ISSN : 2394-3580 VOLUME - 12 No. : 10, Aug. - 2025

Swadeshi Research Foundation

A MONTHLY JOURNAL OF MULTIDISCIPLINARY RESEARCH

Two Days National Conference on Multidisciplinary Research in
Indian Journalism in the Digital Era : Opportunities and Challenges

Date : 23-24 August, 2025 (Saturday & Sunday)
Venue : ISSMS Jabalpur (M.P.), India

Indian Tech

GLOBAL CERTIFICATION SERVICES

Research Journal SRF Book Publication

ISRS International Scientific Research Solution

Peer Reviewed & Refereed Journal

Indexing & Impact Factor 5.2

Published by :
Swadeshi Research Foundation & Publication
Seva Path, 320 Sanjeevani Nagar,
Veer Sawarkar Ward, Garha, Jabalpur (M.P.) - 482003

CONTENTS

Cyber Warfare and Critical Infrastructure: Legal Challenges in Protecting Civilian Targets

R. Kalaiselvi
Assistant Professor of Law, School of Law, Vistas

INTRODUCTION :- As technology continues to grow it reshapes the modern warfare beyond traditional ones. Although it is a man-made domain, cyberspace is now become a newest domain of warfare as significant as the other domains. This shift in trend calls into the question of whether the existing international laws can effectively extend to the cyber domain. However, the distinctive quality of cyber warfare makes it difficult to seamlessly integrate traditional legal principles. The Artificial Intelligence (AI) and Autonomous Weapon System (AWS) stretches the challenges to International Humanitarian Law with raising alarming concerns on the ethical dilemmas and accountability in the protection of civilian rights. The paper aims to explore the following key points.

- Cyber warfare and its impact on civilian infrastructure
- Challenges to International Humanitarian Law including AI and AWS
- The need for Legal Reform

CYBER WARFARE :- Cyber warfare has turned civilian infrastructure into a strategic target, making digital attacks just as damaging as physical ones. Jeffrey Carr defines cyber warfare as "The art and science of fighting without fighting; of defeating an opponent without spilling their blood."[1]

A series of cyber attacks produced repeated power blackouts in an area over a protracted period of time, there would likely be a loss of confidence in the electric utilities' ability to provide reliable power to businesses and homes. Some of the earliest and likely most effective cyber criminal operations were conducted through distributed denial-of-service (DDoS) attacks. This was followed by widespread efforts at identity theft. During this period cyber crime began serving as a kind of laboratory where malicious payloads and exploits used in cyber warfare could be developed, tested, and refined.

A DDoS attack occurs when many malicious hosts coordinate to flood the target network with large amounts of traffic simultaneously. The attack's objective is to deny service by exhausting the target's resources. These resources can be network band width, computing power, or operating system data structures. To launch a DDoS attack, malicious users first build a network of computers that they will use to produce the volume of traffic needed to deny services to computer users. To create this attack network, attackers discover vulnerable sites or hosts on the network. As the attacker gains access to vulnerable systems, he installs programs or "attack tools," converting the system into a "bot" or "zombie" that can now be remotely controlled by the attacker. Masses of bots or zombies are called "bot nets" or cyber "armies." Since the process for scanning for vulnerable computers can be automated, botnets can be created relatively quickly. Unlike malicious hackers, criminals engaging in cyber crime were (and are) not interested in using viruses to delete files, turn machines off, or even broadcast love for a stripper (as the Melissa virus did). Rather, cyber criminals were seeking to take control of computer systems and use them to send email (i.e., spam), enabling DDoS attacks. Such at tacks have been used, for example, to extort payment from gambling websites by threatening to take them off-line during periods of peak business (e.g., immediately

[1] Carr, J., Inside Cyber Warfare, 2nd ed., O'Reilly Media Inc., 2012, p. 2.

prior to major sporting events like the Super Bowl).[2]

