

University of Hamburg

European Master's Degree in Human Rights and Democratisation
A.Y. 2015/2016

Strengthening Security in Cyber Space

A brief study of restriction on cyber attacks

Author: Xu Huang

Supervisor: Prof. Götz Neuneck

Abstract

Cyber security has drawn great attention in recent years as nowadays we rely on information and communication technologies (ICTs) more than ever before. From the civilian aspect, cybercrime cast shadow on information security, the increasing number of case is threatening the global economics as well as the public security. Moreover, misuse of ICTs in terrorist activities has enlarged its influence serving as an efficient tool. Furthermore, frequently launched cyber attacks have raised the global awareness concerning the potential risk of applying ICTs for military and political purpose, However, to date international legal framework seems to lack capacity in regulating relevant acts, while the global security and stability could be affected and challenged, there is urgent need for establishment and development on norms and regulation to restrict malicious cyber activities on the global level.

In this thesis, I'm going to investigate on the possible restriction of cyber threats. In Chapter 1, I would make a brief introduction to these emerging cyber threats. Chapter 2 would focus on the updated debates and efforts concerning cyber security issue made by significant global and regional organizations. Last but not least, application of international law and principles on malicious state acts in cyber space would be discussed in Chapter 3.

Contents

Chapter 1 A brief introduction to cyber threats

1.1	<i>Confusion of Terminology</i>	5
1.2	<i>Different impacts of Cyber attacks</i>	7
1.2.1	<i>Confidentiality</i>	7
1.2.2	<i>Integrity</i>	7
1.2.3	<i>Availability</i>	7
1.3	<i>Notable cyber incidents</i>	8
1.3.1	<i>2007 Estonia</i>	8
1.3.2	<i>2008 Lithuania</i>	10
1.3.3	<i>2008 Georgia</i>	11
1.3.4	<i>2009 Stuxnet</i>	13
1.3.5	<i>2014 Sony Pictures Entertainment</i>	14
1.4	<i>Characteristics of cyber threats</i>	15
1.4.1	<i>Complexity of the Multivariate Actors</i>	15
1.4.2	<i>Lack of Capacity and Governance</i>	17
1.4.3	<i>Significant Effect and Damage</i>	19

Chapter 2 Debates and efforts of International and Regional Organizations and other International Fora on Cybersecurity

2.1	<i>International Organizations</i>	20
2.1.1	<i>United Nations (UN)</i>	21
2.1.2	<i>International Telecommunication Union (ITU)</i>	25
2.2	<i>Regional Organizations</i>	27
2.2.1	<i>North Atlantic Treaty Organisation (NATO)</i>	27
2.2.2	<i>European Union (EU)</i>	29

2.2.3	<i>Organization for Security and Co-operation in Europe (OSCE)</i>	31
2.2.4	<i>Council of Europe (CoE)</i>	36
2.2.5	<i>Shanghai Cooperation Organization (SCO)</i>	38
2.3	<i>Other International Conferences and Fora</i>	41
2.3.1	<i>International Governance Forum (IGF)</i>	42
2.3.2	<i>Global Conference on Cyber Space (GCCS)</i>	43
2.3.3	<i>Forum of Incident Response and Security Teams (FIRST)</i>	45

Chapter 3 Applicable existing International Law and Principles that regulates cyber attacks conducted by state actor and the challenge of its application

3.1	<i>Cyberwar and Cyberwarfare</i>	46
3.2	<i>Law of armed conflict-Cyber attack in the context of international armed conflict</i>	50
3.2.1	<i>Jus ad bellum</i>	53
	<i>(1) prohibition on the use of force</i>	53
	<i>(2) justified use of force</i>	57
3.2.2	<i>Jus in bello</i>	59
3.3	<i>Prosecution of perpetrator</i>	62
	Conclusion	64