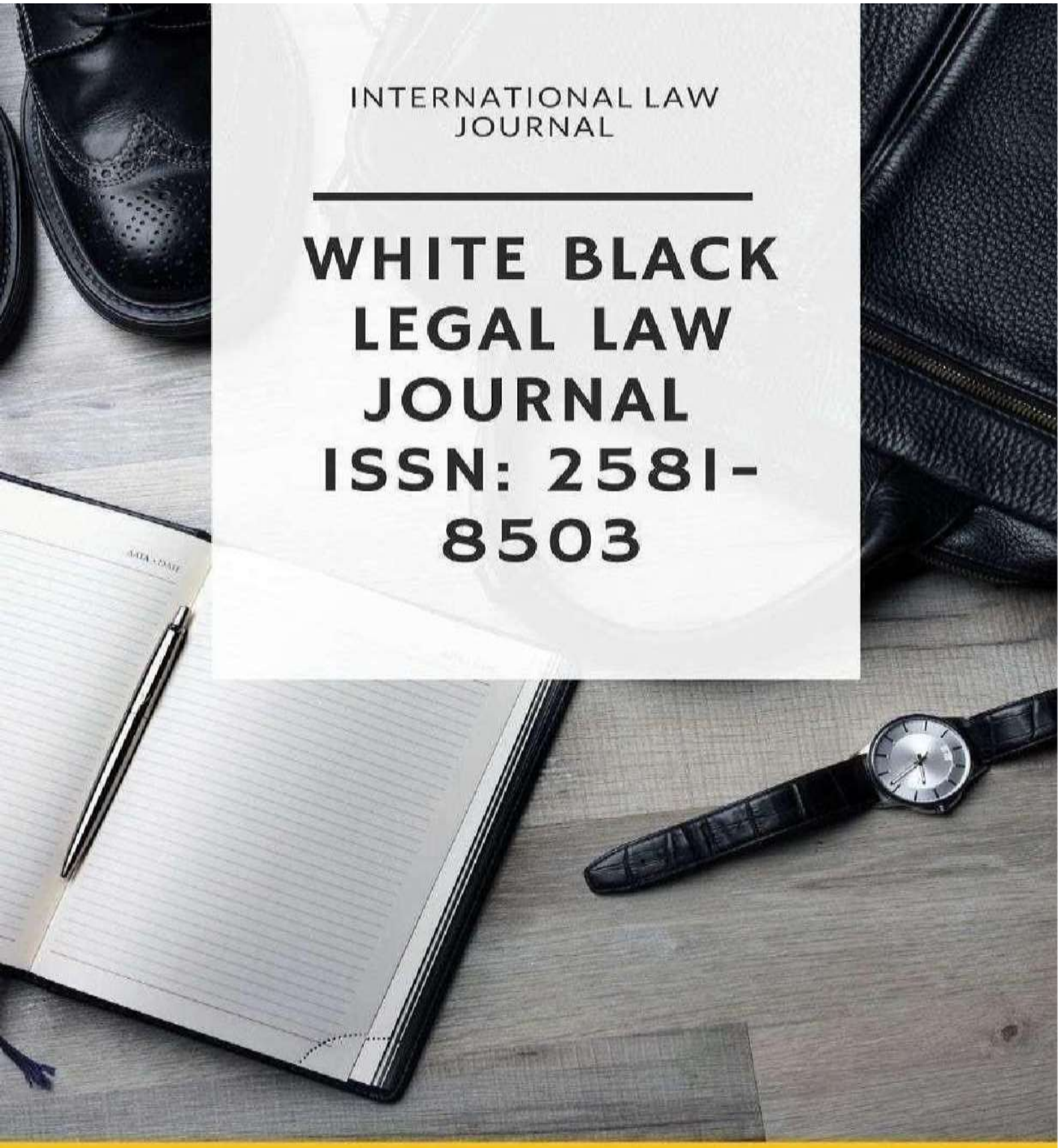

INTERNATIONAL LAW JOURNAL

# WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

## Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

## DISCLAIMER

# EDITORIAL TEAM

## Raju Narayana Swamy (IAS ) Indian Administrative Service officer

Dr. Raju Narayana Swamy popularly known as Kerala's Anti Corruption Crusader is the All India Topper of the 1991 batch of the IAS and is currently posted as Principal Secretary to the Government of Kerala . He has earned many accolades as he hit against the political-bureaucrat corruption nexus in India. Dr Swamy holds a B.Tech in Computer Science and Engineering from the IIT Madras and a Ph. D. in Cyber Law from Gujarat National Law University . He also has an LLM (Pro) ( with specialization in IPR) as well as three PG Diplomas from the National Law University, Delhi- one in Urban Environmental Management and Law, another in Environmental Law and Policy and a third one in Tourism and Environmental Law. He also holds a post-graduate diploma in IPR from the National Law School, Bengaluru and a professional diploma in Public Procurement from the World Bank.

## Dr. R. K. Upadhyay

Dr. R. K. Upadhyay is Registrar, University of Kota (Raj.), Dr Upadhyay obtained LLB , LLM degrees from Banaras Hindu University & Phd from university of Kota.He has succesfully completed UGC sponsored M.R.P for the work in the ares of the various prisoners reforms in the state of the Rajasthan.

# Senior Editor

## Dr. Neha Mishra

Dr. Neha Mishra is Associate Professor & Associate Dean (Scholarships) in Jindal Global Law School, OP Jindal Global University. She was awarded both her PhD degree and Associate Professor & Associate Dean M.A.; LL.B. (University of Delhi); LL.M.; Ph.D. (NLSIU, Bangalore) LLM from National Law School of India University, Bengaluru; she did her LL.B. from Faculty of Law, Delhi University as well as M.A. and B.A. from Hindu College and DCAC from DU respectively. Neha has been a Visiting Fellow, School of Social Work, Michigan State University, 2016 and invited speaker Panelist at Global Conference, Whitney R. Harris World Law Institute, Washington University in St.Louis, 2015.

## Ms. Sumiti Ahuja

Ms. Sumiti Ahuja, Assistant Professor, Faculty of Law, University of Delhi,

