INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

CYBER WARFARE V CYBER TERRORISM- A LEGAL GREY ZONE

AUTHORED BY - ABHISEK PADHI
B.A.LL.B (Criminal Hons) 4th Year 8th Semester
KIIT School of Law (KIIT University)

Abstract

In the contemporary era, the very nature of warfare has undergone a complete transformation. Battles are no longer fought solely with guns; instead, they are now being waged within the 'grey zone'—utilizing computer networks and the internet. This underscores and highlights how cyber warfare and cyber terrorism, despite both being inherently dangerous, remain distinct in terms of their objectives and definitions.

Cyber warfare is viewed as digital activity conducted by one nation against another. Its objective is to neutralize the enemy nation's critical infrastructure, such as power grids, banking systems, and networks.

On the other hand, cyber terrorism is perpetrated by non-state actors or terrorist groups. Its objective is to promote specific political or religious ideologies and to instill fear among the general public, thereby causing nationwide disruption.

The primary distinction between the two lies in their actors and motivations. While cyber warfare is conducted to serve national interests and achieve geopolitical dominance, cyber terrorism is aimed at advancing an ideology and instilling fear within the general public. Warfare is governed by International Humanitarian Law, whereas terrorism is regarded as a criminal act subject to domestic anti-terror legislation.

Ultimately, this document indicates that both of these fall within the "Grey Zone," as they remain below the threshold of open warfare, thereby complicating legal action. The line between them becomes even more blurred when nations utilize proxy terrorist groups to achieve their geopolitical objectives. In the contemporary era, a nation's power is measured less by the strength of its military and more by the robustness of its digital infrastructure.

ISSN: 2582-6433

Keywords - International Humanitarian Law (IHL,) Malware, Anonymity, Grey Zone, Critical Infrastructure, Espionage, Cyber Terrorism, Cyber Warfare.

Introduction-

In today's connected world, wars are no longer fought only with guns and soldiers. Countries and groups now use computers and the internet as powerful weapons. Cyber warfare is when a nation or its agents secretly attack another country's computer networks. They target power grids, banks, military systems, and important infrastructure to create damage and confusion — all without sending a single soldier across the border. The attacker remains hidden, making it difficult to know who is responsible.

Cyber terrorism, on the other hand, is carried out by terrorist groups or individuals. They use the same digital tools to spread fear among common people, disrupt hospitals, transport, or banking systems, and push their political or religious goals.

What makes both dangerous is that they operate in a grey zone — they cause serious harm and chaos, but usually stay below the level of open war. This ambiguity allows attackers to avoid full retaliation while still achieving their objectives.

Cyber warfare-

Cyberwarfare is typically defined as a set of actions by a nation or organization to attack countries or institutions' computer network systems with the intention of disrupting, damaging, or destroying infrastructure by computer viruses or denial-of-service attacks.[1]

It refers to the attacks done by the nation or nation sponsored attacker, on the computer networks, by the computer network, in cyber space, against any other nation, backed by the same motivation as a war would have been. The term cyber is associated with it, as because, the whole procedure of attacking doesn't require any physical action but a digital one where one physically does not enter the boundary of a nation but can destroy its critical infrastructures, electric grid, valuable information military basses etc., just by the using the cyber space.

[1] "Cyber Warfare" *Fortinet*, available at: https://www.fortinet.com/resources/cyberglossary/cyber-warfare (last visited on April 3, 2026).

ISSN: 2582-6433

Cyber warfare typically involves a nation-state perpetrating cyber attacks on another, but in some cases, the attacks are carried out by terrorist organizations or non-state actors seeking to further the goal of a hostile nation.[2]

The nature of this is, only, what make it distinguished from other forms of cyber attacks that is the backing or sponsorship by the state or that its is done by the state itself and when any state is involved in the attack on any other state, be it physical digital or hybrid it is termed as War, generally. One of the defining characteristics of cyber warfare is its anonymity. Attackers can use techniques like hacking, phishing, or social engineering to gain access to systems or information without being detected. This makes it difficult to identify the source of an attack or to retaliate against the attacker.[3]

Cyber warfare and cyber war are interwoven so quite deeply that they looks alike same and are often misinterpreted as one but the difference is quite general and lies in meaning of both- warfare and war.

Cyber war is generally associated with the recognition of the war at cyberspace between the nation as such when two nations are conflicting with each other, armed, so will, it, be called the cyber war when conflict is only limited to the cyber space and no physical breach of boundaries are done.

