumption is based on the percentage of the population using various websites and applications in their respective countries. Furthermore, access via computers is not the only factor in determining usage. With the growing amount of tablet, cell phone and smartphone usage around the world, social applications are more prominent than websites.

Since the end of 2010, Facebook has dominated many East Asian countries as a social media networking website with exception to China (Darwell, 2012). The reason Facebook was not able to penetrate China's market is because the site is banned; however, this does not prevent

users from accessing it through proxy servers. A proxy server is a server that gives a client the ability to access sites and other resources on a server in a different location. With this capability, an anonymous user can pretend to be in another country to gain access to any website offered in that nation. This type of indirect network connection is accessible not only via computer, but also via smartphones (What is a Proxy Server, 2014).

Nevertheless, China's homegrown mobile applications have more users and are more popular than Facebook. Japan's Line and South Korea's Kakao Talk take up a large percentage of their respective countries' mobile application usage and also have a substantial percentage of foreign users. As of January 2014, Japan's Line application had 350 million users; South Korea's Kakao Talk had roughly 100 million, and China's WeChat had over 400 million users (Chan, 2014). Among social messaging users, these three applications make up a large percentage of the world's social media market. This makes East Asia the largest consumer and distributor of social messaging dataflow.

Because of this massive data flow from these three countries in close proximity to each other, there was bound to be an increase in cyber-crime. Cyber-criminals are trying to access information not only from the social messaging applications but also from their respective countries and industries. Unfortunately, the information from applications, government and industry are all connected due to all of the personal information one includes on these applications and websites. Hence, cyber-criminals are able to extract information from these websites/applications and gain private information from unsuspecting private citizens, public officials and industries.

Cyber-Security Problem

This growing cyber-security problem is well known around the world, and it is said that the next world war will not be fought with automatic weapons and bombs, but instead through cyber-attacks in cyberspace. Most of the advanced East Asian nations have been combating this problem. However, Japan is last when it comes to its nation's cyber-security strength and internet related legislation.

Within the past 5 years, cyber-crime has risen tremendously in Japan (El, 2014). A felony that was previously inexistent, cyber-crime has risen to be the second most common crime. This not only includes cyber-attacks from outside Japan but also threats like cyber harassment on internal social applications and websites. A bilateral cyber force between the United States and Japan could counter cyber-attacks coming from outside of Japan (El, 2014). This cooperation is not only required under the 1960 Security Treaty, but it is also in the best interest of the United States. Therefore, both countries should focus more attention toward cyber-attacks coming from within the social media sites and applications. The attacks coming from within may not all be revealing the country's secrets; however, it is also important to protect the privacy of the Japanese citizens.

With the rapid growth of smartphone and mobile application users, cyber-attacks will inevitably be increasingly difficult to combat. In 2010, according to comScore, there were over 10 million smartphones being used in Japan. To add to this, there are over 40 million broadband lines in place, which place Japan in third for broadband use, right behind the U.S. and China (Japan - Broadband Market - Overview, Statistics and Forecasts, 2014). This gives cyber-criminals 40 million access points multiplied exponentially by the individuals connected to them (El, 2013).

Due to the United States security treaty with Japan, Japan has been without a full military. However, they do have a self-defense force comprised of land, air and sea. These troops operate under certain restrictions, such as not attacking another country or leaving their own airspace. This treaty also includes cyber-security attacks, which could be the reason for Japan's lack of a cyber-defense. Nevertheless, they still remain true to their status as a leader in technology and innovation.

Since Japan does not have a full military because of the security treaty, Japan relies on the U.S. for protection. Because of Japan's recent issues with China and North Korea, Japan is a target because of its subpar security and alliance with the U.S. This alliance allows the U.S to protect its interests in the region as a "resident power" in Asia. Therefore, the presence of the United States Forces in Japan (USFJ) represents a symbol of strength to the American power in the region. Due to common security concerns, the Japanese Ministry of Defense (MOD) engage in joint naval drills with the United States Department of Defense (DOD), and share interoperable intelligence, surveillance and reconnaissance capabilities (ISR) (El, 2013).

The Challenge of New Media

As a democracy, Japan should be making its citizens' personal information more secure. Of course, this has become an increasingly difficult task with new media. New media including social media, smart phones, and cloud computing are innovative and have created a new avenue for the world to do business and interact; however; they also pose an increased security risk to all citizens. Does global communication really outweigh personal privacy?