Ms. Sumiti Ahuja completed her LL.M. from the Indian Law Institute with specialization in Criminal Law and Corporate Law, and has over nine years of teaching experience. She has done her LL.B. from the Faculty of Law, University of Delhi. She is currently pursuing Ph.D. in the area of Forensics and Law. Prior to joining the teaching profession, she has worked as Research Assistant for projects funded by different agencies of Govt. of India. She has developed various audio-video teaching modules under UGC e-PG Pathshala programme in the area of Criminology, under the aegis of an MHRD Project. Her areas of interest are Criminal Law, Law of Evidence, Interpretation of Statutes, and Clinical Legal Education.

## Dr. Navtika Singh Nautiyal

Dr. Navtika Singh Nautiyal presently working as an Assistant Professor in School of law, Forensic Justice and Policy studies at National Forensic Sciences University, Gandhinagar, Gujarat. She has 9 years of Teaching and Research Experience. She has completed her Philosophy of Doctorate in 'Intercountry adoption laws from Uttranchal University, Dehradun' and LLM from Indian Law Institute, New Delhi.

## Dr. Rinu Saraswat

Associate Professor at School of Law, Apex University, Jaipur, M.A, LL.M, Ph.D,

Dr. Rinu have 5 yrs of teaching experience in renowned institutions like Jagannath University and Apex University. Participated in more than 20 national and international seminars and conferences and 5 workshops and training programmes.

## Dr. Nitesh Saraswat

E.MBA, LL.M, Ph.D, PGDSAPM
Currently working as Assistant Professor at Law Centre II, Faculty of Law, University of Delhi. Dr. Nitesh have 14 years of Teaching, Administrative and research experience in Renowned Institutions like Amity University, Tata Institute of Social Sciences, Jai Narain Vyas University Jodhpur, Jagannath University and Nirma University.
More than 25 Publications in renowned National and International Journals and has authored a Text book on Cr.P.C and Juvenile Delinquency law.

## Subhrajit Chanda

BBA. LL.B. (Hons.) (Amity University, Rajasthan); LL. M. (UPES, Dehradun) (Nottingham Trent University, UK); Ph.D. Candidate (G.D. Goenka University)

Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International Trade Law.

