Jus ad Bellum and Cyber Warfare in Northeast Asia

Boris Kondoch*

Cyber attacks have become a grave threat to international peace and security. Northeast Asia is a critical point of many of these cyber operations. First, South Korea has been the target of cyber attacks from North Korea. Second, there are harsh debates on this matter between the US and China. While the United States have expressed their concerns about the growing threat of cyber intrusions from China, the People's Republic of China has blamed the US for attacks against their respective computer networks. From the perspective of the jus ad bellum, potential cyber attacks raise a number of difficult and complex issues. The following article examines which cyber operations amount to the use of force as stipulated in Article 2(4) of the UN Charter and discusses the conditions under which type of cyber attacks could trigger the right to self-defense. In addition, other available remedies outside the framework of Article 51 of the UN Charter will be discussed.

Keywords

Cyber Attack, Jus ad Bellum, Right to Self-defense, Armed Attack, Pre-emptive Self-defense, Security Council, ICJ, ICC, Counter-Measures

Cyber war is arguably at the most serious end of the spectrum of security challenges posed by – and within – cyberspace.

On Cyber Warfare[1]

The wars of the 20th century were those of oil and bullets, but the war of the 21st century are information wars.

Kim Jong-il[2]

* Professor at the Far East University, Korea and General Editor of the Journal of International Peacekeeping (Brill/Martinus Nijhoff). Diplom-Jurist (Johann Wolfgang Goethe-Univ.). The article is dedicated to Professor Sung Hack Kang (Korea University), one of the leading political scientists of Korea, for his warm hearted and intellectual support as my mentor. The author would like to express his gratitude to Professor Bruce 'Ossie' Oswald and Professor Eric Yong-Joong Lee for their warm encouragement and comments. The author may be contacted at: kondoch@hotmail.com / Address: Far Eastern University, Eumseong-gun, Chungcheonbuk-do 369-700 Korea.

DOI: http://dx.doi.org/10.14330/jeail.2013.6.2.06

1 P. Cornish et al., *On Cyber Warfare*, A Chatham House Report, Nov. 2010, *available at* http://www.chathamhouse.org/publications/papers/view/109508 (last visited on Aug. 19, 2013).

2 Hyeong-woo Lee & Kang-kyu Lee, *Cyber War and Policy Suggestions for South Korean Planners*, 21 Int'l J. Korean Unification Stud. 2, 85-106, 96 (2012).

1. Introduction

Cyberspace has become a national security concern since the last twenty years.[3] While some commentators view the current debate on cyber war as exaggerated and as hype,[4] others including US Defense Secretary Leon Panetta are warning that a cyber version of 9-11 or Pearl Harbour could take place in the near future.[5] Many States including China, Russia and the United States consider 'cyberspace' as a future battleground. They have responded to the threat from cyberspace by formulating cyber strategies and incorporating cyber units into their armed forces. Although cyber war has not yet occurred, there have been frequent reports about so-called cyber attacks.[6] Cyber attacks may be defined as any harmful activity in cyberspace including *inter alia* those operations with "the aim to degrade, disrupt, deny or destroy information resident in computers, or to compromise the computers themselves."[7] Typical examples of cyber attacks are distributed denial of service attacks, planting inaccurate information, and infiltration of secure computer networks. Many cyber attacks are still carried out by private individuals (hackers, organized criminal networks, industrial spies) rather than government-sponsored hackers.

International lawyers started to show an interest in the legal regulation of cyber warfare during the late 1990s.[8] The academic debate continued after September 11 because of the potential threat of computer network attacks conducted by terrorist

3 For details, *see* D. Reveron, Cyberspace and National Security, Threats, Opportunities, and Power in a Virtual World (2012).

4 *See, e.g.*, T. Rid, *Cyber War Will Not Take Place*, 35 J. Strategic Stud. 5-32 (2011); T. Rid, *Think Again: Cyber War. Don't Fear the Digital Bogeyman. Virtual Conflict Is Still More Hype than Reality*, Foreign Pol'y, Feb. 27, 2012, *available at* http://www.foreignpolicy.com/articles/2012/02/27/cyberwar (last visited on Aug. 20, 2013); B. Valeriano & R. Maness, *The Fog of Cyberwar. Why the Threat Doesn't Live up to the Hype*, Foreign Aff. Nov. 21, 2012, *available at* http://www.foreignaffairs.com/articles/138443/brandon-valeriano-and-ryan-maness/the-fog-of-cyberwar (last visited on Aug. 20, 2013).

5 E. Bumiller & T. Shanker, *Panetta Warns of Dire Threat of Cyberattack on U.S.*, N.Y. Times, Oct. 11, 2012, *available at* http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html?_r=0 (last visited on Nov. 5, 2013); J. Healey, *Preparing for Cyber 9/12*, Atlantic Council, *available at* http://www.atlanticcouncil.org/publications/issue-briefs/preparing-for-cyber-9-12 (last visited on Nov. 5, 2013).

6 For details, *see* H. Dinniss, Cyber Warfare and The Laws of War 281-292 (2012).

7 M. Roscini, *World Wide Warfare – Jus ad bellum and the Use of Cyber Force*, 14 Max Planck U.N.Y.B. 91-96 (2010). For further discussion of the terms cyber warfare, cyber crimes and cyber attack, *see* O. Hathaway et al., *The Law of Cyber Attack*, 100 Calif. L. Rev. 817-886 (2012).

8 *See, e.g.*, M. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 Colum. J. Transnat'l L. 885-938 (1999); W. Sharp Sr., Cyber Space and the Use of Force (1999).

groups.[9] Four further events intensified the discussion to what extent the traditional rules governing *jus ad bellum* and *jus in bello* can be applied to cyber operations. In 2007, a series of cyber attacks took place against Estonian government websites, banks, broadcasters and newspapers. The source of the attacks remains unclear to date. One year later, in the context of the 2008 South Ossetia war, Georgia alleged that Russia had conducted denial of services attacks against Georgian websites.[10] In 2009-10, a computer worm called Stuxnet targeted Siemens computers located in Iran and also affected computers outside of Iran. According to the New York Times, Israel and the United States were behind the attacks. The alleged purpose of the operation was to damage Iran's main nuclear facilities.[11] In 2012, another malware called Flame infected computers in Iran and countries in the Middle East.[12]

Many cyber attacks are allegedly originating from China and North Korea. However, China has claimed that it was the target of extensive hacking by the United States. From the perspective of international law, potential cyber attacks from China, North Korea and the United States raise a number of interesting and complex questions: Does international law provide sufficient and adequate protection to target States of cyber attacks? Should the existing rules concerning *jus ad bellum* and *jus in bello*[13] be modified or changed?[14] When do cyber attacks amount to illegal uses of force under Article 2(4) of the UN Charter or even to the crime of aggression? What kinds of remedies do exist in case of proven cyber attacks? As the legal advisor of the US Department of State, Harold Koh points out that the right of self-defense

9 T. Marauhn, *The Debate about a Revolution in Military Affairs – A Comment in the Light of Public International Law*, 77 Die Friedens-Warte 411-435 (2002).