Through new media, many databases of information have consisted of individuals' information, including information such as addresses, phone numbers, and maybe even maiden names. This information was always available, but new media has made it more accessible.

Along the same lines, communication with friends was always possible, but social media made communication instantaneous among people across the world. As stated in the 2013 National Security Strategy, new technology has created avenues that are necessary for modern business strategies, but it also created security risks for companies and citizens.

There is not much that can be done about the amount of information in cyberspace, but the information can be protected through security measures. Large corporations such as Google, Line and Apple all have many customers' personal information in their databases. Therefore, when a cyber-criminal attacks one of these companies, it is not just the company, but also the customers' information that is at risk. Therefore, Joichi Ito, an advocate for Internet freedom, said, "It is essential to understand the difference between personal privacy and transparency. While individuals have a right to privacy, powerful institutions must operate transparently so that abuses of power are not concealed by veils of secrecy" (Ito, 2014).

One aspect of protecting customers' data is divulging information about attacks that have occurred. This information may be critical to preventing similar attacks. Therefore, the problem lies within the corporations that are not operating transparently.

Not only could they be preventing other attacks, but they also could be helping to rebalance democracy (Ito, 2014). Japan, as one of the world's technology powerhouses, is the hub for a great deal of the data flow in the 21st century. This gives us the ability to contact almost anyone with Internet access anywhere in the world. Democratic countries are built on the thought that democracy is based on the will of the majority while also protecting the rights of minorities. This can only happen if there is a "competition of ideas." This entails the ability to criticize those in power without backlash (Ito, 2014).

Evolving Threat to Democracy

New media has surely started to affect the balance of democracy as it has given those in positions of power and influence the ability to control what is on the Internet. The control of information in one medium is not necessarily significant when it comes to democracy; however, when most of these countries have a large percentage of their population using the Internet, it can affect the competition of ideas. Also, when ideas of the majority cannot be heard or their voice is silenced by power figures, this creates an imbalance on the structure of democracy (Ito, 2014).

The Japanese government imposed a national order censoring the freedom of speech and press between 1925 and 1945 because the international communist movement drew the suspicions of the government. During this period, over 75,000 Japanese citizens were arrested and prosecuted for violating the law which suppressed freedom of speech (Japan's New Secrecy Law Revives Prewar Memories, 2014). Because of this history, a large percentage of the Japanese civilian population developed animosity towards censorship. So when the Diet passed the Special Secrecy Law, developed after the U.S. National Security Agency in November 2013, it angered the populace. The populace met this new law with protest. However, Japan's government was pressured into implementing this law. For example, the U.S pressured Japan in order to ensure that shared confidential information is kept secure (Japan Today, 2013; El, 2013).

The Government and Social Media

Unlike China, Japan is trying to balance individual rights with modern technological advances and regulations. When it comes to elections, conventional campaigns that only utilize posters, loud speakers, leaflets and town hall meetings are becoming archaic. Until the summer of 2013, the Public Officers Election Law (POEL) of 1950 was the official law governing elections in Japan. It regulated politicians' campaigning abilities two to three weeks before the

national, municipal parliamentary, and prefectural elections. Politicians were prohibited from using the Internet and other social media outlets to promote their campaigns. At over 80% penetration, Japan is one of the largest populations of internet users in the world (Tang, 2014). Thus, many Japanese politicians found it imperative to be able to reach the vast majority of the population through social media and the Internet during the most important time of their campaigns.

In America today, our politicians always utilize social media and the Internet to promote their campaigns. President Barack Obama successfully utilized social media, including Facebook and Twitter, to promote his campaign during both his 2008 and 2012 campaigns. In addition, both Facebook and Twitter have tutorials and technical support to help politicians improve their sites.

Conversely, South Korea had a similar law to that of Japan against campaigning via the Internet during the last few weeks of campaigns. Towards the beginning of 2013, however, the South Korean legislature lifted this law and allowed politicians to utilize the Internet for campaigns. Not long after this amendment, Japan followed this movement and, in February of 2013, it relaxed the Public Officers Elections Law (Mie, 2013). Japan came one step closer to advancing in cyber and social media related legislation; however, this does not begin to solve the cyber-security and defense issues that have been bombarding this country for years.