The Love Bug While potential major problems associated with computer systems and networks were hardly un known in the 1990s (e.g., the Y2K scare), arguably it was not until 2000 that the power of computer viruses was revealed. That year the Love Bug virus was set loose by a pair of hackers in the Philippines. The virus successfully attacked roughly 55 million computers.[3] The malware was sent to a computer user as an attachment to an email with the text "ILOVEYOU" in the subject line. If the recipient opened the attachment, the worm embedded in it sent a copy of itself to everyone in the user's ad dress book. The worm also made a number of malicious changes to the user's system, overwriting files with a copy of itself. Only computers with the Microsoft Windows operating system were vulnerable. However, reflecting the risks associated with a largely global computing monoculture, estimates of the damage wrought by the Love Bug ran as high as $15 billion.[4]

Critical infrastructure functionality is growing progressively more vulnerable to cyber attack, given its increasing reliance on information systems in general and access to the Internet in particular. Secretary of Defense Leon Panetta is among those sounding the alarm, declaring that: [W]hen it comes to national security, I think this [i.e., cyber warfare] represents the battleground for the future. I've often said that I think the potential for the next Pearl Harbor could very well be a cyber attack. If you have a cyber attack that brings down our power grid system, brings down our financial systems, brings down our government systems, you could paralyze this country[5]. Chinese military officers see the cyber threat in a similar manner, to include linking cyber weapons with nuclear weapons. For example, an essay by two People's Liberation Army (PLA) scholars, Senior Colonel Ye Zheng and his colleague Zhao Baoxian, in China Youth Daily stresses the importance of China's cyber warfare capabilities, concluding that "Just as nuclear warfare was the strategic war of the industrial era, cyber-warfare has become the strategic war of the information era, and this has become a form of battle that is massively destructive and concerns the life and death of nations."[6]

Further they added Cyberware is an entirely new mode of battle that is invisible and silent, and it is active not only in wars and conflicts, but also flares in the everyday political, economic, military, cultural and scientific activities.[7]

CIVILIAN INFRASTRUCTURE IN THE CYBER BATTLEFIELD :- Cyber attacks on the critical civilian infrastructures like power grids, transportation networks, communication networks and financial institutions could cripple the entire segments of the society. For example any attack on the vital infrastructure such as power grid or hospital services could easily trigger a catastrophic impact, spreading widespread chaos on safety and economic stability.

On April 4, 2024, the North American Electric Reliability Corporation (NERC) reported that the number of points in the US power grids that are vulnerable to cyber attacks is increasing at

---

[2] Andress et al., Cyber Warfare, p. 176.

[3] 'The Love Bug Virus: A Hacker's Tale' (Wired, 4 May 2010) https://www.wired.com/2010/05/0504i-love-you-virus/ accessed 04 March 2025

[4] Joseph S Nye Jr, 'Power and National Security in Cyberspace' in Kristin M Lord and Travis Sharp (eds), *America's Cyber Future: Security and Prosperity in the Information Age* (Center for a New American Security 2011) 13.

[5] United Press International, 'Cybersecurity "battleground of the future"' (10 February 2011) http://www.upi.com/Top_News/US/2011/02/10/Cybersecurity-battleground-of-the-future/UPI-62911297371939/ accessed 03 March 2025

[6] Chris Buckley, 'China PLA officers call internet key battleground' (3 June 2011) https://www.reuters.com/article/technology/china-pla-officers-call-internet-key-battleground-idUSTRE7520OV/ accessed 04 March 2025

[7] Ibid

a rate of approximately 60 per day. In 2022 the number of susceptible points grew from 21,000 to 22,000. Now it is between 23-24,000.[8]

INTERNATIONAL HUMANITARIAN LAW – IHL :- International humanitarian law (IHL) is a set of rules that seeks, for humanitarian reasons, to limit the effects of armed conflict. It came in to the existence in the form of Hague and the Geneva Conventions. It protects persons who are not, or are no longer, directly or actively participating in hostilities, and imposes limits on the means and methods of warfare. IHL is also known as "the law of war" or "the law of armed conflict". Persons protected by IHL are entitled to respect for their lives, their dignity, and their physical and mental integrity.

International humanitarian law is a set of rules that seek to limit the effects of armed conflict on people, including civilians, persons who are not or no longer participating in the conflict and even those who still are, such as combatants. To achieve this objective, international humanitarian law covers two areas: the protection of persons that is Jus ad Bellum ("Right to War"); and restrictions on the means and the methods of warfare that is Jus in Bello ("Law in War").