10 For details, *see* E. Tikk, et al., *Cyber Attacks against Georgia: Legal Lessons Identified*, CCDOE, Nov. 2008, *available at* http://www.carlisle.army.mil/DIME/documents/Georgia%201%200.pdf (last visited on Aug. 17, 2013).

11 Staff Writer, *Obama Ordered Sped Up Wave of Cyberattacks against Iran*, N.Y. Times, Jun. 1, 2012, *available at* http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=0 (last visited on Nov. 5, 2013).

12 Staff Writer, *Flame Virus Most Powerful Espionage Tool Ever, UN Warns*, The Telegraph, May 29, 2012, *available at* http://www.telegraph.co.uk/news/worldnews/middleeast/iran/9298488/Flame-virus-most-powerful-espionage-tool-ever-UN-warns.html (last visited on Nov. 4, 2013). *See also* D. Fidler, *Recent Developments and Revelations Concerning Cybersecurity and Cyberspace: Implications for International Law*, 16 ASIL Insight (2012), *available at* http://www.asil.org/insights/volume/16/issue/22/recent-developments-and-revelations-concerning-cybersecurity-and (last visited on Aug. 19, 2013).

13 While the *jus ad bellum* refers to those rules of international law governing the resort to the use of force, the *jus in bello* concerns those rules of international law governing the actual conduct of armed conflict. The latter rules can be found, *e.g*, in the Geneva Conventions of 1949 and their Additional Protocols of 1977.

14 For an excellent commentary on how the *jus ad bellum* and the *jus in bello* applies to the cyber context, *see* the Tallin Manual on the International Law Applicable to Cyber Warfare (hereinafter Tallin Manual), *available at* http://www.nowandfutures.com/large/Tallinn-Manual-on-the-International-Law-Applicable-to-Cyber-Warfare-Draft-.pdf (last visited on Jun. 21, 2013); *supra* note 6.

potentially applies against any illegal use of force including cyber attacks.[15] This leads to the question: When are cyber attacks regarded as armed attacks triggering the right to self-defense? The following paper attempts to provide some answers to these questions. However, questions related to *jus in bello* will not be addressed. The study will pursue these issues in the following way. First, an overview on cyber attacks and Northeast Asia will be provided. Second, the use of force and the right to self-defense in regard to cyber attacks will be addressed. Third, other available remedies outside the framework of Article 51 of the UN Charter will be discussed.

2. Cyber Attacks and Northeast Asia

Cyber attacks have also become a security concern in Northeast Asia. According to media reports, many of these attacks originate from China and North Korea. For one commentator, the People's Republic of China is perhaps the leading country in the use of cyber attacks 'short of war,' so-called patriotic hacking, e-spying and computer network attacks.[16] China has certainly the most extensive cyber-warfare capabilities in whole Northeast Asia. Many governments including Australia, Canada, Germany, India, South Korea and the United States have accused China of engaging in cyber operations against them.[17] Other well-known cyber attacks originating from China include Operation Ghostnet which penetrated, among others, the computer networks related to the Dalai Lama and Operation Aurora which targeted Google and dozens of other organizations.[18] The 2011 US Office of the National Counter Executive Report labeled "Chinese actors as the world's most active and persistent perpetrators of economic espionage."[19] However, it should

15 For details, *see* Harold Koh, *International Law in Cyberspace*, US Department of State, Sept. 18, 2012, *available at* http://www.state.gov/s/l/releases/remarks/197924.htm (last visited on Aug. 18, 2013).

16 C. Malis, *Unconventional Forms of War*, *in* The Oxford Handbook of War, 185 & 194 (J. French & Y. Boyer eds., 2012). *See also* D. Ball, *China's Cyber Warfare Capabilities*, 7 Security Challenges 81-103 (2011); J. Rogin, *The Top 10 Chinese Cyber Attacks (That We Know of)*, Foreign Pol'y, Jan. 22, 2010, *available at* http://thecable.foreignpolicy.com/posts/2010/01/22/the_top_10_chinese_cyber_attacks_that_we_know_of (last visited on Aug. 18, 2013).

17 Ball, *id*. For the relevant materials, *see Chinese Intelligence Activity Abroad*, *available at* http://en.wikipedia.org/wiki/Chinese_intelligence_activity_abroad (last visited on Aug. 17, 2013).

18 For more detailed list of cyber attacks related to China, *see* B. Krekel, *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation*, The US-China Economic and Security Review Commission Report 68-74(2009), *available at* http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB424/docs/Cyber-030.pdf (last visited on Jun. 21, 2013).

19 Office of the National Counterintelligence Executive, *Foreign Spies Stealing US Economic Secrets in Cyberspace,* Oct. 2011, *available at* http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf (last

be noted that in many cases no clear link to the Chinese government could be established. It rather appears that Chinese citizens had conducted cyber attacks.[20] In 2013, concerns over cyber security moved to forefront in the relations between China and the United States. In February 2013, the internet security firm Mandiant released a report, according to which the Chinese military Unit P.L.A. 61398 conducted cyber attacks against government institutions and defense contractors from the United States.[21] Because of the Mandiant report there is the growing fear that Unit 61398 did not only steal information but also obtained the ability to harm critical infrastructure inside the United States including power grids.[22] The Chinese Ministry of Foreign Affairs responded that these allegations were 'unprofessional' and that "China resolutely opposes hacking actions and has established relevant laws and regulations and taken strict law enforcement measures to defend against online hacking activities."[23] The United States claims the right to self-defense "against certain hostile acts conducted through cyberspace."[24] China has taken the position in diplomatic groupings that cyber attacks should not trigger the right to self-defense under the UN Charter but called for new international legal regulations in regard to cyber space.[25]

When President Obama met China's President Xi Jinping in 2013, he complained about ongoing cyber attacks against US government and corporate websites organized by the Chinese military.[26] In the past, China rejected all accusations and pointed out that it had been the world largest victim of cyber attacks and the victim of cyber warfare from the United States.[27] In 2010, China claimed it was hit by nearly 500,000 cyber attacks almost half originating from abroad, according to

visited on Jun. 21, 2013).

20 For details, *see* D. Creekman, *A Helpless America? An Examination of the Legal Options Available to the United States in Response to Varying Types of Cyber-Attacks from China*, 17 Am. U. L. Rev. 641-681 (2002).

21 *See* Mandiant Intelligence Center Report, APT 1: Exposing One of China's Espionage Units, *available at* http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf (last visited on Jun. 21, 2013).

22 *Id*.

23 *See Chinese Army Unit Is Seen as Tied to Hacking against U.S.*, N.Y. Times, Feb. 18, 2013, *available at* http://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html (last visited on Nov. 5, 2013).

24 The White House, International Strategy for Cyberspace, 2011, at 14, *available at* http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (last visited on Jun. 21, 2013).

25 M. Waxman, *Self-defensive Force against Cyber Attacks: Legal, Strategic and Political Dimensions*, 89 Int'l L. Stud. 109-122 (2013).

26 *See Barack Obama and Xi Jinping Meet as Cyber-Scandals Swirl*, The Guardian, Jun. 8, 2013, *available at* www.theguardian.com/world/2013/jun/08/obama-xi-jinping-meet-cyberscandals (last visited on Nov. 4, 2013).

