

---

# CYBER SECURITY & CYBER WARFARE: A COMPARATIVE STUDY OF THE PRINCIPLES OF INTERNATIONAL LAW IN CYBERSPACE

---

Divyanshu Saxena, NALSAR University of Law, Hyderabad

## ABSTRACT

The *primary objective* of the research study is to understand the conceptual distinction between the terms ‘Cyber Warfare’ and ‘Cyber Attacks’ by using the example of the recent breach of information attack that was targeted at the US Presidential Elections in the year 2016 to cause electoral disadvantage to the candidate of Democratic National Committee (DNC), Hillary Clinton. The *secondary objective* of the research study is to analyse the recent progressive legal and technological developments that have been incorporated in the principles of ‘International Law in Cyberspace’. The research study includes a comparison between the civil and military national doctrines of the nation-states to promote the development of adequate ‘Cyber Capabilities’ and ‘Cyber Defence Systems’. The critical aspects of the research elaborate upon the immediate necessity of the nation-states to develop progressive technological mechanisms to protect the military computers and systems during the instances of Cyber Warfare. The *final objective* of the research study is to suggest significant structural changes that are required to prevent the emerging threats of ‘Cyber Attacks’ and ‘Cyber Terrorism’ through mutual cooperation and uniform accommodation of the 2 major principles of International Law as adopted by the nation-states under the UN Charter and Geneva Conventions- ‘*Jus in Bello*’ and ‘*Jus Ad Bellum*’, that refer to ‘*conducting war*’ and ‘*going to war*’ respectively.

**Keywords:** ‘*Cyber Attacks*’, ‘*Cyber Warfare*’, ‘*Cyber Capabilities*’, ‘*Cyber Defence Systems*’, ‘*International Law in Cyberspace*’, ‘*Jus In Bello*’, ‘*Jus Ad Bellum*’

## CHAPTER – 2: RESEARCH METHODOLOGY

The research study has been conducted by using the methodology of '*Comparative Analysis*' of the several contemporary '**Civil and Military Cyber Security Doctrines**' as adopted by the various nation-states between the years **2006 - 2012** due to the emerging threats of '**Cyber Attacks**'. The research aims at a '*Conceptual Analysis*' of the distinction between the meaning of the terms '**Cyber Attacks**' and '**Cyber Warfare**' to understand the offensive and defensive approaches adopted by the various national doctrines to promote '**Cyber Security**'. The Article – 2(4) and Article-51 of the UN Charter enshrines the International law principles of '**necessity**' and '**proportionality**' during the instances of '**Cyber Warfare**'. Moreover, the research has accommodated the principles of **International Conventions** as signed by the member parties of the **United Nations (UN), Council of Europe etc.** to understand the legal changes that have led to the shift in the public policy of the nation-states towards the development of '**Cyber Capabilities**' and '**Cyber Defence Infrastructure**'. In conclusion, the researcher has used a '*Methodological and Comparative approach*' to deal with the legal as well as the policy related issues raised during the course of the research study.

**KEYWORDS** – '*Civil and Military Cyber Security Doctrines*', '*Comparative Analysis*', '*Conceptual Analysis*', '*Cyber Defence Infrastructure*', '*Methodological and Comparative Approach*'

## CHAPTER – 3: THEORETICAL DISCUSSION

### 3.1 THE DEVELOPMENTS IN THE PRINCIPLES OF INTERNATIONAL LAW IN 'CYBERSPACE':

The research study elaborates upon the applicability of the 2 principles of international law i. e. **Jus Ad Bellum and Jus In Bello**, which refer to '*going to war*' and '*conducting war*' within the sphere of international 'Cyber Security'. The **Jus in Bello** principle can be derived from the agreements adopted by the nation-states through the ratification of the Geneva conventions, IV Hague convention etc. and thereby, can be applied in the circumstances where two or more nation-states have been actively involved in '**Armed Conflicts**' leading to the threat of 'Cyber Attacks' being launched to destruct the critical and military infrastructures. The objective of nation-states functioning under the ambit of the *Jus In Bello principle* is to attain technological advancements in the development of '**Cyber Capabilities**' – both offensive and defensive, in

order to ensure 'Cyber Security' within the 'Cyberspace'. Whereas, the **Jus Ad Bellum** principle can be derived from the provisions of the UN Charter as adopted by the member states upon the doctrine of '**use of force**'.