LEGAL COMPLEXITIES IN CYBER WARFARE :- The current IHL regime does not specifically address cyber weapons in the way it has banned other conventional weapons, biological weapons and chemical weapons. IHL is an adaptive body of law, which can be deduced from Article 36 of Additional Protocol I to the Geneva Conventions ("API"). The International Court of Justice's ("ICJ") Advisory Opinion on the Legality of the Threat or Use of Nuclear Weapons supports this notion, where the court affirmed that the rules and principles of IHL apply to "all forms of warfare and to all kinds of weapons, including those of the future"[9]. Therefore, as a new means and method of warfare, States are required to conduct a legal review of all "cyber weapons" to ensure compliance with IHL before using them in operations.

IHL aims to minimize human suffering in armed conflict. However, its adaptation to cyber warfare remains a major challenge. The legal complexities in Cyber Warfare differ from the traditional warfare. International humanitarian law (IHL), which consists of rules that seek to limit the effects of armed conflict for humanitarian concerns, has been applied to cyber warfare in an attempt to fill this gap, but legal gray areas have emerged, as cyber operations often do not raise to the level of armed conflict.[10]

The technology evolved so fast that the existing laws cannot keep pace with the technology. The cyber space became the fifth domain after the sea, land, and space. The information that flowed through the cyber space was now being manipulated, stolen, disseminated during the time of peace as well as during military combat to gain an advantage over the adversary. The rise of new form of warfare resulted into blurring the lines between the wartime and the peacetime. These tactics were employed during the time of peace as well to steal the sensitive information and render the victim of the theft defenseless in the event of the theft of the sensitive data. The events of this theft were not restricted to the information that was military in the nature. As the cyber space grew leaps and bound the number of the cyber actors multiplied.

[8] Kierney, Laila, 'US Electric Grid Growing More Vulnerable To Cyberattacks, Regulator Says,' Reuters, April 4, 2024, https://www.reuters.com/technology/cybersecurity/us-electric-grid-growing-more-vulnerable-cyberattacks-regulator-says-2024-04-04 accessed 01.03.2025

[9] International Court of Justice, Legality of the threat or the use of nuclear weapons, Advisory Opinion, 8 July 1996, para. 86.

[10] **International Committee of the Red Cross,** *Cyber Warfare and International Humanitarian Law* (2013) https://www.icrc.org/en/doc/assets/files/2013/130621-cyberwarfare-q-and-a-eng.pdf accessed 03.03.2025

However, given the unique nature of the cyber space that transcends the physical boundaries and the anonymity of the actors operating in the cyber space it could not be said and concluded if the acts were perpetrated from within the jurisdiction of the state or outside the jurisdiction of the state

Plethora of questions that presented here such as whether there was an attack? What was the nature of the attack? Even if there was an attack no kinetic weapon was used. Can use of cyber malware be equated with the use of kinetic weapon such as a missile or gun? Since, there was no use of the traditional kinetic weapon during the alleged attack can it be termed as an armed attack. There was no arms or ammunition involved in the incident so it cannot be termed as an armed attack. But the effects generated at the site of the attack were that of the weapon that was kinetic in nature. Can it be said that there was use of force and the violation of Article 2(4) of the UN Charter. It prohibits the threat or use of force and calls on all Members to respect the sovereignty, territorial integrity and political independence of other States

CHOOSING WEAPONS AND METHOD OF WARFARE :- The leadership of the attacked community, on the other hand, needs to take feasible steps to minimise the anticipated harm towards its own civilian population, most notably by not situating military objects close to civilian objects. When several targets serve the same military purpose, the attacker should choose the target which is expected to cause the least danger to the civilians and their property. A military operation has to be cancelled if they foresee an excessive harm to the civilians.

AI POWERED CYBER ATTACKS :- AI-generated attacks refer to cyber threats that leverage artificial intelligence and natural language processing to deceive and compromise individuals, organizations, and systems. Threat actors with malicious intent use AI-powered models and tools to generate convincing phishing emails, social engineering messages, and other AI-generated text that bypass traditional security measures. These attacks are becoming increasingly sophisticated, mimicking the language and style of legitimate emails to trick users into disclosing sensitive information or committing fraudulent activities.