27 *See China is the Biggest Victim of Spyware Most Attacks Origin from U.S.*, Xinhua News, Apr. 10, 2009.

the country's computer security agency.[28] In June 2013, the former NSA employee, Edward Snowden confessed that US intelligence had hacked hundreds of computers in China, including the Tsinghua University in Beijing.[29] Because of Snowden's revelations China's official Xinhua news agency labeled the US as the "biggest villain in our age."[30]

Japan is also growingly concerned about cyber attacks. In 2012, the Japanese foreign minister Koichiro Genba claimed that Japan would have the right to self-defense against cyber attacks.[31] According to media reports, Japanese government institutions and defense contractors including Mitsubishi Heavy Industries Ltd., IHI Corp and Kawasaki Heavy Industries were hit by cyber attacks. In response to the threat from cyber space, Japan plans to establish a cyber defense unit whose task will be to monitor the computer networks of the Japanese self-defense forces.[32]

There have also been a number of reported cyber attacks against institutions in South Korea which appears to be particularly vulnerable because approximately 40 million people are using the internet there. South Korea leads in the number of DSL connections worldwide. In March 2011, distributed denial-of-services ("DDoS") attacks targeted South Korean government websites and the network of US Forces Korea ("USFK"). A report published by the computer security company McAfee arrived at the conclusion that "this may have been a test of South Korea's preparedness to mitigate cyber attacks, possibly by North Korea or their sympathizers."[33] In April 2011, the computer network of the Nonghyup Bank collapsed due to a cyber attack. South Korean prosecutors concluded that the attacks originated from North Korea.[34] Other reported cases include attempts to

28 Staff Writer, *China Victim of 500,000 Cyber-Attacks in 2010, Says Security Agency*, Associated Press, Aug. 9, 2011. *available at* www.theguardian.com/world/2011/aug/09/china-cyber-attacks (last visited on Nov. 5, 2013).

29 Staff Writer, *Snowden Says U.S. Hacking Targets China; NSA Points to Thwarted Attacks*, The Japan Times, Jun. 14, 2013, *available at* http://www.japantimes.co.jp/news/2013/06/14/world/u-s-hacking-effort-targets-china-snowden/#.Uni9mHA71Vg. *See also* Lama Lam, *NSA Targeted China's Tsinghua University in Extensive Hacking Attacks, Says Snowden,* South China Morning Post, Jun. 22, 2013, *available at* http://www.scmp.com/news/china/article/1266892/exclusive-nsa-targeted-chinas-tsinghua-university-extensive-hacking?page=all (all last visited on Nov. 5, 2013).

30 *See China's Xinhua News Agency Condemns "US Cyber–Attacks'*; BBC News, Jun. 23, 2013, *available at* http://www.bbc.co.uk/news/world-asia-23018938 (last visited on Nov. 5, 2013).

31 A. Westlake, *Japanese Government Claims its Right to Self-defense against Cyber-attacks*, Japan Daily Press, May 17, 2012, *available at* http://japandailypress.com/japanese-government-claims-its-right-to-self-defense-against-cyber-attacks-172322 (last visited on Nov. 5, 2013).

32 *See Bolster Cyber Attack Defenses*, Japan Times, Apr. 1, 2012, *available at* http://www.japantimes.co.jp/opinion/2013/04/01/editorials/bolster-cyber-attack-defenses/#.Uni-pnA71Vg (last visited on Nov. 5, 2013).

33 *See Ten Days of Rain: Expert Analysis of Distributed Denial-of-Service Attacks Targeting South Korea*, McAfee White Paper, Jul. 2011, *available at* http://blogs.mcafee.com/wp-content/uploads/2011/07/McAfee-Labs-10-Days-of-Rain-July-2011.pdf (last visited on Mar. 8, 2013).

34 *See* Yonhap News Agency, *Practical Threat of Cyber Attacks from North Korea*, *in* Korea Focus, May 3, 2011, *available*

hack the website of the G20 preparatory summit committee and personal computers of members of the National Assembly. In April and May 2012, Incheon airport became a target when computer viruses had been planted into game programs.[35] In June 2012, one of South Korea's leading newspapers, the Joongang Ilbo Daily was hit by a major cyber attack.[36] During summer 2012, North Korea allegedly jammed GPS signals in South Korea.[37] In March 2013, three South Korean banks and two broadcasters were hit by cyber attacks.[38] There is a strong assumption that North Korea should be blamed for these incidents,[39] but some commentators are more cautious, pointing out there is no conclusive evidence and a lack of reliable information.[40]

North Korea has shown interest in cyber warfare for long time. Some experts argue that North Korea even belongs to the leading cyber powers in the world.[41] None of the above-mentioned incidents led to the loss of life or physical destruction of property. However, there is growing concern that North Korea's cyber attack capabilities pose a real threat to the security interests of the United States and South Korea. Another expert warned that major infrastructures in South Korea could be compromised in only five minutes if North Korea launched a full-blown cyber attack.[42] In March 2012, the commander of USFK, General James Thurman explained

at http://www.koreafocus.or.kr/design2/layout/content_print.asp?group_id=103542 (last visited on Nov. 5, 2013).

35 Chul-jae Lee & Gwang-lip Moon, *Incheon Airport Cyberattack Traced to Pyongyang*, JOONGANG DAILY NEWS, Jun. 5, 2012, *available at* http://koreajoongangdaily.joins.com/news/article/article.aspx?aid=2953940 (last visited on Nov. 5, 2013).

36 *See South Korean Paper Hit by Major Cyber Attack*, SIDNEY MORNING HERALD, Jun. 12, 2012.

37 S. Waterman, *North Korean Jamming of GPS Shows System's Weakness*, WASHINGTON TIMES, Aug. 23, 2012, *available at* http://www.washingtontimes.com/news/2012/aug/23/north-korean-jamming-gps-shows-systems-weakness/?page=all (last visited on Nov. 5, 2013).

38 Sang-hun Choe, *Computer Networks in South Korea Are Paralyzed in Cyberattacks*, N.Y. TIMES, Mar. 20, 2013, *available at* http://www.nytimes.com/2013/03/21/world/asia/south-korea-computer-network-crashes.html (last visited on Nov. 5, 2013).

39 J. Lewis, *The "Korean" Cyber Attacks and Their Implications for Cyber Conflict*, Center for Strategic & International Studies, Oct. 2009, *available at* http://csis.org/files/publication/091023_Korean_Cyber_Attacks_and_Their_Implications_for_Cyber_Conflict.pdf (last visited on June 21, 2013). *See also* J. Lewis, *Speak Loudly and Carry a Small Stick: The North Korean Cyber Menace*, 38 NORTH, Sept. 7, 2010, *available at* http://38north.org/2010/09/speak-loudly-and-carry-a-small-stick-the-north-korean-cyber-menace (last visited on Nov. 5, 2013). *See also* L. Petrov, *Cyber Attacks May Spark New War in Korea*, 38 NORTH, Jul. 9, 2012, *available at* http://38north.org/2012/07/lpetrov070912/ (all last visited on Aug. 19, 2013).