For example, In the year 2011, the government of Albania has entered into a 1-year programme with the government of USA to develop '**Air Control mechanisms**' and strategic 'Cyber Capabilities' under the '**Albanian Cyber-Security Program**'. Similarly, the government of UK planned to spend as much as 1.06 billion euros towards the development of a three-fold '**Cyber Security Strategy**' between the year 2009-2013. In April 2010, the government of India established a '**Cyber Security Laboratory**' to develop current threat assessment reports, offensive cyber capabilities etc.

### **3.2 THE APPLICABILITY OF THE INTERNATIONAL CONVENTIONS IN 'CYBERSPACE':**

The Article – 2(4) of the UN Charter prescribes that the wider scope of the meaning of the phrase '*use of force*' signifies the inclusive nature of the same provision while resolving the question of the applicability of the principles of International law in '**Cyberspace.**' The Article -51 of the UN Charter enshrines the nation-state's '**Right to Self-Defence**' against the emerging threats of '**Cyber Warfare**' by invoking the '**Proportionality**' principle and '**Necessity**' principle of International law. The applicability of the several '**International Conventions**' can be derived from the consent of the nation-states that ratify the obligations imposed upon them such as the '**UN Convention Against Transnational Organized Crime, 2000**'<sup>1</sup> that obligates the member nation-states to enact domestic laws in order to bring the 'Cyber Crime Offences' under the purview of the uniform legal principles and standard mechanism of law enforcement. Moreover, the '**Convention on the Rights of the Child, 1989**'<sup>2</sup> aims to direct the member nation-states to prevent the illegal human-trafficking of children and the subsequent, sexual exploitation of them by organized criminal groups through sale, prostitution, pornography etc.

The '**Council of Europe**' has also drawn several international conventions to achieve 'Cyber Security' such as the '**Convention on Cyber Crime, 2001**'<sup>3</sup>, also known as the '**Budapest**

---

<sup>1</sup> 2225 U.N.T.S. 209

<sup>2</sup> 1577 U.N.T.S. 3

<sup>3</sup> E.T.S. 185

**Convention**' to prevent the incidence of computer-related crimes, develop inter-departmental cooperation amongst law enforcement agencies, etc. The '**Convention on the Protection of Children Against Sexual Abuse, 2007**'<sup>4</sup> as ratified by the member European nation-states have been adopted to implement progressive provisions such as the Article – 21(1)(f) to prohibit the use of internet to access child porn, the Article – 30(5) to prohibit the distribution of child porn and the Article- 23 to prohibit the solicitation of the children for sexual purposes in order to prevent the violation of '**International Humanitarian Law**' in '**Cyberspace**.'

## CHAPTER – 4: CONCEPTUAL DISCUSSION

### 4.1 THE DOCTRINE OF 'CYBER SECURITY':

The doctrine of '**Cyber Security**' has evolved over the past two decades due to the emerging threat of the possibility of '**Cyber Attacks**' being perpetrated by the non-state actors as well as the state actors. The research study has focussed on the central precepts of the concept by the assessment of the legal, technical and policy-related issues that have arose due to the recent developments in the field of '**International law in Cyberspace**'. In the **1990s**, the early doctrine of '**Cyber Security**' was termed as the '**Doctrine of Prevention**', which involved the setting-up of '**Cyber Defence Systems**' that were not vulnerable to the specific '**Cyber Attacks**', which were specifically targeted to destruct and to gain remote control access over another nation-state's '**Critical Military Infrastructure**'. The '**Doctrine of Risk Management**' elaborates upon the assessment of the '**Cost of Cyber Attacks**' in the light of the '**Probability of Cyber Attacks**' in order to take policy-decisions over cyber threats, to pass civil/criminal legislations upon '**Cyber Security**', to impose regulations in the '**Cyberspace**' etc. In the early **2000s**, the '**Doctrine of Accountability**' emerged on the basis of the principles of '**necessity**' and '**proportionality**' that were derived from the **Article -51** of the UN Charter. Thus, the application of the doctrine encourages nation-states to deter the '**Cyber Attacks**' through adequate threats of retribution. In the year **2010**, the '**Doctrine of Public Health**' proposed that meaning of the term '**Cyber Security**' must be synonymous to the concept of '**Public Health**' and thereby, it was iterated that the nature of '**Cyber Security**' is a '**non-excludable**' and '**non-rivalrous**' **public good**. This was a progressive step towards the evolution of the contemporary '**Doctrine of Public Cyber Security**' that endorses the

---

<sup>4</sup> C.E.T.S (201)

intervention of Internet Service Providers (ISP) to minimize the exploitation of the public interests in the ‘Cyberspace’.

