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).