Japan is now trying to change this imbalance of democracy by allowing social media to influence more decisions and become more prominent. As social media and the Internet become more widely used in Japan, the limitation of their use will hinder the competition of ideas. Including the relaxing of the POEL, the Japanese government has made strides to develop social media sites in order to help release pertinent information. An example is the transparency of the

Tokyo Metropolitan Police in releasing a twitter site in October of 2012 to disclose recent crimes and also solicit assistance from its citizens (Hongo, 2014). Citizens are able to collaborate with an officer and relay any information that they may have in conjunction with the case. They also receive any updates on the crime in real time. This has played a big role in solving recent crimes and is only one example of how social media has made an impact on Japan.

US/ Japan Relations

It is difficult, if not impossible, for one country to handle the global challenge of securing cyberspace. Therefore in 2012, Prime Minister Noda Yoshihiko issued a joint statement with President Obama agreeing to share information on cyber-attacks and continue their important partnership in cyber-security. The United States Department of Defense (DOD) and other intelligence agencies like the National Security Agency (NSA) are working together with Japan to help thwart cyber-attacks. This collaboration is essential because in January 2013 the Japanese ministry was exposed to a cyber-attack where over 300 documents were compromised. Some of these documents were reported to be conversations between the previous Japanese Prime Minister Noda Yoshihiko and United States President Barack Obama, according to the Japan Daily Press (El, 2013). There were also other cyber-attacks over the disputed Senkaku/Diaoyu islands that originated from Chinese hackers (Torres, 2013).

At a press conference in May 2009, President Obama said: “cyber-threat is one of the most serious economic and national security challenges we face as a nation” and that “America's economic prosperity in the 21st century will depend on cyber-security.” Japan is key to the U.S. stability in Asia, but very vulnerable to cyber-threats. Therefore, intelligence sharing between Japan and the U.S. is vital to securing the critical information technology infrastructure we both share (El, 2013).

America has helped Japan in implementing and improving their cyber-security strategies. However, the majority of these strategies involve corporation's security systems, and do not protect against social media sites, or the many applications on citizens' smart phones. This is a major problem for Japan because their security implementations are not fully inclusive. They overlooked the fact that over 40 percent of their populace is using the social messaging application, Line. Nevertheless, because the government must be sensitive to its citizens' fear of censorship, this is still an improvement for Japan (El, 2014).

Government Strategies

Luckily in 2013, Japan began to recognize that it needed a cyber-security act to help combat this new type of crime. High-ranking officials from Japan also met with President Obama and the American military generals to strengthen their information sharing and cyber-defense (Kyodo, 2013). As a result, Japan is now forming Internet security partnerships with its allies. Lastly, Japan relaxed the Public Officers Election Law to give politicians the opportunity to take advantage of a source that 80 percent of their population is using (Tang, 2014).

Japan's 2013 national security strategy covers numerous benefits and risks of innovations during the 21st century. This new technology not only makes the average citizen's ability to communicate with friends and family easier, it also creates instantaneous communication for the government and large corporations. With new technology, the government is able to move large quantities of information at a moment's notice. This new technology and innovations have also helped Japan to expand economically by developing into one of the most technologically advanced countries in the world (El, 2014).

Advancements in technology have changed the world. With Japan in the center of technology innovation, it has an exponentially growing network of social systems and advanced

networks. Ultimately, cyberspace is essential in order to keep information flowing and business booming. The majority of businesses use some sort of cyberspace in their daily operation ("National Security Strategy", 2013; El, 2014).

Big data is a subject that has been discussed in recent political news in Japan. It refers to the vast amount of information that is stored in cyberspace by many different companies. Large companies like Google and Apple all have an abundance of information in cyberspace, which can be accessed anywhere in the world. Social media companies operate in the same way with all of their customers' information sitting in cyberspace able to be accessed anywhere in the world. Therefore, the privacy of these companies using this cyberspace or cloud computing must be protected.

Companies in Japan and around the world are not always openly transparent when using cyberspace and technology in their business. One controversial use of big data that became public recently in Japan dealt with supermarkets and retail stores. These stores were collecting data after every purchase. The data collected consisted of the customers' gender, age and amount of the purchased items. All of this information was collected without the customers' consent. The company or store would then proceed to use the information gathered to align their product inventory to the buying habits their prospective consumers.

Stores used this data to grasp the *dankaiseidai* (baby boomer) market. This market was a hard market to grasp because baby boomers purchase items that someone roughly 10 years younger would usually buy. Furthermore, these consumers also like expensive items. From this information, stores were able to change their marketing campaigns in order to attract the *dankaiseidai* market. They knew the age range from their data and started selling items that appealed to this market, such as golf clubs with gemstones.