# *ABOUT US*

WHITE BLACK LEGAL is an open access, peer-reviewed and refereed journal providededicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you

www.whiteblacklegal.co.in
Volume 3 Issue 1 | March 2025 ISSN: 2581-8503

# DECIPHERING THE DIGITAL BATTLEFIELD: A COMPREHENSIVE ANALYSIS OF CYBER WARFARE IN THE 21ST CENTURY

AUTHORED BY: THOMAS K JOSEPH
Undergraduate Student
School of Law
Christ (Deemed to be University)

## *ABSTRACT*

The ashes of World War II ignited a never-ending arms race, innovating technology that posse's threat to humanity. Modern combat transcends beyond the physical battlefield, embracing the five domains: land, sea, air, space and the ever-evolving cyberspace. This exponential increase in scale needs a new view of conflict, as a single strike can have global consequences. Cyberwarfare, an unknown concept in the past, has now become a major aspect of modern warfare, silently infiltrating critical infrastructure and blurring the line between military personnel and civilians as they are exposed to the digital nexus. A cyber network is a collection of two or more electronic devices, connected together with an objective of sharing resources and exchanging data. Users can access the data on such platforms through the internet. Such data carrying vital information is prone to cyber threats. In a digital era, where the world is connected through a cyber network. Threats rise to an international degree. Although there is no definite definition for Cyber Warfare, it can be defined as a grey zone warfare between states by the forefront weapon as the internet to gain an advantage over an enemy state. Cyber Warfare, unlike traditional war, is not fought using kinetic weapons and existing laws of war do not apply to such grey zone warfare. The International Convention on Cyber Crime, 2001 (Budapest Convention) is recognised as the law binding on cybercrimes although there exists a source of international law it was not effective due to its limitations. Data protection legislations in India are experiencing various challenges and resentments owing to the lack of a strong legislative framework. The research paper briefly discusses the types of Cyber Warfare, its legal position in the international community and India's efforts to subdue cybercrimes.

**KEYWORDS:** Cyber Warfare, Cyber Crime, Stuxnet, Modern Warfare, Cybersecurity.

## *CHAPTER 1: HISTORY AND EVOLUTION*

Throughout history, humans have resorted to violence to achieve worldly desires. From the swords, maces, and spears of the ancient era to the gunpowder revolution that transformed warfare, our methods of conflict have evolved alongside our ingenuity. however, with the dust settling from World War II, a new kind of battleground emerged. Fueled by an ideological arms race, the Cold War saw superpowers like the United States and the Soviet Union recognize the growing importance of communication networks. This realization sowed the seeds of cyber warfare, a conflict fought not with bullets and bombs, but with lines of code. While the Cold War did not witness any large-scale cyberattacks, it mirrored the traditional arms race where each side developed offensive and defensive cyber capabilities, creating a constant push and pull in technological advancement[1]. This led to countries trying to disrupt each other's military communications and intelligence gathering. This dynamic continues today, with majority nations actively developing offensive cyber weapons. The rise of the internet in the 20th century marked a significant point in history. The world in 1998 witnessed the "Moonlight Maze" attacks, where US hackers infiltrated Chinese military systems, which showcased the offensive potential of cyberspace[2]. The recent decade has seen a significant increase in complexity. Cyber weapons such as Stuxnet blurred the gap between digital and physical warfare, as attacks with ransomware devastated key infrastructure. The emergence of cryptocurrency has made cybercrime monetizable, and the possible integration of Artificial Intelligence into cyberattacks creates horrifying future possibilities. This rapid increase demonstrates the ever-changing nature of cyber warfare, which necessitates ongoing adaptation and creativity in security strategies.

### DEFINITION OF CYBER WARFARE

Cyber warfare refers to the use of computer networks and digital tools to attack an enemy state, organization, or individual[3]. Cyber warfare can be highly targeted, allowing attackers to inflict significant damage with minimal physical footprint. This makes it a cost-effective and potentially deniable tool for achieving political or military objectives.