AI-generated attacks employ various methods to exploit vulnerabilities, deceive systems, and cause damage or compromise trust.[11] Two common attack methods used in these attacks are input attacks and poisoning attacks. Input attacks involve manipulating the input data that is fed into AI systems. The goal is to deceive the system by introducing malicious inputs that result in unintended or harmful actions. For example, an AI-generated attack could cause a self-driving car to ignore stop signs or take incorrect steps by feeding it manipulated sensor data.

Poisoning attacks, on the other hand, involve maliciously manipulating the training data used by AI models. By injecting false or misleading information, attackers can bias the model towards making wrong predictions or behaving unexpectedly. For instance, an AI-generated attack might manipulate the training dataset of a content filter to allow inappropriate content to bypass detection.

These attack methods can cause significant damage and have far-reaching consequences. A successful input attack on an autonomous vehicle can jeopardize the safety of passengers and pedestrians, leading to accidents and injury. Similarly, a poisoning attack on a content filter can result in disseminating harmful or inappropriate content that goes undetected, potentially harming users or degrading online spaces.

Furthermore, AI-generated attacks can erode trust in AI systems and undermine the integrity of those systems. By exploiting their

[11] MixMode, 'What are AI Generated Attacks?' (MixMode) https://mixmode.ai/what-is/ai-generated-attacks/ accessed 5 March 2025.

vulnerabilities, attackers can doubt the reliability, safety, and effectiveness of AI-enabled tools and techniques, leading to a loss of confidence among users and cybersecurity professionals.

These examples highlight the potential threats and risks associated with AI-generated attacks and emphasize the importance of implementing robust security measures and continuously monitoring and updating AI models to defend against such attacks.

AUTONOMOUS WEAPON SYSTEM IN CYBER WARFARE :- Autonomous Weapon Systems (AWSs) are perhaps one of the most contentious forms of technology. An AWS, in its fully developed form, can act independently of humans to kill and destroy. Whether it is ethical to use smart (i.e. autonomous) weapon systems in war is a big question before us. The fear is that an AWS is indiscriminate in who and what it targets. Nevertheless. it is accepted that there are certain targets that are legitimate to attack, but also that there are illegitimate targets.

CONCLUSION :- To address the complexities of cyber warfare and eliminate ambiguity, it is essential to establish a clear consensus on its fundamental concepts and related terminologies. Defining these terms will enhance the applicability of laws and foster greater cooperation among member states. Information sharing must be facilitated to ensure accessibility, aiding in the deterrence of cyber threats originating from neutral territories. Strengthening collaboration in resource sharing, skill development, and knowledge exchange is crucial for safeguarding critical national infrastructure and enhancing resilience. The development of advanced attribution mechanisms is necessary to identify perpetrators of cyber-attacks effectively. Additionally, early warning systems must be implemented to counter threats proactively. Establishing a specialized international expert team, similar to CERT and ICS-CERT, would enhance investigative and prosecutorial efforts. Strict measures should be in place to hold violators accountable, ensuring the stability of cyberspace. Moreover, raising awareness about safe online practices will promote a secure and inclusive digital environment.

Rather than viewing cyber arsenals as sophisticated weapons for gaining an advantage over adversaries, states should collectively recognize cyber warfare as a threat to global peace, security, and order. In an era where information dominates, the focus should shift from exploitation to cooperation, fostering information sharing among nations. Such collaboration can channel intellectual resources toward innovation, driving humanity toward progress and well-being. Cyber warfare is a reality, and regardless of intent, everyone is an unwitting participant in this digital battlefield

REFERENCES :-

1. Carr, J., Inside Cyber Warfare, 2nd ed., O'Reilly Media Inc., 2012, p. 2.
2. Andress et al., Cyber Warfare, p. 176.
3. 'The Love Bug Virus: A Hacker's Tale' (Wired, 4 May 2010) https://www.wired.com/2010/05/0504i-love-you-virus/ accessed 04 March 2025
4. Joseph S Nye Jr, 'Power and National Security in Cyberspace' in Kristin M Lord and Travis Sharp (eds), America's Cyber Future: Security and Prosperity in the Information Age (Center for a New American Security 2011) 13.
5. United Press International, 'Cybersecurity "battleground of the future"' (10 February 2011) http://www.upi.com/Top_News/US/2011/02/10/Cybersecurity-battleground-of-the-future/UPI-62911297371939/ accessed 03 March 2025.