This technology does infringe on privacy if its use is not divulged, but at the same time it can be utilized by both companies and the government. This ability can help companies with their inventory management advertising through the Internet and social media to reach a certain demographic. It can also help the government make economic decisions. In 2013 Prime minister Shinzo Abe was able to see how new economic policies were affecting spending in supermarkets and online avenues through Big Data (Obe, 2013). Big Data is not a perfect source for economics, but it is useful for gauging the spending habits and interests of the populace.

Pertaining to the 2013 National Security Strategy, this globalization and technology boom does have its downside. Before technology and information was stored in the cloud and cyberspace, it was easier for Japan to prevent attacks and secure its citizens' privacy. This technology has created a new type of crime, and it is making the citizen's feel vulnerable as these attacks cannot be predicted or well traced. At the same time, the architects of the security strategy recognize that new technology, such as cloud computing and Big Data, is effective and necessary to keep business and the government performing at high levels of productivity and innovation.

The Cost

The cost of cyber-security is continuing to rise globally, and Japan ranks in the top three for spending behind Germany and America, respectively. Companies are quickly discovering that having a security strategy in place, even though it may be costly, will ultimately pay off in the end. Unfortunately, Japan was slow to realize this. However, in recent years (2013 -2014), Japan's defense strategies toward cyber-threats have been well funded and implemented.

Cyber-attacks affect all industries, but technology, energy and financial industries encounter the highest cost associated with cyber-crime. Over 30 million dollars are spent

annually to defend these industry sectors (2014 Global Report on the Cost of Cyber Crime). With the vast amount of technology innovations that are conducted in Japan, all technology or energy related companies must have a solid cyber-security strategy in order to protect their information.

From 2012 to 2014, cyber-attacks have risen from 262 to 429 attacks per week (2014 Global Report on the Cost of Cyber Crime, 2014). This is a major increase in attacks, and it shows how prevalent these types of attacks are. The most costly threat comes from malicious insiders, and Japanese corporations are affected by this type of attack substantially more than any other country in the world (2014 Global Report on the Cost of Cyber Crime, 2014). This is surprising as this means there are many trusted individuals that are attacking their own company. Japanese salary men, unlike that of their western counterparts, are known to be loyal to their companies and rarely switch jobs during their career (Lincoln and Doerr, 2012). Therefore, it is interesting that Japan has the highest percentage of malicious insiders.

Furthermore, defending against malicious insiders is a difficult task, and the impact of these cyber criminals could be catastrophic. If these offenders work at a security or technology facility, they already have access to secure networks and individuals' personal information. These savvy cyber criminals do not need to hack into any servers or get past any firewalls. This makes them very dangerous, especially if they are giving information to experienced criminals outside of their company or country. Moreover, since it would take longer to find this sort of perpetrator, the cost to defend this threat also increases (2014 Global Report on the Cost of Cyber Crime, 2014).

Path Forward

Ultimately, there are many changes that need to be implemented in order for Japan to protect itself and its citizens. Communication with the United States and allies under the 1960

security treaty needs to be continued. Furthermore, Japan has to improve its cyber-attack detection systems not only in industry applications but also in its government systems. Japan also needs to regulate the information that can be taken by a company from its customers. Moreover, it must require cyber-attacks be reported whether they are inside or outside the government. This is what Japan seeks to change with the National Security Strategy.

With the advanced technology of Japan, improving cyber detection systems should not be difficult; however, the cyber-hackers are usually just as smart as or smarter than the engineers of the detection systems. Therefore, the government should fund training honorable individuals in computer science and cyber-warfare in order to combat these criminals. Similar to what the U.S. has with the NSA and what China is doing with cyber-warriors, creating a group of specialists or a task force solely for combating these attacks will strengthen Japan.

A democratic country should want the support of its citizens. Therefore in order to keep this support, Japan needs to regulate the data that companies are allowed to collect on their customers. For a company to prosper, it must know its market; however, this information should only be taken with the consent of the customer.

The most important step that needs to be made is improving communication regarding cyber-attacks whether they take place inside or outside of the government. This means that the large corporations like Line, Google and Facebook (that have a large presence in Japan's cyberspace) need to share information on cyber-attacks in order to secure their critical cyber infrastructure. It happens too often that a cyber-criminal goes after multiple companies attempting to take the same information. Without communication, all companies could fall prey to the intrusion in the same way (El, 2014).

