ASIAN CAUCUS
Topic A: Obstructing the Advance of Cyber-terrorism

Chair: Justice Howard
Vice-Chair: Leandro Campos
SALMUN 2014

INDEX

Background Information

Over the past decade, Internet usage has exploded, growing five-fold from 361 million users in 2000 to 2.8 billion today. The World Wide Web is very much a part of our everyday lives and provides a vast wealth of information and communication possibilities. However, the easy access and widespread use of the Internet has attracted a range of criminal activities. In fact, the US Director of National Intelligence has ranked cybercrime as the top national security threat, higher than that of terrorism, espionage, and weapons of mass destruction and recently FBI Director James B. Comey remarked at a recent security conference that "The playground is a very dangerous place right now."

As one of the fastest-growing criminal activities on the planet, cybercrime is moving higher up the agenda of countries around the globe. Critical infrastructure systems used in electrical power distribution, oil and gas pipelines, water supplies, and transportation are particularly vulnerable because their legacy architecture may be easier to compromise. Last month, more than 20 countries in the region of Asia and the Pacific joined UNODC, guardian of the United Nations Convention against Transnational Organized Crime, and the

International Telecommunication Union (ITU) to discuss ways in which cybercrime can be tackled.

The rapid growth in Internet use in Asia, including a tenfold or more increases in access in China, Indonesia, and India since 2002 has also been accompanied by significant increases in cybercrime. The development of commercial-scale exploit toolkits and criminal networks that focus on monetization of malware has amplified the risks of cybercrime. The law-enforcement response in Asia is briefly reviewed in the context of the 2001 Council of Europe's Cybercrime (Budapest) Convention. We describe the nature of cybercrime and compare the laws and regulations in Asian states with the provisions of the Convention. The challenges faced in developing effective cross-national policing of cybercrime in Asia are also addressed as problems emerge around cloud computing, social media, wireless/smart phone applications and other innovations in digital technology.

On the other hand, developing preventive measures capable of withstanding attacks from other governments has been a growing trend. Especially after the Obama administration's very public indictment of five Chinese military hackers for cyber-attacks against U.S. companies and a labor union. The indictments have revealed the sheer scope of China's large-scale cyber warfare and cyber espionage operations. Beijing's key cyber warfare and cyber spying unit is a secretive, Shanghai-based group called Unit 61398 that has deep roots in the Chinese military, the People's Liberation Army (PLA).

Timeline

November 2003: Hackers, believed by U.S. officials to be backed by the Chinese military, search to find vulnerable computers in the military's computer network and steal sensitive information. The attacks continued for about three years and were given the name Titan Rain by U.S. officials.

July 2008: In the weeks before the war between Russia and Georgia, Georgia is hit by distributed-denial-of-service (DDoS) attacks and many of the government's computer networks are disabled, including that of President Mikheil Saakashvili. Media and transportation companies are also affected. Georgian officials accused Russia of launching the attack.

November 2010: Iranian president Mahmoud Ahmadinejad acknowledges that the Stuxnet worm destroyed about 1,000 of the country's 6,0000 centrifuges at its nuclear facility in Natanz. Israel and the U.S. are believed to be behind the attack in an attempt to slow Iran's progress toward obtaining nuclear weapons.

December 2010: Anonymous attacks several businesses seen as "enemies" of WikiLeaks. The action was in response to the arrest of WikiLeaks founder, Julian Assange. In 2010, WikiLeaks provided several news organizations with hundreds of thousands of secret government and military documents about the wars in Iraq and Afghanistan, as well as cables that gave a behind-the-scenes look at American diplomacy from the perspective of high-level officials.

June 2011: Officials at the International Monetary Fund report that in the previous months it had been hit by "a very major breach" of its computer systems. The FBI announced evidence linking the Chinese government to the attack.

May 2012: The U.S. Department of Homeland Security announces that spear fishers have penetrated the computer systems of U.S. gas pipeline systems.

September 2012: Nine banks in the U.S., including the Bank of America, Wells Fargo, and JP Morgan Chase, were hit by a distributed-denial-of-service attack that denied customers access to the banks' websites for several days. The Islamic hacktivist group Izz ad-Din Al-Qassam Cyber Fighters (also called the Al-Qassam Brigades) takes responsibility for the attack. The group is linked to the military wing of Hamas.

May 2014: The U.S. the Justice Department unsealed an indictment of five members of Unit 61398 of the Chinese People's Liberation Army, charging them with hacking into the computer networks of Westinghouse Electric, U.S. Steel Corp., and other companies. Shanghai-based Unit 61398 is the cyber division of China's national army. The move is considered largely symbolic since there is little chance the men will surrender.

Key Terms

Cybercrime - refers to any crime that involves a computer and a network. The computer may have been used in the commission of a crime, or it may be the target.

Cyber-warfare - politically motivated hacking to conduct sabotage and espionage. It is a form of information warfare sometimes seen as analogous to conventional warfare.

Unit 61398 - the Military Unit Cover Designator (MUCD)[1] of a People's Liberation Army advanced persistent threat unit that has been alleged to be the source of Chinese computer hacking attacks.

United Nations Convention against Transnational Organized Crime - the main international instrument in the fight against transnational organized crime.

International Telecommunication Union (ITU) - specialized agency of the United Nations (UN) that is responsible for issues that concern information and communication technologies. The ITU coordinates the shared global use of the radio spectrum, promotes international cooperation in assigning satellite orbits, works to improve telecommunication infrastructure in the developing world, and assists in the development and coordination of worldwide technical standards. The ITU is active in areas including broadband Internet, latest-generation wireless technologies, aeronautical and maritime navigation, radio astronomy, satellite-based meteorology, convergence in fixed-mobile phone, Internet access, data, voice, TV broadcasting, and next-generation networks.

Distributed-denial-of-service (DDoS) - attempt to make a machine or network resource unavailable to its intended users.

Guiding Questions

- What constitutes a cyber-attack, cyber espionage, and hacking?

- How should these actions be responded to? When does the use of information technology constitute an act of aggression?

- What principles can guide an international agreement on the limitations of the use of information technology for the sake of maintaining international peace and security?

- What role should existing bodies, such as the United Nations Security Council have in determining the responsibility for destabilizing cyber attacks?

- How should member states respond to the potential threat from non-state actors that acquire offensive cyber technology?

Further Research

Insightful analysis:
http://www.pwc.com/en_US/us/increasing-it-effectiveness/publications/assets/2014-us-state-of-cybercrime.pdf
http://www.emc.com/collateral/white-paper/rsa-cyber-crime-report-0414.pdf
http://limun.org.uk/FCKfiles/File/DISEC_St_Gd_Final.pdf

Official Documents:
http://www.unodc.org/unodc/en/frontpage/2011/October/cybercrime-in-asia-pacific_-countering-a-21st-century-security-threat.html

News and articles:
http://www.atlcom.nl/site/english/nieuws/wp-content/Hughes.pdf
http://link.springer.com/chapter/10.1007%2F978-1-4614-5218-8_4#page-1
http://www.nytimes.com/2014/05/23/world/asia/us-case-offers-glimpse-into-chinas-hacker-army.html?_r=0