40 *See, e.g.*, J. McGee, The Difficulties of Assessing North Korea's Cyber Strategy, Center for Strategic and International Studies, *available at* http://csis.org/blog/difficulties-assessing-north-koreas-cyber-strategy (last visited on Jun. 21, 2013).

41 J. Arquilla, *Cyber Fail*, FOREIGN POL'Y, Sept. 5, 2012, *available at* http://www.foreignpolicy.com/articles/2012/09/05/cyber_fail (last visited on Aug. 20, 2013).

42 Jong-in Lim, *Cyber Attack from DPRK may Bring down Traffic, Electricity and Stock Markets in Five Minutes* (임종인 고려대 정보보호대학원장 경고 "北 사이버 공격 5분이면 교통 전력 증시 다 무너져" (available only in Korean), DONG-A

at a Congressional hearing that:

> North Korea employs sophisticated computer hackers trained to launch cyber-infiltration and cyber-attacks against the ROK and U.S. Such attacks are ideal for North Korea, providing the regime a means to attack ROK and U.S. interests without attribution, and have been increasingly employed against a variety of targets including military, governmental, educational, and commercial institutions.[43]

North Korea has also experienced cyber attacks. On the anniversary day of the Korean War in 2013, major websites in North and South Korea went down. The hackers infiltrated, among others, the state run North Korean websites Rodong Sinmun, the Korean Central News Agency and Air Koryo (Korea). North Korea blamed the US and South Korea of backing the international hacking collective Anonymous which had already attacked the North Korea in spring 2013 by launching "Operation Free Korea."[44] However, it should be noted that Anonymous denied any responsibility for the cyber attacks on the anniversary of the Korean War.

3. Cyber Attacks and Article 2(4) of the UN Charter

The first question to be addressed is whether cyber attacks are a violation of Article 2(4) of the UN Charter which provides that:

> All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any manner inconsistent with the Purposes of the United Nations.

Ilbo, May 7, 2012, *available at* http://news.donga.com/NEWS/3/all/20120506/46047415/1# (last visited on Jun. 21, 2013).

43 *See* General Thurman's statement, *available at* http://www.usfk.mil/usfk//Uploads/110/Statement.pdf (last visited on Aug. 19, 2013). For a critical evaluation of South Korea's response to cyber-security, *see* Lee & Lee, *supra* note 2, at. 85-106; Sang-ho Song, *Army, University to Create Cyber Defense Course*, Korea Herald, Jun. 28, 2011, *available at* http://www.koreaherald.com/view.php?ud=20110628000706 (all last visited on Nov. 5, 2013).

44 A. Abad-Santos, *Anonymous Wants to Ruin North Korean War Anniversary*, The Atlantic Wire, Jun. 25, 2013, *available at* http://www.theatlanticwire.com/global/2013/06/anonymous-north-koreas-korean-war-anniversary/66561/ (last visited on Nov. 5, 2013); Staff Writer, *Anonymous Hacks North Korea Social Network Accounts*, BBC, Apr. 4, 2013, *available at* http://www.bbc.co.uk/news/technology-22025724 (last visited on Nov. 5. 2013).

The ban on the use of force in Article 2(4) covers wars, forcible measures short of war, illegal threats of force[45] and the narrower concept on the prohibition of aggression. The Charter allows the use of force in case of enforcement measures under Chapter VII and reserves the right of individual or collective self-defense under Article 51.[46] In addition, force may also be used under certain circumstances by foreign military forces on the territory of another State if the host State gives the consent to the military operation. The vast majority of international lawyers consider Article 2(4) to be a principle of customary international law and agree that this provision constitutes a pre-emptory norm of international law (*jus cogens*).[47]

There is no generally accepted definition of the use of force in cyberspace. As the Tallin Manual points out, "State practice is only beginning to clarify the application to cyber operations of the *jus ad bellum*."[48] Even in case of Stuxnet, Iran refrained from declaring the cyber operation an armed attack according to Article 51 of the Charter.[49] One may therefore wonder which types of cyber attacks may amount to the use of force according to Article 2(4) of the Charter. It is uncontroversial that force refers to armed force in the sense of Article 2(4). Obviously, the founding fathers of the UN did not have cyber attacks in mind when they adopted the UN Charter. Article 31 of the Vienna Convention on the Law of Treaties of 1969 ("VCLT") provides that terms within a treaty such as the UN Charter shall be interpreted in accordance with the ordinary meaning and in light of the treaty object and purpose. Taking into account the ordinary meaning of the word 'force,' one could arrive at the conclusion that Article 2(4) covers all types of force since the qualification 'armed' has been omitted. This is different from the preamble, Articles 41 and 46 of the UN Charter where the adjective 'armed' was added. The drafting history of the UN also shows that proposals to include moral and physical force (Ecuador), the threat and the use of economic measures (Brazil), and indirect and direct political force in

45 On the threat of cyber operations, *see* Tallinn Manual Rule 12.

46 The third exception laid down in Articles 53(1) and 107 of the UN Charter provides for measures against former enemy States. The so-called 'enemy clause' became obsolete; when Italy in 1955, Japan in 1956 and Germany in 1973 were admitted as "peace loving nations" to the UN. *See* U.N. Charter art. 4

47 *Jus cogens* can be defined as a norm "accepted and recognized by the international community of states as a whole as a norm from which no derogation is permitted and which can be modified only by a subsequent norm of general international law having the same character." *See* VCLT art. 53. For details, *see* L. Hannikainen, Peremptory Norms (Jus Cogens) in International Law (1988); A. Orakhelashvili, Peremptory Norms in International Law (2009).

48 Tallinn Manual, at 42.

49 G. Brown, *Why Iran Didn't Admit Stuxnet Was an Attack*, 63 Joint Force Q. 70-73 (2011). For a legal analysis, *see* A. Foltz, *Stuxnet, Schmitt Analysis, and the Cyber Use of Force Debate*, 67 Joint Force Q. 40-48 (2012); D. Hollis, *Could Deploying Stuxnet be a War Crime?*, Opinio Juris, *available at* http://opiniojuris.org/2011/01/25/could-deploying-stuxnet-be-a-war-crime/ (last visited on Jun. 21, 2013); K. Ziolkwoski, *Stuxnet – Legal Considerations*, 25 Humanitäres Völkerrecht Informationsschriften 139-147 (2012).

Article 2(4) had been rejected.[50] As the International Court of Justice ("ICJ") clarified, Article 2(4) applies to "any use of force, regardless of the weapons deployed."[51] Therefore, in addition to kinetic, chemical, biological or nuclear weaponry, cyber operations may fall under Article 2(4) of the Charter.