If this information was shared among the government, public, and private sector, one cyber-attack may be enough to prevent a second threat from the same cyber-criminal. The communication agreement between Japan and the United States will accomplish this task (El, 2014). They are now relaying information regarding intrusion attempts on government agencies. Under the 2013 fiscal year budget, Japan created a cyberspace defense unit (Bolster cyber-attack defenses, 2013). This unit was launched in early 2014 and is composed of personnel form the air, ground, and maritime branches of the Japanese Self Defense Force. This is a joint task force with the purpose of thwarting cyber-attacks. This force does not have the ability to retaliate; however, with the communication agreement with the U.S. and NATO allies, this could be a big step toward combating attacks.

Also in 2013, the National Police Agency decided to create a unit to investigate cyber-attacks. These units were set up in 13 different locations across Japan and were manned with 140 cyber specialists. These units will be working with the precincts in their prospective areas to help defend against cyber-attacks happening within Japan (Bolster cyber-attack defenses, 2013).

This all works well to protect the government and populace of Japan; however, when there is important information in a private company, and they are not told about the attempt on the government, they could be susceptible to the same attack. This is where Japan and the rest of the world needs to improve. There needs to be better communication between the private industry and the government when it comes to cyber security.

Overall, it appears that social media has a great impact on cyber-security and politics in East Asia. Japan has the largest percentage of its population using the Internet in the world, and most of this usage is through mobile applications. In the 5 years from 2008 to 2012, cyber-crime has risen to the second most frequent crime, and before 2013 there was no legislation regarding

security of social media. In addition, there is no communication between the government and industry regarding hacking attempts. Like the communication between the United States and Japan on this topic, large companies with a presence in cyberspace need to be in communication not only with the Japanese government but with other allied nations as well.

Conclusion

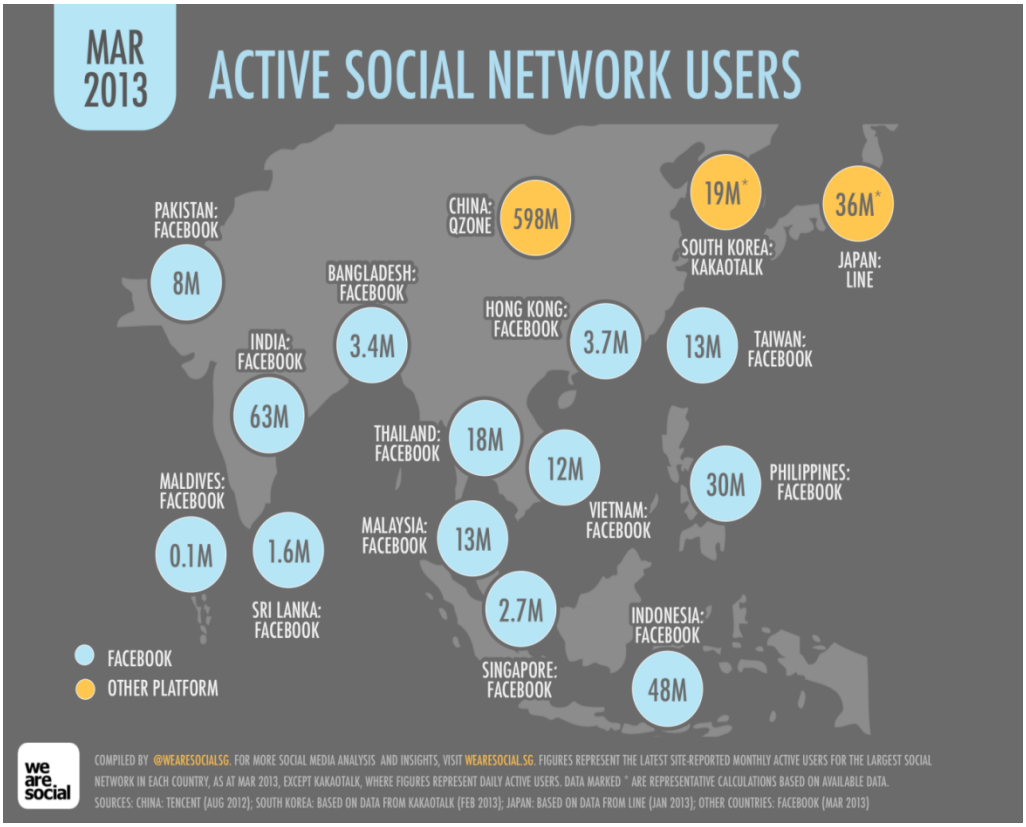
As the third largest economy in the world, and with 80% of the population using social media, Japan's economic strength cannot survive without improved cyber-defense. Recently, Japan has taken encouraging steps toward strengthening its cyber-defense on a broader scale. For instance, the Diet passed a secrecy law to set up a cyber-defense system and to monitor Internet activity. Presently, officers from the Japanese Self-Defense Force (SDF) are now receiving advanced cyber-defense training at the U.S. Cyber Command. This is necessary because the SDF seeks intelligent members who are well versed in cutting edge cyber-defense infrastructures. In addition to the U.S., Japan is now sharing intelligence with counterparts in Great Britain, NATO, India, Belgium, France and Germany (Miller, 2014).