Cyber warfare can include a variety of operations, but these are some of the most prevalent

[1] History.com editors, 'Arms Race'.
[2] Trystan Orr, A Brief History Of Cyberwarfare
[3] James A. Green, 'Cyber Warfare: A multidisciplinary analysis'.

ones:

- Espionage: It is defined as stealing classified information or intellectual property using digital means. This can include hacking into government or corporate networks, installing malware, or deceiving employees into disclosing sensitive information (phishing).
- Sabotage: It is defined as the deliberate disruption or disablement of essential infrastructure or military systems. This might include attacks on power grids, transportation systems, financial institutions, and weapon control systems. Manipulating control systems, planting harmful malware, or conducting denial-of-service assaults to overwhelm a system are all potential tactics.
- Disinformation campaigns involve spreading incorrect or misleading information in order to create confusion, destroy trust, and manipulate public opinion. This can be accomplished by manipulating social media, hacking news websites, or creating phony online personas to promote propaganda.
- Denial-of-Service (DoS) attacks include overwhelming a website or server with traffic, rendering it unreachable to genuine users. This may impair critical services such as online banking, government websites, and communication platforms.
- Data manipulation: It refers to tampering with or manipulating data for a variety of purposes. This could include stealing financial information, influencing election results, or interrupting scientific research.

The practical distinction between cyber terrorism and information warfare is that cyber terrorism is about inflicting fear and harm to everyone nearby, whereas information warfare has a specific objective in a conflict (ideological or declared). Information warfare is well defined as a planned attack by nations or their agents against information and computer systems, computer programs, and data that result in enemy losses. In addition to these phrases, law enforcement authorities frequently refer to the problem of cybercrime. Cybercrime is a crime perpetrated with the use of information technology. We must note that the physical manifestations of cyber terrorism, information warfare, and cybercrime frequently resemble one another.

Assume that someone gains access to a hospital's medical database and changes the medicine of a pro-business, anti-environmental leader at a Fortune 100 company to one to which he or she is critically allergic, as well as removing the allergy from his or her digital record. The

nurse gives the medicine, and the patient dies. So, what definition applies? The solution is not in the mechanics of the occurrence, but in the intent that motivated the individual's actions. If it was done on purpose, for example, as a result of strained relations between these two people, it would be both murder and a cybercrime. If the executor later announces that he or she is willing to execute similar acts if their demands are not met, this could be classified as cyber terrorism. If the operations were carried out by an agent of a foreign power, they could be classified as information warfare. The distinction between these phrases is critical because there are non-technological concerns and solutions that will influence any approach for addressing cyber warfare and cyber terrorism. The most crucial part of cyberattacks with physical implications is understanding the attacker's objective.

## *CHAPTER 2: CASE STUDY (STUXNET)*

### STUXNET

In 2010, a highly complex computer worm was revealed called the Stuxnet. This state-sponsored cyber weapon was made with an aim to stop Iran's nuclear enrichment program, specifically targeting the centrifuges which were used in separating the fissile isotopes used in development of nuclear weapons. Stuxnet was capable enough to influence industries by taking control of its industrial control system (ICS) and could be used to cause destruction in the physical realm. This demonstrated the growing threat and everchanging nature of cyber warfare.[4]

Although the official responsibility for Stuxnet remains unclear, a plethora of evidence suggests that the United States and Israel worked together on the operation. The complexity of the operation, the accuracy with which Iranian nuclear facilities were targeted, and the technology needed to develop a weapon of that kind all suggest state involvement.[5]

The Stuxnet attack had a significant impact on Iran's nuclear program, allegedly slowing uranium enrichment processes for several years. It sparked a global debate on the legality and ethics of cyber warfare. There is presently no established international law governing cyberattacks, making it hard to hold criminals accountable. Furthermore, the likelihood of unanticipated consequences and heightened hostilities between states causes serious concern.

[4] Samuli Haataja, 'Cyber Attack and International Law on Use of Force'.
[5] Ibid, Chapter 4.

The Stuxnet attack highlights the importance of international cooperation in developing standards and guidelines for cyber warfare. These standards should address attribution, proportionality, and the targeting of civilian infrastructure. Furthermore, international frameworks are required to encourage responsible state behaviour in cyberspace and set consequences for malevolent activity, the international community must collaborate to establish organizations and laws that promote peace and stability in cyberspace.