Legal scholars have developed different and competing analytical frameworks determining whether cyber operations amount to "use of force" in accordance with Article 2(4) of the Charter.[52] An instrument-based approach analyses whether cyber operations have the traditional characteristics associated with armed force and whether critical infrastructure has been hit.[53] A strict liability approach considers any cyber operation targeted against critical infrastructure of a State as a use of force.[54] For Sharp, any State activity in cyberspace that intentionally causes destructive effect within the sovereign territory of another State would be an unlawful use of force.[55] The majority of international lawyers look at the consequences of cyber operations (the so-called consequence-based or effect-based approach). If the indirect or direct effects of cyber-attacks are similar to those of kinetic, biological or chemical weapons, meaning they cause death, physical injury or destruction of property, then such cyber-attacks would fall under the Article 2(4) prohibition.[56] According to the Tallinn Manual, "a cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of force.[57] Examples frequently mentioned in the legal literature include cyber operations causing airplanes to crash, leading to the meltdown in a nuclear plant or the collapse of an air traffic system. Cyber attacks which produce no death, physical injury or destruction of property as in case of the Nonghyup Bank, Incheon Airport or the Joogang Ilbo Daily cannot be regarded as a violation of Article 2(4) of the UN Charter. In case of the alleged cyber attacks from China and the United States, all

50 *See* UN General Assembly's Declaration on Principles of International Law Concerning Friendly Relations of 1971 which confirms the understanding that neither economic nor political pressure amount to force, G.A. Res 2625 (XXV), U.N. GAOR, 25th Sess., Supp. No. 28, U.N. Doc. A/5217 (Oct. 24, 1970), *available at* http://www1.umn.edu/humanrts/instree/principles1970.html (last visited on Nov. 5, 2013).

51 Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996, I.C.J. ¶39 (Jul. 8).

52 For a short summary of scholastic writings, *see* Dinniss, *supra* note 6, at 58-74.

53 D. Graham, *Cyber Threats and the Law of War*, 4 J. Nat'l Security L. & Pol'y 87-102, at 91 (2010).

54 *Id.*

55 Sharp, *supra* note 8, at 102.

56 One of the leading legal scholars on cyber warfare, Michael N. Schmitt developed a number of criteria (severity; immediacy; directness; invasiveness; measurability; presumptive legitimacy; and responsibility) which may help States to assessing whether cyber operation amount to illegal use of force. Whether States will follow his policy-oriented approach in state practice remains to be seen. For details, *see* M. Schmitt, *Cyber Operations and the Jus ad Bellum Revisited*, 56 Vill. L. Rev. 569-605 (2011).

57 Tallinn Manual Rule 11.

are arguably related to sabotage, theft of data or cyber espionage;[58] they may not be illegal uses of force.[59] However, they may violate the principle of non-intervention,[60] the principle of territorial integrity, and the obligation under international law of a state "not to allow knowingly its territory to be used for acts contrary to the rights of other states."[61]

4. Cyber Attacks and Article 51 of the UN Charter

Article 51 of the UN Charter provides that:

> Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures to maintain international peace and security.

The UN Charter, however, does not provide for a definition on armed attack.[62] According to ICJ, not every use of force is to be regarded as an armed attack, but only uses of force which are of a particular scale and effect.[63] Mere border incidents are outside the scope of Article 51.[64] Therefore, only cyber operations would be armed attacks which cause physical damage to property or persons of a sufficient scale and effect. It is unclear whether the intention of the attacker is relevant in characterizing a cyber operation as armed attack pursuant to Article 51 of the UN Charter. In the *Oil Platforms* case, ICJ examined whether Iran carried out attacks against US targets

58 For a legal opinion that cyber espionage should be treated as potential armed attacks, *see* A. Melnitzky, *Defending America against Chinese Cyber Espionage through the Use of Active Defenses*, 20 Cardozo J. Int'l & Comp. L. 537-570 (2012).

59 For an overview of legal responses under US and Chinese domestic law, *see* Creekman, *supra* note 20.

60 Arguably, there is a thin line between an illegal intervention and perfectly legitimate political pressure on another State. For details, *see* R. Buchan, *Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?*, 17 J. Conflict & Security L. 211-217 (2012); J.-C. Woltag, *Computer Network Operations Below the Level of Armed Force*, ESIL Conference Paper, No. 1, 2011, *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1967593 (last visited on Aug. 19, 2013).

61 Corfu Channel (U.K. *v.* Alb.), Judgment, 1949 I.C.J. 4 & 22 (Apr. 9).

62 U.N. Charter arts. 39, 51 & 53.

63 Military and Paramilitary Activities in and against Nicaragua (Nicar. *v.* U.S.), Judgment, 1984 I.C.J. 437, ¶¶ 191 & 195. (Nov. 26).

64 *Id.* For the division of legal doctrine, *see* E. Wilmshurst, *Principles of International Law on the Use of Force by States in Self-Defence*, Chatham House Papers, Oct. 2005, at 15, *available at* http://www.chathamhouse.org/publications/papers/view/108106 (last visited on Apr. 19, 2013).

with the specific intention of causing harm.[65] The ICJ's approach appears to exclude the right to self-defense in cases when cyber operations accidentally cause significant harm to persons and property. The International Group of Experts in the Tallin Manual rejected the view that the intention of the attacker plays a decisive role when qualifying an operation as an armed attack since any response of the victim State would have to comply with principles of necessity and proportionality.[66]

In the case of North Korean or Chinese cyber attacks which are below the threshold of an armed attack under Article 51 of the UN Charter but still considered as force according to Article 2(4) of the UN Charter, South Korea or the United States may consider invoking the "accumulation of events" theory. Based on the "accumulation of events" theory, sometimes called the "pin-prick theory," or in German, 'Nadelstichtaktik,'[67] a State that is a victim of minor attacks over a period of time can still act in self-defense by taking into account the whole series of attacks. Proponents of the accumulation of events theory are Israel and the United States. Last century, South Africa and the United Kingdom also claimed self-defense based on the "accumulation of events" theory.[68] In recent years, there appears to be growing support among academics and practitioners including the International Group of Experts who addressed cyber warfare from the perspective of international law in the Tallinn Manual.[69] However, the "accumulation of events" theory has not yet received wide support by states or the Security Council.[70] It has not been applied by South Korea or any other States in Northeast Asia, either.

Another issue concerns the question when a cyber armed attack has occurred and whether States could act in self-defense against the threat of cyber armed attacks. Considering the wording of Article 51 of the UN Charter, the right to self-defense requires the existence of an armed attack. There is a strong argument that the drafters of the UN Charter have been aware of threats,[71] but intentionally left out the possibility to act in self-defense in cases of threats. Most scholars make reference to the *Caroline* formula of 1837, according to which there must be a "necessity of self-defense, instant, overwhelming, leaving no choice, of means, and no moment

65 Oil Platforms (Iran *v.* U.S.), Judgment, 2003 I.C.J. 191, ¶ 64 (Nov. 6).

66 Tallinn Manual Rule 13, commentary 11.

67 Y. Blum, *State Response to Acts of Terrorism*, 19 German Y.B. Int'l L. 235-237 (1976).

68 For a short summary of State practice, *see* K. Szabó, Anticipatory Action in Self-Defence 206-215 (2011).

69 Tallinn Manual Rule 13.

70 *See, e.g.*, the Security Council's response to Israel's armed intervention against the PLO in Lebanon, S.C. Res. 509, 515, 517, 520 & 521 (1981).