These timely actions by Japan will foster a better partnership with its allies in combating the escalating territorial dispute with China over the Senkaku/Diayou islands in the East China Seas, military drills between China and Russia in a gray area of the East China Seas, recent rocket launches by their adversary in North Korea, and internal and external cyber-security threats. Although sensitive to its citizen's fears regarding these changes, Japan's leadership in implementing drastic measures to secure cyberspace is commendable. After its 1st cyber-security drill in March 2014, Japan's cyber-security Chief Cabinet Secretary, Yoshihide Suga, said, "Cyber-attacks are becoming more subtle, sophisticated and international, and strengthening Japan's response to them has become a critical issue" (Kelly and Kubo, 2014).

Image of China's Cyber Warriors

Figure 1: Source: Epstein, Mike. Digital Trends Mar 28, 2014

Largest Social Media Networks in East Asia by Country



Source: We are Social http://wearesocial.net/tag/statistics/ Jan. 2014
Figure 2

WORKS CITED

2014 Global Report on the Cost of Cyber Crime. Rep. N.p.: Phonemon Institute, October, 2014. Web.

Alabaster, Jay. "LOLCats and PC Viruses - Japan Gets a Lesson in Cybersecurity." *Computerworld*. Web. 18 May 2014.

Barboza, David. "China's President Will Lead a New Effort on Cybersecurity." *The New York Times*. The New York Times, 27 Feb. 2014. Web. 17 May 2014.

Bloomberg Business Week. Bloomberg. Web. 18 May 2014.

"Bolster cyber-attack defenses." The Japan Times. (April 1, 2013, Monday): 519 words. LexisNexis Academic. Web. Date Accessed: 2014/12/06.

Chan, Stephanie. "The 10 Most Popular Mobile Messaging Apps In The World." ReadWrite. Web. 18 May 2014.

"Chat Apps." Tech in Asia. Web. 18 May 2014.

"China's WeChat Focuses on US-Based Users." TNW Network All Stories RSS. Web. 18 May 2014.

Corrin, Amber. "Can Our Cyber Cadre Compete with China?" Web. 6 May 2014

Darwell, Brittney. "Facebook Reaches 10M in Japan, Doubles Users in 6 Months - Inside Facebook." Inside Facebook. Web. 18 May 2014.

"EDITORIAL: Internet Election Campaigns Can Change Japan's Politics - AJW by The Asahi Shimbun." AJW by The Asahi Shimbun RSS. Web. 18 May 2014.

El, Wynton. "Regional Political Economics Essay." GLS 200 final paper, University of Arizona, 2013.

El, Wynton. "Cyber Security in Japan." POL 202 final paper, University of Arizona, 2014.

Epstein, Mike. "Chinese Security Experts Partly Blame the U.S. for Last Year's Surge in Cyber Attacks." Digital Trends. Web. 18 May 2014.

Espinosa, Johnathan. "Facebook Overtakes Japanese Social Network Mixi in Japan - Inside Facebook." Inside Facebook. Web. 18 May 2014.

Hongo, Jun. "Tokyo's Criminal Investigators Launch Twitter Account #Finally." *Japan Real Time RSS*. N.p., 29 May 2014. Web. Oct. 2014.

Ito, Joichi, and Jon Lebkowsky. "Weblogs and Emergent Democracy." *1 Emergent Democracy*. N.p., n.d. Web. Sept. 2014.

"Japan - Broadband Market - Overview, Statistics and Forecasts." - BuddeComm. Web. 18 May 2014.