## *CHAPTER 3: INTERNATIONAL LAWS*

### UNITED NATIONS CHARTER

Walter Benjamin, a German philosopher distinguishes between two forms of violence: law making violence and law preserving violence. Law making violence is the violence evident in the establishment of legal order, whereas on the other hand refers to violence used to preserve legal order.[6] International law therefore is concerned particularly with the violence associated with war and its containment through and within positive law.

Article 2(4) of the United Nations Charter prohibits the threat or use of force and calls on all Members to respect the sovereignty, territorial integrity and political independence of other States[7]. This article contains many principles, such as; Principle of non-intervention: 'it involves the right of every sovereign state to conduct its affairs without outside interference'.[8] The principle is derived from customary international law. The ICJ elucidates the important element of coercion, which defines, and indeed forms the very essence of, prohibited intervention, is particularly obvious in the case of an intervention which uses force.[9]

#### *'FORCE' AS ENVISAGED IN ARTICLE 2(4):*

Black's law Dictionary defines force as, 'power, violence or pressure directed against a person or thing.[10] The UN Charter or any instrument subsequently adopted within the international community does not have any qualifications as to the type of 'force'. Questions arise due to this ambiguity in the law. However, the general interpretation of the term 'force' is limited to

[6] Benjamin, Walter. (2007). Critique of Violence. In B. Lawrence & A. Karim (Ed.), *On Violence: A Reader* (pp. 268-285). New York, USA: Duke University.
[7] U.N. Charter art. 2(4).
[8] Case Concerning Military and Paramilitary Activities In and Against Nicaragua (Nicaragua v. United States of America); Merits, -, International Court of Justice (ICJ), 27 June 1986, at para 202.
[9] Ibid, at para 205.
[10] Black's Law Dictionary, 9th edn (Thomas-West, 2009), at 717.

'armed force' ('equipped with a weapon'[11]). The UN Charter was of course drafted in the 1940s in an era where means of violence were through bombs, rifles, aircrafts, etc which were engaged in the second world war. The law however must be interpreted as years pass by.

*Does use of Non-Conventional weapons amount to 'use of force' under article 2(4):*
Clausewitzian strategic theory begins with the notion that all battles throughout history have certain features; for example, the essence of war itself does not vary, although warfare, or the methods by which wars are carried out, is always changing.

[12] In other words, the modern warfare takes place in a different terrain and methods of violence is reformed. William Boothby adopts the position that a cyber weapon is defined by its violent consequences - where a means of cyber-attack is 'designed, intended or used, in order to have violent consequences, that is, to cause death or injury to persons or damage or destruction of objects'[13]. Article 2(4) is an effects-based prohibition. The generally accepted interpretation of Article 2(4) is that only those interventions that produce physical damage will be regarded as an unlawful use of force.[14] cyber operations resulting in physical damage or injury will almost always be regarded as a use of force.[15] The majority of analysts disagree with this stringent interpretation due to the possible destabilizing effects of cyber operations on a broad spectrum. Countries are calling for a new convention to control cyber activities, citing alleged flaws in Article 2(4).[16]

**CONVENTION ON CYBERCRIME BUDAPEST, 23.XI.2001**

Adopted in 2001 under the auspices of the Council of Europe. The convention is aimed at criminalising cyber-crime through a common criminal policy in the interest of peaceful usage of technology. The Convention in its core calls for all sectors along with governments to actively participate, an international collaboration of nations and private sectors to combat against cyber-crime. Among its many interests it also aims to protect personal data, individual privacy, smooth operations of transaction of data, etc.

[11] Ibid, at 123.
[12] Von Clausewitz, C. (1997). *On War* (J. J. Graham, Trans.). Wordsworth Editions.
[13] William H. Boothby, Methods and Means of Cyber Warfare (2013), US NAVY College.
[14] Russell Buchan, 'Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?' (2012) 17 Journal of Conflict and Security Law 212, at 219-221.
[15] Andrew. C. Flotz, 'Stuxnet, Schmitt Analysis, and the Cyber "Use-of-Force" Debate', 2012.
[16] Clarke and Knake, 219–255; Hollis, "Why States Need an International Law for Information Operations," 1053; and Silver, 78.