#### **4.2 THE DOCTRINE OF ‘CYBER WARFARE’:**

The doctrine of ‘Cyber Warfare’ has developed over the recent years due to the changes in the public-policies of several nation-states towards the development of technologically advanced ‘**Cyber Capabilities**’ and the achievement of ‘**Cyber Superiority**’. The general precepts of the doctrine include actions of the nation-states or international organizations to damage the computer systems or information networks of another state. The broader definition of ‘Cyber Warfare’ was given by **Parks and Duggan** that was inclusive of ‘**Computer Network Attack**’ as well as ‘**Computer Network Defence**’. The research study has examined the practical difficulties in determining a ‘**precise and proportionate force**’ against ‘Cyber Attacks’ because of the lack of investigative techniques to apprehend the intended target in order to control the emerging cyber threats. The applicability of the 2 principles of International law – **Jus In Bello and Jus Ad Bellum** becomes necessary in the circumstances of the nation-states exercising their ‘**Right to Self-Defence**’ in response to the emerging sovereign threats in the ‘Cyberspace’. The legal limitations of the ‘**Doctrine of Cyber Warfare**’ includes unresolved issues in relation to the identification of the non-state ‘**proxy actors**’ perpetrating ‘Cyber Attacks’; restricted interpretation of the terms like ‘**armed conflicts**’, ‘**necessity**’, ‘**proportionality**’ within the provisions of the UN Charter, Geneva Conventions, 4<sup>th</sup> Hague Convention etc.

### **CHAPTER – 5: ANALYSIS**

#### **5.1 COMPARTITIVE ANALYSIS:**

*[ The comparative analysis is based upon a research submitted to the United Nations Institute for Disarmament Research (UNIDIR) by the Centre for Strategic and International Studies (CSIS) in the year 2011.]*

##### **5.1.1 NATION-STATES THAT ADOPTED ‘MILITARY DOCTRINE’ OF ‘CYBER SECURITY’:**

###### **a. Albania:**

The government of Albania has proposed a modification to their military doctrine over the issues related to 'Cyber Security & Cyber Warfare' by establishing an '**Interinstitutional Maritime Operational Centre**' (IMOC) to develop '**Airspace Control Mechanisms**' and 'Cyber Defence Capabilities' to protect the sovereignty of the nation during the instances of 'Cyber Attacks'. On **13 June, 2011**, they entered into a one-year initiative called '**Albanian Cyber Security Program**' with the **government of USA** to develop proper 'Cyber Security' response systems in order to prevent the destruction of the critical military infrastructure.

**b. Denmark:**

The **Danish Military Doctrine** is focussed towards the **defensive aspects** of 'Cyber Warfare' that pertain to the protection of the disruption or malfunctioning of the military computer systems. The public policy highlights the 'Cyberspace' as a **war-prone zone** and thereby, provides technical and legal definitions in order to develop a progress 'Cyber Security Policy'. The **modernization plan (2000-14)** of the Danish military aims at the development of '**Cyber Network Operations Units**' to attain '**Interdepartmental coordination**' amongst the different organs of the state to work towards the protection of the information systems and computer systems.

**c. India:**

In the late 1990s, the government of India incorporated 4 major elements within the military policy – *Information Technology, Protection of Critical Infrastructure, Army Mobility and Electronic Warfare*. The government has set -up a '**Cyber Security Laboratory**' at the Military College of Telecommunications Engineering in the year **2010** to conduct technological tests for the generation of current threat assessments, policy recommendations etc. The **NTRO** along with the support of **DRDO** has been working towards the development of **offensive 'Cyber Capabilities'** to combat the emerging threats of '**Cyber Attacks**'. Recently, the suggestions of the **National Security Advisory Board** have recommended the government to set-up a '**Central Cyber Security Command**' based upon the **US Model** in order to encourage mutual sharing of information across the different agencies and organizations of the state.