"Japanese Social Media & Internet Facts." Japanese Social Media & Internet Facts. Digital Jungle. Web. 18 May 2014.

"Japan's New Secrecy Law Revives Prewar Memories." *East Asia Forum*. Web. 18 May 2014.

"Japan Today." Japan Today RSS. Web. 18 May 2014.

Kan, Michael. "Security." InfoWorld. Web. 18 May 2014.

Kelly, Tim, and Nobuhiro Kubo. "Japan Holds First Broad Cybersecurity Drill, Frets over Olympics Risks." Reuters. Thomson Reuters, 18 Mar. 2014. Web. 18 May 2014.

Kurtenburch, Elaine. "Obama Visit to Asia Seen as Counterweight to China." The Big Story. Web. 18 May 2014.

Kyodo. "Japan, U.S. Agree to Beef up Cybersecurity." *The Japan Times*. The Japan Times, 3 Oct. 2013. Web. 6 July 2014.

Lincoln, James, and Bernadette Doerr. "Cultural Effects on Employee Loyalty in Japan and The U. S.: Individual- or Organization-Level? An Analysis of Plant and Employee Survey Data from the 80's." *Cultural Effects on Employee Loyalty in Japan and The U. S.: Individual- or Organization-Level? An Analysis of Plant and Employee Survey Data from the 80's*. N.p., Apr. 2012. Web. 24 Nov. 2014.

McKenzie, Hamish. "As It Faces Bloody Battle with Messaging Apps, It Seems Facebook's Doing Just Fine on Mobile." Web. 18 May 2014.

Mie, Ayako. "Diet OKs Internet Election Campaigns." Japan Times RSS. Web. 18 May 2014.

Miller, J. Berkshire. "How Will Japan's New NSC Work?" The Diplomat. Web. 18 May 2014.

"National Security Strategy." 17 Dec. 2013. Web. 18 May 2014.

Obe, Mitsuru. "Japan Looks to Big Data for Timely Economic Indicator." *Japan Real Time RSS*. The Wall Street Journal Japan.Web. 23 Sept. 2013.

"Security Incidents Continue to Rise in Cost and Frequency While Budgets Decrease, Accordingto PwC, CIO and CSO's The Global State of Information Security® Survey 2015."*Pricewaterhouse Coopers*. N.p., Sept.-Oct. 2014. Web. 24 Nov. 2014.

Smith, Craig. "27 Amazing Facebook Mobile & App Statistics (Updated April 2014)." DMR. Web. 18 May 2014.

Smith, Craig. "By the Numbers: 105 Amazing Facebook Statistics (Updated April 2014)." DMR. Web. 18 May 2014.

Song, Huei. "Battle of the Mobile Messaging Apps - Whatsapp, Line, WeChat, Kakao Talk, ChatON and Viber | Lowyat.NET." LowyatNET Battle of the Mobile Messaging Apps WhatsApp LINE WeChat Kakao Talk ChatON and Viber Comments. Web. 18 May 2014.

Takahashi, Toshiya. "Japan's New Secrecy Law Revives Prewar Memories." East Asia Forum. Web. 18 May 2014.

Tang, Haiya. "KakaoTalk." We Are Social Singapore RSS. Web. 18 May 2014.

"The 10 Most Popular Mobile Messaging Apps In The World." ReadWrite. Web. 18 May 2014.

Thomas, Nicholas. "Cyber Security in East Asia: Governing Anarchy." Taylor & Francis. Web. 18 May 2014.

Torres, Ida. "Top Secret Trade Documents Stolen from Farm Ministry Computers." *The Japan Daily Press*. N.p., 03 Jan. 2013. Web.

"U.S., Japan Have Two-day Meeting on Cybersecurity Issues." UPI. Web. 18 May 2014.

"WeChat Hits 355M Users, Ahead of International Push - Mobile World Live." Mobile World Live. Web. 18 May 2014.

"WeChat Is Nothing like WhatsApp-and That Makes It Even More Valuable." Quartz. Web. 18 May 2014.

"What Is a Proxy Server?" *What Is a Proxy Server?* What Is My IP Address, n.d. Web. 11 Dec. 2014. <http://whatismyipaddress.com/proxy-server>.

"World Map of Social Networks." Vincos Blog. Web. 18 May 2014. https://ideas.repec.org/p/cdl/indrel/qt8sc9k91b.html.