71 U.N. Charter arts. 2(4) & 39.

for deliberation."[72] Even more controversial is the right to pre-emptive self-defense referring to military action which may occur somewhere in the future.[73] The concept was asserted in the so-called 'Bush doctrine.'[74] The doctrine itself is not new. Myres McDougal argued that a State cannot be expected to be in a position of a sitting duck waiting for a fatal blow.[75] This appears to even more true in the age of global terrorism and weapons of mass destruction. During the last twenty years, pre-emptive strikes have also been proposed by policymakers and military leaders in Japan, South Korea and the United States in regard to North Korea's nuclear weapon program.[76] However, to allow States to attack each other simply based on the assumption that they regard each other as a threat will automatically lead to the escalation of violence.

Last but not least, there remains the issue of abuse and vagueness.[77] The UN Secretary General's High Level Panel on United Nations Reform and the subsequent report by Kofi Annan rejected the concept of pre-emptive self-defense.[78] In a similar way, the World Summit Outcome Document also reaffirmed that "the relevant provisions of the Charter are sufficient to address the full range of threats to international peace and security."[79] Therefore, Northeast Asian States would have no legal right to act in self-defense against mere threats of cyber armed attacks. However, the International Group of Experts in the Tallinn Manual convincingly argue that a State may act in self-defense "when the attacker is clearly committed to

72 C. Greenwood, *The Caroline*, MAX PLANCK ENCYCLOPEDIA OF PUBLIC INTERNATIONAL LAW VOL.1, 1142-1143 (2012).

73 The terms anticipatory and pre-emptive self-defence have been used interchangeably by legal scholars. This articles uses the terms in the following way: 'Anticipatory self-defence' refers to action taken in response to an imminent armed attack. 'Pre-emptive self-defence' refers to action taken in response to a perceived but remote threat. *See* B. SIMMA ET AL. (EDS.) THE CHARTER OF THE UNITED NATIONS: A COMMENTARY VOL. 1, 803-804 (2002).

74 The White House, The National Security Strategy of the United States of America (2002), at 15, *available at* http://www.state.gov/documents/organization/63562.pdf (last visited on Nov. 5, 2013). The Obama administration has neither explicitly endorsed nor rejected the Bush doctrine.

75 M. McDougal, *The Soviet Cuban Quarantine and Self-defence*, 57 AM. J. INT'L L. 601 (1963).

76 *See, e.g.*, D. Pinkston & Kazutuka Sakurai, *Japan Debates Preparing for Future Preemptive Strikes against North Korea*, 18 KOREAN J. DEF. ANALYSIS 95-121 (2006); K. Malone, *Preemptive Strikes and the Korean Nuclear Crisis, Legal and Political Limitations on the Use of Force,* 12 PAC. RIM. L. & POL'Y J. 807-834 (2003); *Military Commander Hints at 'Pre-emptive Strike' on N. Korea*, KOREA HERALD, Feb. 6, 2013, *available at* http://www.koreaherald.com/view.php?ud=20130206001071 (last visited on Nov. 5, 2013).

77 M. Bothe, *Terrorism and the Legality of Pre-emptive Force*, 14 EUR. J. INT' L L. 237 (2003).

78 *See* A More Secure World: Our Shared Responsibility, Report of the High-Level Panel on Threats, Challenges and Change, U.N. Doc. A/59/565 (Nov. 17, 2004), ¶¶ 183-209, *available at* http://www.unrol.org/doc.aspx?n=gaA.59.565_En.pdf; In Larger Freedom. Towards Security, Development and Human Rights for All, Report of the SG, U.N. Doc. A/59/2005 (Mar. 21, 2005) ¶¶ 122-126, *available at* http://www.unrol.org/doc.aspx?d=2139 (all last visited on Nov. 5, 2013). *See also* Armed Activities on the Territory of the Congo (Congo *v.* Uganda), Judgment, 1999 I.C.J . 123, ¶ 148 (Jun. 23).

79 *See* 2005 World Summit Outcome Document, G.A. Res. 60/1. U.N. Doc. A/RES/60/1 (Oct. 24, 2005), *available at* http://www.unrol.org/doc.aspx?n=2005+World+Summit+Outcome.pdf (last visited on Nov. 5, 2013).

launching an armed attack and the victim State will lose its opportunity to effectively defend itself unless it acts."[80] Should any State in Northeast Asia act in self-defense against cyber armed attacks, the response would have to comply with the *jus ad bellum* principles of proportionality, necessity and immediacy.[81] International law does not provide for a clear cut definition of 'proportionality.' As Terry Gill points out "the measures taken must be roughly comparable in scale and effects to that of the armed attack and the overall threat of the attack posed by the attacking State or entity."[82] 'Necessity' requires that "there must be no practical alternative to the proposed use of force that is likely to be effective in ending or averting the attack."[83] Furthermore, the South Korean government would have to comply with the standard of immediacy. 'Immediacy' requires that "the action taken in self-defense must be taken within a reasonable timeframe in relation to the occurrence of the attack."[84]

International law does not require the victim of an armed cyber attack to respond in the same manner by using cyber action. It permits the victim State to react by using kinetic force, as well. The right of collective self-defense under Article 51 of the UN Charter could be invoked against cyber attacks.

When Non-State Actors ("NSAs") are conducting a cyber armed attack,[85] this would be considered an armed attack under Article 51 of the UN Charter if a State exercises some sort of control over the armed group.[86] However, the standard of control is disputed. While ICJ in the *Nicaragua* case required that there must be 'substantial involvement' on part of a State,[87] the International Criminal Tribunal for the Former Yugoslavia adopted the 'overall control' test.[88] It remains controversial whether States can also act in self-defense against NSAs absent of any direction by another State.[89] In case of North Korea, the scenario appears to be unlikely that

80 Tallinn Manual, Rule 15, commentary 4.

81 Military and Paramilitary Activities in and against Nicaragua (Nicar. *v.* U.S.), Judgment, 1984 I.C.J. 94, ¶ 176. (Nov. 26); Oil Platforms (Iran *v.* U.S.), Judgment, 2003 I.C.J. 196-198 (Nov. 6).

82 T. Gill, *Legal Basis of the Right of Self-Defence under the UN Charter and under Customary International Law*, *in* The Handbook of the International Law of Military Operations 196 (T. Gill & D. Fleck eds. 2011).

83 E. Wilmshurst, *Principles of International Law on the Use of Force by States in Self-Defence*, Chatham House Papers, Oct. 2005, at 7-8, *available at* http://www.chathamhouse.org/publications/papers/view/108106 (last visited on Aug. 19, 2013).

84 *Supra* note 82, 197.

85 Tallinn Manual Rule 16.

86 *Id.* Rule 13, commentary 13.

87 Military and Paramilitary Activities in and against Nicaragua (Nicar. *v.* U.S.), Judgment, 1984 I.C.J. ¶ 109. (Nov. 26).

88 Prosecutor v. Tadic, Appeals Chamber Judgment, Case No. IT-94-1-A 115 (July 15, 1999).

89 For an analysis of the so-called "unable and unwilling test," *see* A. Deeks, *'Unwilling or Unable': Toward an Normative*

hackers could attack South Korea independently from any involvement of the North Korean regime, since the North Korean apparatus controls almost every aspect of life there.