**d. The Russian Federation:**

The government proposed modifications to the public policy in the year **2010** to extend the meaning of '**Public Health**' towards the development of '**Public Cyber Security**' standards

and encouraged the use of **informational and political instruments** towards the fulfilment of the **national interests**. The **Federal Security Service** that was established in the year **2003** has achieved great advancements in the field of cryptology, code-breaking etc. The international allies of the Russian Federation are working together towards attaining '**Cyber Superiority**' through the mutual cooperation of the nation-states, development of precision weapons etc.

**e. The United Kingdom:**

In **2009**, the government proposed a **three-fold 'Cyber Security Strategy'** in the light of the recent hostile '**Cyber Attacks**' that occurred due to the actions of the non-state actors and thereby, allocated a **sum of 650 million euros** to set up an '**Office of Cyber Security**' to prevent the destruction or breach of the information networks of the state. The UK government is planning to invest **1.06 billion euros** between **the years 2009-2013** in order to develop adequate response system mechanisms and offensive cyber capabilities.

**f. Malaysia:**

The Prime Minister of Malaysia announced the '**Cyber Security Malaysia Programme**' in the year **2007** to promote the protection of the interests of the state and the business organizations within the '**Cyberspace**'. The development of **training centres for IT professionals**, education and awareness programmes etc. is include within the objectives of the law enforcement agencies in the light of the **hostile 'Cyber Attacks'** that happened in the year **2011**.

**g. The United States:**

The **Department of Homeland Security** along with the support of the Department of Defence have established a **central 'Cyber Command'** in order to generate information control over the functioning of the several law enforcement agencies as well as to develop inter-departmental coordination to ensure the early identification of the '**Cyber Attacks**'. The **National Cyber Response Coordination Group** comprises of **13 federal agencies** that work together towards the attainment of '**Public Cyber Security**'.

### **5.1.2 NATION-STATES THAT ADOPTED 'CIVIL DOCTRINE' OF 'CYBER SECURITY':**

**a. Japan:**

In **2006**, the government established a **‘Cyber Clean Centre’** through the passing of several civil legislations in the form of an emergency response system against the emerging threats of **‘Cyber Attacks’**. Moreover, the government established a **‘Central Cyber Command’** to promote the mutual assistance of different institutions and agencies towards **‘Cyber Security’** in the year **2008**. In **2011**, Japan signed a **non-binding bilateral strategic policy dialogue** with US to deal with **‘Cyber Warfare’** issues.

**b. Indonesia:**

Due to the **absence of military or technological organizations** to prevent the threats of **‘Cyber warfare’**, the nation-state is a signatory to the several conventions of the **Council of Europe** to work towards the development of security standards during electronic transactions, prevention of data theft or data intervention etc. Therefore, the government of Indonesia has passed **IT and Offense (RUUPITPI) Bill in the year 2010** to promote **‘Cyber Security’** in the **‘Cyberspace’**.

**c. Belgium:**

The Belgian government has **no central authority** to deal with the cyber threats and thereby, they have established a consultative platform, called as **‘Belgian Network of Information Security’** to protect the critical military infrastructure of the state. They have also entered into memorandum of understanding agreements with **the Netherlands and Luxembourg** to develop mutual cooperation towards the achievement of **‘Cyber Security’**.

**d. The Czech Republic:**

In the year 2010, due to the absence of any organizations or command to control the infliction of sovereign and financial threats in the **‘Cyberspace’**, the government of the Czech Republic **lost 10 million euros** during a transaction upon the **European Union Emissions Trading System**. Therefore, the **Ministry of Interior** have proposed several recommendations to the new **‘Cyber Policy’** through legislation like development of **‘Cyber Defence Infrastructure’**, **‘Cyber Emergency Response Team’** etc.



**e. South Africa:**

The government has set-up a **Cyber Inspectorate in the year 2012** to deal with the emerging hostile and xenophobic ‘Cyber Attacks’ by developing current threat assessment reports, recommendations to the national cyber policy etc. Therefore, the South African cabinet announced **the ‘Cyber Security Policy’ in the year 2011** to bring all the institutions and departments under the purview of information sharing networks and security systems.