Cyber warfare, on the other hand, is a means to achieve the goal of cyber war, its technique of conflicting with other nations. Cyber warfare refers to the activity or plan as to how the nation is to engage in the war[4]

Cyber warfare operations typically target systems that influence national power and are of much importance so that maximum damage may be inflicted upon. This includes telecommunications infrastructure, satellite networks, energy grids, logistics platforms, defense contractors, and government agencies. Damaging these systems can create leverage

[2] "Cyber Warfare" *Imperva*, available at: https://www.imperva.com/learn/application-security/cyber-warfare/ (last visited on April 3, 2026).
[3] G. Mahmudov, "Cyber Terrorism and Cyber Warfare: Similarities and Differences" *Scientific Journal of the National University of Defense* (2023), available at: https://institute.nvu.bg/sites/default/files/inline-files/2023-2-03-mahmudov.pdf (last visited on April 3, 2026)
[4] "Cyber Warfare" *Fortinet*, available at: https://www.fortinet.com/resources/cyberglossary/cyber-warfare (last visited on April 3, 2026).

ISSN: 2582-6433

during geopolitical disputes without requiring traditional military confrontation.[5]

The damage inflicted upon, can be varying depending upon the nature of attack but cannot be limited to the computers only but expand up to the death of people. Today's world has been mostly dependent upon the computer network, and everything is controlled by it, be it army operation infrastructure, economics, trade and energy etc. And one wrong click can turn everything into chaos so it's easy through the cyber warfare to inflict the physical harm, through computer networks.

Methods and means of cyber warfare-

The difference between the methods of cyber warfare and the means of cyber warfare lies in their focus.

Methods of warfare are tactics or strategies to weaken the enemy or gain an advantage during military operations, while means of warfare refer to the weapons or devices used in combat. For instance, the use of ruses in armed conflicts is a lawful and commonly accepted method of warfare. Ruses include using decoys or dummy materials, feigning activity or inactivity, and using camouflage, among many other tactics and techniques. Human shields, misuse of protected emblems, or perfidy are examples of methods of warfare that are prohibited.[6]

By contrast, means of warfare include weapons or devices such as machine guns, tanks, airplanes, submarines, missiles, drones, rifles, and many others. A weapon is "generally understood as that aspect of the system used to cause damage or destruction to objects or injury or death to persons," and characterizes both weapons and weapon systems as means of warfare. Various rules of IHL operationalize the terms weapons, methods, and means. These include, but are not limited to, the weapon review requirement and process, the prohibition on unnecessary suffering, precautions in the attack, and the law of neutrality.[7]

[5] Reza Rafati, "What is Cyber Warfare? Definition, Doctrine, and Real-World Examples" *Cyber Warzone*, March 9, 2026, available at: https://cyberwarzone.com/2026/03/09/what-is-cyber-warfare-definition-doctrine-and-real-world-examples/ (last visited on April 3, 2026).

[6] "Means and Methods of Cyber Warfare" *CCDCOE Cyber Law Toolkit*, available at: https://cyberlaw.ccdcoe.org/wiki/Means_and_methods_of_cyber_warfare (last visited on April 3, 2026).

[7] "Means and Methods of Cyber Warfare" *CCDCOE Cyber Law Toolkit*, available at: https://cyberlaw.ccdcoe.org/wiki/Means_and_methods_of_cyber_warfare (last visited on April 3, 2026).

ISSN: 2582-6433

Methods of cyber warfare-

The method involves the technique to inflict the attack on cyber space of the target nations and following are various notable techniques used earlier in this cyber warfare and can include following[8]-

- Malware: these refers to any software that is designed to cause harm to computer systems or networks. Malware can be used to steal data, destroy files, or gain unauthorized access to systems.
- Phishing: A technique in which attackers use fraudulent emails or messages to trick individuals into divulging sensitive information, such as passwords, credit card numbers, or other personal data.
- Social engineering- it involves the use of psychological manipulation to trick individuals into divulging sensitive information or granting access to computer systems. This can include tactics such as impersonation, pretexting, or baiting.
- Denial-of-Service (DoS) attacks: DoS attacks involve flooding a computer system or network with traffic to overwhelm it and make it unusable.
- Advanced Persistent Threats (APTs): APTs are a type of targeted cyber-attack that are typically carried out over a long period of time, with the goal of gaining access to sensitive data or systems.
- Zero-day exploits: Zero-day exploits are faults in software that are not yet known to the software vendor or security community. Attackers can use these vulnerabilities to gain access to systems or launch attacks without being detected.