The burden of proof concerning the existence of an armed attack would lie on the victim of that armed attack.[90] While there is no consensus among international lawyers on the exact "standard of proof," it is generally agreed that the standard should be high in cases concerning self-defense.[91] In the *Oil Platforms* case, ICJ rejected circumstantial evidence.[92] Mary O'Connell argues that the standard of proof should be "clear and convincing."[93] In case of doubt, State cannot act in self-defense. Cyber attacks raise significant identification and attribution problems.[94] As pointed out by Marco Roscini, "anonymity is in fact one of the greatest advantages of cyber warfare; even though the attacks might appear from computers located in a certain country, this does not necessarily mean that that country or even the owners were behind the action."[95] It would also be possible for hackers acting on behalf of North Korea to conduct cyber operations from Seoul or Daejeon. In some cases, there may even be doubts whether a State has been attacked or whether a problem has been caused by technical failure.

5. Resort to the UN Security Council

In case of continued cyber attacks, Northeast Asian States may refer the situation to the Security Council under Article 35(1) of the UN Charter. In accordance with Articles 24(1) of the UN Charter, the Council takes 'primary' responsibility for the

Framework for Extra-Territorial Self-Defense, 52 Va. J. Int'l L. 483-540 (2012). For the response *see* K. Heller, *Ashley Deeks' Problematic Defense of the "Unwilling or Unable" Test*, Opinio Juris, *available at* http://opiniojuris.org/2011/12/15/ashley-deeks-failure-to-defend-the-unwilling-or-unable-test (last visited on Jun. 22, 2013).

90 Military and Paramilitary Activities in and against Nicaragua (Nicar. *v.* U.S.), Judgment, 1984 I.C.J. 437, ¶ 101. (Nov. 26).

91 For details, *see* R. Wolfrum, *International Courts and Tribunals, Evidence*, Max Planck Encyclopedia of Public International Law vol. 5, 566 (2012).

92 *See* Oil Platforms (Iran *v.* U.S.), Judgment, 2003 I.C.J. 188-190 (Nov. 6).

93 M. O'Connell, *Evidence of Terror*, 7 J. Conflict & Security L. 22-28 (2002)

94 N. Tsagourias, *Cyber Attacks, Self-Defence and the Problem of Attribution*, 17 J. Conflict & Security L. 229-244 (2012). *See also* S. Gaycken, *The Necessity of Some Certainty – A Critical Remark Concerning Matthew Sklerov's Concept of Active Defense*, 12 J. Military & Strategic Stud. 2 (2010); H. Lipson, Tracking and Tracing Cyber – Attacks: Technical Challenges and Policy Issues, (CERT CMU/SEI-2002-SR-009, Nov. 2002). *See also* Tallinn Manual Rules 7 & 8.

95 Roscini, *supra* note 7, at 96.

maintenance of international peace and security. Under Chapter VII of the UN Charter, moreover, the Security Council may take enforcement measures to maintain or restore international peace and security. Decisions under Chapter VII will bind all member States.[96] Since the end of the Cold War, the Security Council has been mainly concerned with threats to global and regional peace and stability which originate within States.

To date, the Security Council has passed no resolution in regard to cyber operations. However, there is no legal or political reason why it could not address cyber operations as a threat to the peace pursuant to Chapter VII. While the Security Council deals mostly with specific incidents or conflicts, it may also address significant phenomena, amounting to a threat to peace.[97] The Security Council generally enjoys a wide margin of discretion about when to act and how to act.[98] Before adopting enforcement measures[99] or provisional measures[100] under Chapter VII against a cyber attacker, two preconditions have to be fulfilled. On the one hand, the Council must have determined the existence of a threat to the peace, breach of the peace, or act of aggression. On the other hand, the measures to be taken should serve "to maintain or restore international peace or security." Currently, the Security Council would not be able to adopt any measures because China, Russia and the United States are deeply divided about how to address cyber security. During the June 2013 summit with China, US President Obama attempted unsuccessfully to address cyber related problems between the two countries. Since China and the United States could not resolve their issues regarding cyber espionage and cyber theft on a bilateral level, it is difficult to see that they would find a consensus on cyber security in the Security Council.

6. Cyber Warfare and the International Tribunals

A. ICC

Although there is no international court or criminal tribunal specifically dealing

96 U.N. Charter, art. 25.

97 S.C. Res. 1373, U.N. Doc. S/RES/1373 (Sept. 28, 2001); S.C. Res. 1540, U.N. Doc. S/RES/1540 (Apr. 28, 2004).

98 The Charter does not explicitly define the limits of the SC to act under Chapter VII. This lead to an intensive academic debate. *See* E. De Wet, The Chapter Vii Powers of the United Nations Security Council 133 (2004).

99 U.N. Charter arts. 40 & 41.

100 *Id*.

with the most serious cyber crimes,[101] the International Criminal Court ("ICC") could have jurisdiction over cases related to cyber attacks. The ICC has jurisdiction over genocide, crimes against humanity, war crimes and the crime of aggression under the Rome Statute of the International Criminal Court (hereinafter Rome Statute).[102] As of June 2013, 122 States including Japan and South Korea have ratified or acceded to the Rome Statute, while China, North Korea and the United States are not parties to it.

Since South Korea is a State party to the Rome Statute, ICC may have jurisdiction over cyber operations amounting to a crime under the Statute. Pursuant to Article 12(2) of the Rome Statute, the Court may prosecute crimes committed on the territory of a State party, even though the perpetrator is not a national of a State party. After years of discussions, the State parties agreed at Kampala in 2010[103] in defining the "crime of aggression" as "the planning, preparation, initiation or execution, by a person in a position effectively to control over to direct the political or military action of a State, of an act of aggression which by its character, gravity and scale, constitutes a manifest violation of the Charter of the United Nations."[104] According to Article 8 *bis* of the Rome statute, any of the acts set forth in United Nations General Assembly Resolution 3314 (XXIX)[105] would be qualified as 'aggression.' However, it remains unclear which violations of Article 2(4) of the UN Charter are so manifest that they would fall under the jurisdiction of ICC. International lawyers would agree that preventive self-defense and humanitarian interventions without the Security Council's authorization lack a legal basis in customary international law.[106] However, since humanitarian interventions are sometimes considered as morally justified, this raises the question whether they should be also considered as aggression.[107] Another controversial issue concerns the mechanisms to trigger cases concerning the crime

101 For a proposal, *see* S. Schjolberg, *Peace and Justice in Cyberspace: An International Criminal Court or Tribunal for Cyberspace*, a paper presented for the 13th International Criminal Law Congress, Sept. 16, 2012, *available at* http://www.crimlaw2012.com/papers/0011.pdf (last visited on Jun. 21, 2013).

102 2187 U.N.T.S. 90. *See* Rome Statute arts. 5, 6, 7 & 8.

103 *Id.* art. 8 *bis*, *available at* http://www.icc-cpi.int/iccdocs/asp_docs/Resolutions/RC-Res.6-ENG.pdf (last visited on Aug. 21, 2013).

104 ICC, *Review Conference of the Rome Statute*, Conference Room Paper on the Crime of Aggression, RC/WGCA/1, May 25, 2010, *available at* http://www.icc-cpi.int/iccdocs/asp_docs/RC2010/RC-WGCA-1-ENG.pdf (last visited on Jun. 21, 2013).