75 countries worldwide have ratified the convention and 20 countries are invited to accede. Members of the Cybercrime Convention Committee share information and experience, assess implementation of the Convention, interpret the Convention through Guidance Notes, or prepare templates for mutual assistance requests and other tools to facilitate the application of the treaty to counter cybercrime more effectively.[17] The Convention on Cybercrime has also received significant opposition for its specific provisions that fail to protect the rights of persons and nations, as well as its overall inadequacies in ensuring a criminal-free cyberspace.[18] Since the crime is borderless, jurisdiction of crime becomes a crucial question to which the convention fails to address. The Budapest Convention through its Article 32b allows for transborder access to data and thus infringes on national sovereignty[19], creating a privacy issue among nations. In consideration of the backlashes of the Convention India among other nations, however abstained from signing the treaty.

### TALLIIN MANUAL 2.0 ON INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS

The Talliin Manual 2.0 on International Law Applicable to Cyber Operations[20] is a non-legally binding study authored by a group of experts led by Micheal Schmitt at the request of the NATO Cooperative Cyber Defence Center of Excellence located in Tallinn, Estonia. The Tallinn Manual 2.0 plays a crucial role in shaping norms, practices, and policies related to international law and cybersecurity. Its contributions extend beyond academia to practical applications in statecraft, conflict resolution, and the promotion of a rules-based international order in cyberspace. Tallinn Manual provides a thorough and careful analysis of how the jus ad bellum and jus in bello translate to cyberspace, along with helpful descriptions of divisive issues that remain to be resolved through state practice and debate[21].

## ***CHAPTER 4: DOMESTIC LAWS***

Until the mid-1990s, most trade and transactions were conducted via post, telegram, and telex. Traders, entrepreneurs, and other professionals were able to gain from the internet due to modern technology.

[17] Cybercrime Convention Committee (T-CY) 'The Budapest Convention on Cybercrime: benefits and impact in practice', Council of Europe, 13 July 2020.
[18] Shalini S, March 3, 2016, 'Budapest Convention on Cybercrime – An Overview.
[19] Alexander Seger, 'India and the Budapest Convention: why not?', 10 August 2016.
[20] Refer Tallinn Manual on The International Law Applicable To Cyber Warfare
[21] Kristen Eichensehr, *Review of "Tallinn Manual on the International Law Applicable to Cyber Warfare"* 108 American Journal of International Law 585–589 (2014).

**INFORMATION TECHNOLOGY ACT 2000**

The Information Technology Act, 2000 was passed by the Indian government, the first legislation in India on technology, computers, e-communication & e-commerce. The IT Act, 2000 legalizes transactions conducted by electronic data interchange and other electronic means of communication, sometimes known as electronic commerce transactions. Because of a few shortcomings in the act, it sparked heated arguments, detailed reviews, and criticism. In 2009, further amendments were made to the act. The Act applies to whole of India and has extra territorial jurisdiction, since the nature of crime being borderless, it made essential to create a wider applicability.[22]

Along with the IT Act, 2000 several policies were formed such as National Cyber Security Policy, 2013[23] and National Policy of Information Technology, 2012[24]. The policies contribute to the protection of critical infrastructure such as the air defense system, nuclear power plants, banking systems, and many others in order to ensure India's economic stability.

National Nodal Agency (NNA) is an organization appointed by the government responsible for all measures including research and development relating to protection of critical infrastructure information.[25] Cyber-Terrorism has also been identified under Section 66(F) of the IT Act punishes anyone whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment for life. Cyber-crimes are also recognized and interpreted under The Indian Penal Code, 1860. The realm of cyber-crimes evolves each day and recognition of these crimes are crucial and due to the shortcoming of appropriate legislation, interpretation of preexisting laws to such crimes become difficult for the judiciary.

[22] Refer Sec 75, Information Technology Act, 2000.
[23] National Cyber Security Policy, 2013.
[24] National Policy of Information Technology, 2012.
[25] Refer Sec 70(A) of IT Act, 2000.