Means or types of cyber warfare-

Cyber warfare can be conducted through various means and can include-

- Espionage- it involves the gain the unauthorized economic political or military information by use of cyberdecks.[9]
- Denial of service attacks- it involves overwhelming of websites with fake traffic, making them inaccessible to legitimate users. By targeting websites critical to citizens,

[8] G. Mahmudov, "Cyber Terrorism and Cyber Warfare: Similarities and Differences" *Scientific Journal of the National University of Defense* (2023), available at: https://institute.nvu.bg/sites/default/files/inline-files/2023-2-03-mahmudov.pdf (last visited on April 3, 2026).

[9] "Cyber Espionage" *SentinelOne*, available at: https://www.sentinelone.com/cybersecurity-101/threat-intelligence/cyber-espionage/ (last visited on April 3, 2026).

ISSN: 2582-6433

the military, or researchers, attackers can disrupt essential operations and communication.[10]

- Propaganda- Propaganda attacks aim to influence the beliefs and morale of a target population. These attacks can spread misinformation, expose embarrassing secrets, or fabricate lies to erode public trust in the government
- Economic disruption- it targets financial networks, stock markets, payment systems, and banks and disrupt economic activities by stealing funds or blocking access to essential financial resources.
- Sabotage- use of digital or malware to deliberately destruct, damage or disrupt the enemy's material equipment resource or infrastructure.[11]

Real life example of cyber warfare-

Stuxnet 2010-

This was the first known use of cyber space to create the harm to the neuclear facility of any nation. A sophisticated worm was targeted in the iran's natanz nuclear facility which physically damaged uranium enrichment centrifuges by altering their speed, setting back Iran's nuclear program by years.this attack was attributed to be carried on by the USA and Israel.[12]

Ukrainian power grid attack 2015

Carried on by the Russian based hackers they attacked the power grid remotely and took control of electric substation which caused blackout at massive level affecting thousands of Ukrainian.

Not Petya 2017-

The most devastating attack not Petya to which Russian military agency launched a malware in the Ukrainian tax software update, appeared to be ransomware which spread all across the globe causing 10bn dollar of loss to various companies.[13]

[10] Abhishek Arora "What is Cyber Warfare?" *CloudDefense.AI*, available at: https://www.clouddefense.ai/what-is-cyber-warfare/ (last visited on April 3, 2026).
[11] "Sabotage, n." *Oxford English Dictionary*, available at: https://www.oed.com/dictionary/sabotage_n?tl=true (last visited on April 3, 2026).
[12] Reza Rafati, "Stuxnet: The Cyber Weapon That Changed Warfare" *Cyber Warzone*, March 9, 2026, available at: https://cyberwarzone.com/2026/03/09/stuxnet-the-cyber-weapon-that-changed-warfare/ (last visited on April 3, 2026).
[13] Tibor Moes, "NotPetya: The Most Devastating Cyberattack in History" *SoftwareLab*, available at: https://softwarelab.org/blog/notpetya/ (last visited on April 3, 2026).

ISSN: 2582-6433

Cyber terrorism-

The U.S. Federal Bureau of Investigation (FBI) defines cyberterrorism as any "premeditated, politically motivated attack against information, computer systems, computer programs and data, which results in violence against noncombatant targets by subnational groups or clandestine agents." Per the FBI, a cyberterrorist attack is a type of cybercrime explicitly designed to cause physical harm.[14]

It is an act done by groups or organizations to disrupt violation and terror across the country with political or military motives. Cyberterrorism is simply an act of terrorism by means of cyber space aimed at infiltrating the security of a nation and expanding the network of his terror. Cyberterrorism not only includes an act of damage but also the act of hiring people in their motive that in long-term shall have the adverse effect on that nation for instance various terrorist organization in Pakistan through cyberspace contacts local youth in bordering areas and mislead them towards the terrorism.