105 G.A. Res. 3314 (XXIX), U.N. Doc. A/RES/3314 (Dec. 14, 1974), *available at* http://www1.umn.edu/humanrts/instree/GAres3314.html (last visited on Nov. 5, 2013).

106 For details, *see supra* note 73.

107 For details, *see* E. Leclerc-Gagné & M. Byers, *A Question of Intent: The Crime of Aggression and Unilateral Humanitarian Intervention*, 41 Case W. Res. J. Int'l L. 379-390 (2009); S. Murphy, *Criminalizing Humanitarian Intervention*, 41 Case W. Res. J. Int'l L. 341-377 (2009).

of aggression.[108] The implementation of jurisdiction over the crime of aggression is therefore delayed until January 1, 2017.

It should be emphasized that aggression is a so-called leadership crime. The perpetrator must have exercised effective control or leadership over the State's illegal use of force.[109] This seems to exclude ordinary hackers acting on instructions of a State. ICC also has jurisdiction over war crimes. In case that cyber operations would, *e.g.*, be intentionally directed against civilians (not taking part in hostilities) or civilian objects in another country, they may be regarded as a war crime under the Rome Statute.[110].

B. ICJ

Northeast Asian States may also bring case against a State being responsible for cyber-attacks before ICJ and ask for reparation which can take the form of restitution, compensation or satisfaction because of the violation of Article 2(4) of the UN Charter or the principle of non-intervention. As the principal judicial organ of the United Nations,[111] the Court may decide legal disputes between States.[112] ICJ has addressed issues in regard to the use of force in the two different contexts: first, when States requested provisional measures to prevent alleged acts of aggression;[113] and second, when legal disputes arose in respect to the alleged unlawful use of force or act of aggression committed by a State, which was subject of a case referred to ICJ.[114] Although all members of the United Nations are *ipso facto* parties to the Statute of the Court, ICJ may only decide a dispute between States if jurisdiction has been conferred on it by the two countries.

108 Rome Statute art. 15 *bis*.

109 R. Cryer et al, An Introduction to International Criminal Law and Procedure 271-272 (2007).

110 Rome Statute art. 8(2) (b) (i)-(ii).

111 U.N. Charter art. 92.

112 I.C.J. Statute art. 36.

113 Military and Paramilitary Activities in and against Nicaragua (Nicar. v. U.S.), Provisional Measures, 1984 I.C.J. (May 10); Frontier Dispute (Burkina Faso *v.* Mali), Provisional Measures, 1986 (Jan. 10); Land and Maritime Boundary (Cameroon *v.* Niger.), Provisional Measures, 1996 I.C.J. (Mar. 15); Armed Activities on the Territory of the Congo (Congo *v.* Uganda), Provisional Measures, 2000 I.C.J. (Jul. 1).

114 *See* Military and Paramilitary Activities in and against Nicaragua (Nicar. *v.* U.S.), Judgment, 1986 I.C.J. (Jun. 27); Armed Activities on the Territory of the Congo (Congo *v.* Uganda), Judgment, 1999 I.C.J (Jun. 23). *See also* the Oil Platforms (Iran *v.* U.S.), Judgment, 2003 I.C.J. (Nov. 6); Border and Transborder Armed Actions (Nicar. *v.* Hondu.), Judgment, 1992 I.C.J. 222 (May 27).

7. Cyber Warfare and Countermeasures

Countermeasures are an important tool for a State to respond to breaches of its international rights.[115] Countermeasures are acts which are otherwise prohibited by international law but justified because of previous wrongful act by another State. Cyber operations with the aim to cause civil strife would be a wrongful act as good as the illegal use of force or violating the principle of non-intervention or cyber operations. Before resorting to cyber-countermeasures, a certain requirements need to be met.[116] Any counter measure must be taken in response to an international wrongful act against the State which committed the wrongful act. Countermeasures must be proportional and they shall not affect certain fundamental obligations including the prohibition on the use of force[117] and the duty to protect fundamental human rights.[118] The purpose of countermeasures is not to punish, but to induce the wrongdoing State to comply with its obligations arising from international law. Before taking countermeasures, the injured State would also have a legal obligation to call upon the responsible State to discontinue the wrongful action.[119] In addition, the offended state might undertake retorsions, which are unfriendly but lawful actions under international law. Typical examples are travel restrictions and the severance of diplomatic relations.

8. Conclusion

It is a major challenge for international lawyers to address cyber attacks from the perspective of *jus ad bellum*. Until today no incident in Northeast Asia discussed in this article referred to as cyber attack has constituted a use of force or reached the threshold of an armed attack under Article 51 of the UN Charter. In general, there is little agreement whether a cyber attack which does not cause any physical damage,

115 For details, *see* J. Crawford, The International Law Commission's Articles on State Responsibility: Introduction, Text and Commentaries 282 (2002).

116 ILC Article on State Responsibility art. 49; Tallinn Manual Rule 9. *See also* Gabcikovo-Nagymoros Project (Hung. *v.* Slovk.), Judgment, 1997 I.C.J. ¶ 85 (Sept. 25).

117 Oil Platforms (Iran *v.* U.S.) 2003 I.C.J. ¶¶ 12-13 (Nov. 6)(Separate Opinion of Judge Simma), *available at* http://www.icj-cij.org/docket/files/90/9735.pdf (last visited on Nov. 7, 2013).

118 ILC Articles on State Responsibility arts. 50, 51 & 52.

119 Gabcikovo-Nagymoros Project (Hung. *v.* Slovk.), Judgment, 1997 I.C.J. ¶ 85 (Sept. 25).

death or injury but disrupts or damages critical infrastructure of a State is an illegal use of force. State practice in the future or a treaty providing definitions and a legal framework may solve the problem. A regional or global treaty on cyber security could also address cyber operations including cyber theft and cyber espionage which are below the threshold of an armed attack. It will establish mechanisms for interstate co-operation and prevent private actors from engaging in cyber attacks. However, there is currently no consensus for such a treaty among major powers[120] or at the regional level in Northeast Asia.

Cyber operations add another controversial category to *jus ad bellum* in the post-Cold War era. Arguably, a state which feels threatened by cyber attacks will likely favor a broad and flexible interpretation of Articles 2(4) and 51 of the UN Charter. However, such interpretation may be open to abuse, lead to the escalation of violence, and the erosion of the existing legal framework under the UN Charter. In the past, States in Northeast Asia appeared to be attached to a narrow conception of the use of force in international relations. They avoided, *e.g.*, controversial statements justifying humanitarian interventions or regime change towards North Korea. After the shelling of the Yeonpyeong Island and the *Cheonan* incident, plausible arguments were put forward to act in self-defense. However, the South Korean government avoided escalation. One may therefore not expect novel claims in regard to the use of force in cyberspace. Time will tell which types of cyber attack States in Northeast Asia will classify as an armed attack pursuant to Article 51 of the UN Charter.

[120] For details, *see* J. Goldsmith, *Cybersecurity Treaties. A Skeptical View February 2011*, *in* Future Challenges in National Security and Law (P. Berkowitz ed., 2011) *available at* http://media.hoover.org/sites/default/files/documents/FutureChallenges_Goldsmith.pdf (last visited on June. 25, 2013).