**f. Pakistan:**

The country is deeply affected by the threats of ‘**Cyber Terrorism**’ due to the presence of a large-scale hacker community within the territorial boundaries of the state. The ‘**Electronic Crime Ordinance**’ was recently passed by the government to promote the development of Early Warning Systems and investigative capabilities to identify the perpetrators of the ‘Cyber Attacks’. The government established ‘**The Cyber Centre**’ in **2003** to develop greater standards of ‘Public Cyber Security’.

**g. Singapore:**

The government developed the **Infocom Security Masterplan** in the year **2003** to promote the protection of the national interests as well as the interests of the business organizations. The **Infocom Technology Security authority** controls all the operational cyber activities and also, hires IT professionals as ‘**Cyber Defenders**’ to ethically hack in the pursuance of national interests.

**CHAPTER – 6: CONCLUSIVE REMARKS**

The example of the **2016 US Presidential Elections** reflects legal concerns about the protection of the values of ‘Electoral Democracy’ in the light of the emerging cyber threats and thus, it must be inferred that it is the responsibility of the ‘**Modern State**’ to achieve ‘Cyber Security’ and ‘Information Security’ to prevent the unnecessary exploitation of the fundamental rights of the citizens. After the ‘Cyber Attacks’ of 2016, US is working towards the development of ‘**Cyber Defence Systems**’ and ‘**Early Warning Systems**’ and moreover, the US public policy has been modified towards adopting the ‘**Smart Power Approach**’ to strategically deal with the diverse forms of ‘**Cyber Warfare**’. Thus, it must be inferred from the conceptual analysis of the distinction between the terms ‘Cyber Warfare’ and ‘Cyber

Attacks’ that the latter refers to a **‘deliberate or malicious attempt’** to damage the information network systems of another state and must be dealt under the provisions of the **Article-2(4)** of the UN Charter.

In conclusion, the research study prescribes that the **‘Doctrine of Public Cyber Security’** must be implemented by the mutual efforts and cooperation of the nation-states in order to prevent the use of internet as a means of inflicting ‘Cyber Attacks’ against the sovereignty of another state. The comparative analysis of the military and civil cyber security doctrines as adopted by the several nation-states clearly reflects the necessity of the development of **‘Cyber Capabilities’** and **‘Cyber Defence Infrastructure’** to prevent the instances of information breach, data theft, etc. The unresolved issues like the identification of the non-state actors working as **‘proxy actors’**, **‘use of precise and proportionate force’** etc. must be dealt under the two principles of International law – **Jus In Bello and Jus Ad Bellum**, which are applicable in the **‘Cyberspace’** to promote the fundamental objectives of the **‘International Humanitarian Law’**.

## **CHAPTER – 7: BIBLIOGRAPHY**

1. ‘NATO opens new centre of excellence on Cyber Defence’, NATO News, 14<sup>th</sup> May, 2008
2. Irfan Ahmad, ‘The new cyber law in Pakistan restricts free speech’, One World, South-Asia, 24<sup>th</sup> January, 2008
3. The first National Strategy on Information Security, Japanese National Information Security Policy council, 2006, pg. 1
4. The second National Strategy on Information Security, Japanese National Information Security Policy council, 2009, pg. 54
5. “Czech Republic Country Report”, European Network and Information Security Agency, 2011, pg. 11
6. “Country Report: Belgium”, European Network and Information Security, 2009, pg. 9
7. Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization and Protection, 17<sup>th</sup> December, 2003
8. Eleanor Keymer, ‘UK recruits cyber experts to protect key networks’, Jane’s Defence Weekly, 6<sup>th</sup> February, 2011
9. ‘Cyber Security Strategy of the UK, UK Office of Cyber Security, pg. 6
10. Danish Defence Agreement (2010-2014), 24<sup>th</sup> June 2009, pg.11

11. The First Annual Analysis of the Interinstitutional Maritime Operational Centre, Albanian Ministry of Defence, 21<sup>st</sup> December, 2010
12. 'USAID launches the Albanian cyber security programme', United States Agency for International Development, 13 June, 2011
13. Nicola Berkovic, "Defence on a cyber footing", The Australian, 16<sup>th</sup> January 2010
14. 'Denmark: Country Report', European Network and Information Security Agency, 2011, pg. 16
15. Tom Espiner, 'UK cyber security centre starting operations in March', ZDNet, 13<sup>th</sup> November, 2009