So, Cyber terrorism refers to the use of computers, networks, and the internet to carry out terrorist activities. It aims to create fear, disruption, and damage to critical systems such as government, military, or public infrastructure. Cyber terrorism is a form of cybercrime where attackers use digital technologies to threaten or harm national security, public safety, or essential services.[15]

- To create fear and panic among people
- To disrupt critical infrastructure like power, banking, or transport
- To damage government or military systems
- To spread propaganda and influence public opinion

These attacks can take many forms, such as disseminating propaganda, stealing or manipulation of data, or disrupting critical infrastructure To achieve a political or social goal, this is done through intimidating or threatening a government or its citizens.[16]

[14] Rahul Awati, Robert Sheldon "Cyberterrorism" *TechTarget*, available at: https://www.techtarget.com/searchsecurity/definition/cyberterrorism (last visited on April 3, 2026).
[15] "What is Cyber Terrorism?" *GeeksforGeeks*, available at: https://www.geeksforgeeks.org/computer-networks/what-is-cyber-terrorism/ (last visited on April 3, 2026).
[16] Saman Iftikhar, "Cyberterrorism as a Global Threat: A Review on Repercussions and Countermeasures" 10 *PeerJ Computer Science* e1772 (2024), available at: https://pmc.ncbi.nlm.nih.gov/articles/PMC10803091/ (last visited on April 3, 2026).

ISSN: 2582-6433

Characteristics of cyber terrorism- [17]

- **Minimal Resources Required**

  Cyber terrorism activities are less expensive to perform and less dangerous than traditional terrorist activities. Very few resources are required for committing cyber terrorism attacks.

- **Anonymity**

  Terrorists use online nicknames or log on to a website as an unidentified guest user, making it very hard for security agencies and police forces to track down the terrorist's real identity.

- **Enormous**

  The variety and number of targets are enormous. The cyberterrorist could target the computers and computer networks of government, individuals, public utilities, private airlines, etc.

- **Boundaryless**

  Cyberspace is boundary-less. The cyberterrorist can make an attack from a remote location or from multiple remote locations simultaneously. Cyber terrorism can be conducted remotely.

- **Wider Effect**

  Cyber terrorism has the potential to affect directly a larger number of people than traditional terrorist methods, thereby generating greater media coverage, which is ultimately what terrorists want.

- **Greater Potential**

  A. Attacks on electrical power systems, water supply systems, banking, and financial systems.

  B. Access hospital records and change patient blood types.

  C. Report stolen information to others.

Types of cyber terrorism-

- Malware- it is malicious software that gains unauthorized access to computers and networks, and damages or disrupts them with the goal of causing harm to the victim and/or financial gain for the attacker[18]

[17] Sandeep Singh "Characteristics of Cyber Terrorism" *SolutionWeb*, available at: https://www.solutionweb.in/characteristics-of-cyber-terrorism/ (last visited on April 3, 2026).

[18] "What is Malware?" *McAfee*, available at: https://www.mcafee.com/en-us/antivirus/malware.html (last visited

ISSN: 2582-6433

- Phishing- it is an attack disguised as email to trick the recipient into launching malware that collects personal information or does other damage. This is the most common method for cyber terrorists and other criminals to infect the machines and networks of their victims.[19]
- Ransomware- A malicious software that locks victims out of their computer files and blocks other resources, releasing them only after the victims pay a ransom, typically in the form of a cryptocurrency such as Bitcoin.[20]
- Man in the middle attack- A man-in-the-middle attack is like spyware whichin the attacker lurks on the victim's network or computer, tracking and recording all the information that the person accesses or transmits.[21]

Real life incidents-

Shamoon Malware Attack on Saudi Aramco (2012) -A disruptive malware wiped data from about 30,000 computers at Saudi Aramco, one of the world's largest oil companies. The attack replaced files with an image of a burning American flag. It was Suspected to be carried out by Iranian-linked or hacktivist groups with ideological motives to disrupt the economy and create fear in the energy sector.[22]

WannaCry Ransomware Attack (2017)- This global ransomware infected over 200,000 computers in 150 countries, including UK's National Health Service (NHS) hospitals, causing cancelled surgeries and chaos. Uk govt blamed it on north Korea government.[23]

on April 3, 2026).

[19] Cyber Terrorism: What It Is and How It's Evolved "*Maryville University Online*, available at: https://online.maryville.edu/blog/cyber-terrorism/#examples (last visited on April 3, 2026).

[20] Cyber Terrorism: What It Is and How It's Evolved "*Maryville University Online*, available at: https://online.maryville.edu/blog/cyber-terrorism/#examples (last visited on April 3, 2026).

[21] Kurt Baker, "What is a Man in the Middle (MITM) Attack?" *CrowdStrike*, January 17, 2025, available at: https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/man-in-the-middle-mitm-attack/ (last visited on April 3, 2026).

[22] "List of security hacking incidents" *Wikipedia*, available at: https://en.wikipedia.org/wiki/List_of_security_hacking_incidents (last visited on April 3, 2026).

[23] James Coker, "The Top 10 Biggest Cyber-Attacks and Their Impact" *Infosecurity Europe*, August 24, 2023, available at: https://www.infosecurityeurope.com/en-gb/blog/threat-vectors/biggest-cyber-attacks.html (last visited on April 3, 2026).

ISSN: 2582-6433

Cyber terrorism v cyber warfare-

Feature	Cyber Terrorism	Cyber Warfare
Primary Actor	Non-state actors, extremist groups, or lone individuals.	Nation-states, state-sponsored groups, or military units.
Objective	To provoke terror, spread an ideological message, or coerce a government/civilian population.	To achieve strategic, military, or political dominance over another nation.
Target	Often indiscriminate; focuses on civilians, symbolic sites, or critical infrastructure to maximize public fear.	Military assets, government communications, financial systems, and power grids of an enemy state.
Motivation	Religious, political, or social ideologies.	National interest, territorial defense, or geopolitical maneuvering.
Scale of Attack	Generally smaller or more sporadic, though can be high-impact (e.g., hacking a hospital system).	Massive, coordinated, and sustained operations involving significant resources.
Legal Framework	Treated as a **criminal act** under domestic anti-terror laws (e.g., India's IT Act, Section 66F).	Governed by **International Humanitarian Law** (Jus ad bellum) and the laws of armed conflict.

Cyber Warfare V. Cyber Terrorism- a Legal Grey zone

Grey zone refers to those activities that don't fall with the traditional definition of things. In law, grey zones are considered to those ambiguous activities which are not clearly defined or provisioned by the law. It falls within the two-zone white and black where white stands for

ISSN: 2582-6433

those activities which are clearly defined by law and black refers to those which have clearly not defined, in between lies the grey zone and activities which falls within both the ambit are considered as grey zone.

Cyber warfare and terrorism fit within this category because they allow actors states or non state groups to pursue strategic goals through coercive, disruptive, or violent means while deliberately staying below the threshold of open armed conflict, maintaining ambiguity, and avoiding full-scale retaliation.

Cyber warfare includes state-sponsored operations like hacking critical infrastructure data breaches, espionage, ransomware, and disinformation campaigns. These cause economic damage, erode public confidence, and signal capabilities without triggering conventional war responses. Attribution is often challenging due to proxies, false flags, or technical complexity, enabling plausible deniability.[24]

Terrorism employs premeditated violence against civilians or symbolic targets to advance political, ideological, or religious aims. It creates fear, division, and pressure on governments while operating through proxies or loosely affiliated networks, blurring lines between crime and warfare. State-backed terrorism further complicates accountability.

Both exploit legal gaps in international norms, challenge deterrence, and achieve incremental gains—weakening adversaries, influencing behavior, and sowing instability—without crossing into declared hostilities. [25] Currently there lies no legal manual to address this cyber-attack, except for the Tulin manual which is though not legal yet presents for academic purposes the black words of these activities

Conclusion

The evolution of conflict from physical borders to the digital frontier has fundamentally redefined national security. Cyber warfare and cyber terrorism represent a paradigm shift where

[24] Soumya Awasthi, "Grey-Zone Warfare and Cyber Precursor To Conventional Conflict", Observer Research Foundation Middle East, 28 January 2026, available at: https://orfme.org/research/grey-zone-warfare-and-cyber-precursor-to-conventional-conflict/ (last visited on 3 April 2026).
[25] Sachin Tiwari, "The Reality of Cyber Operations in the Grey Zone – The Emerging Geopolitics", The Defence Horizon Journal, 8 September 2022, available at: https://tdhj.org/blog/post/cyber-operations-grey-zone/ (last visited on 3 April 2026).

ISSN: 2582-6433

the strength of a nation is no longer measured solely by its kinetic military might, but by the resilience of its silicon-based infrastructure.

The Grey Zone of remains the greatest challenge for modern jurisprudence. Because digital attacks allow for plausible deniability, they bypass traditional triggers for armed conflict under International Humanitarian Law. This ambiguity creates a vacuum where state and non-state actors can inflict physical-world damage—such as disabling power grids or disrupting healthcare without a single shot being fired.

Ultimately, the distinction between warfare (strategic/state-led) and terrorism (ideological/coercive) is becoming increasingly blurred as states utilize proxy groups to achieve geopolitical ends.