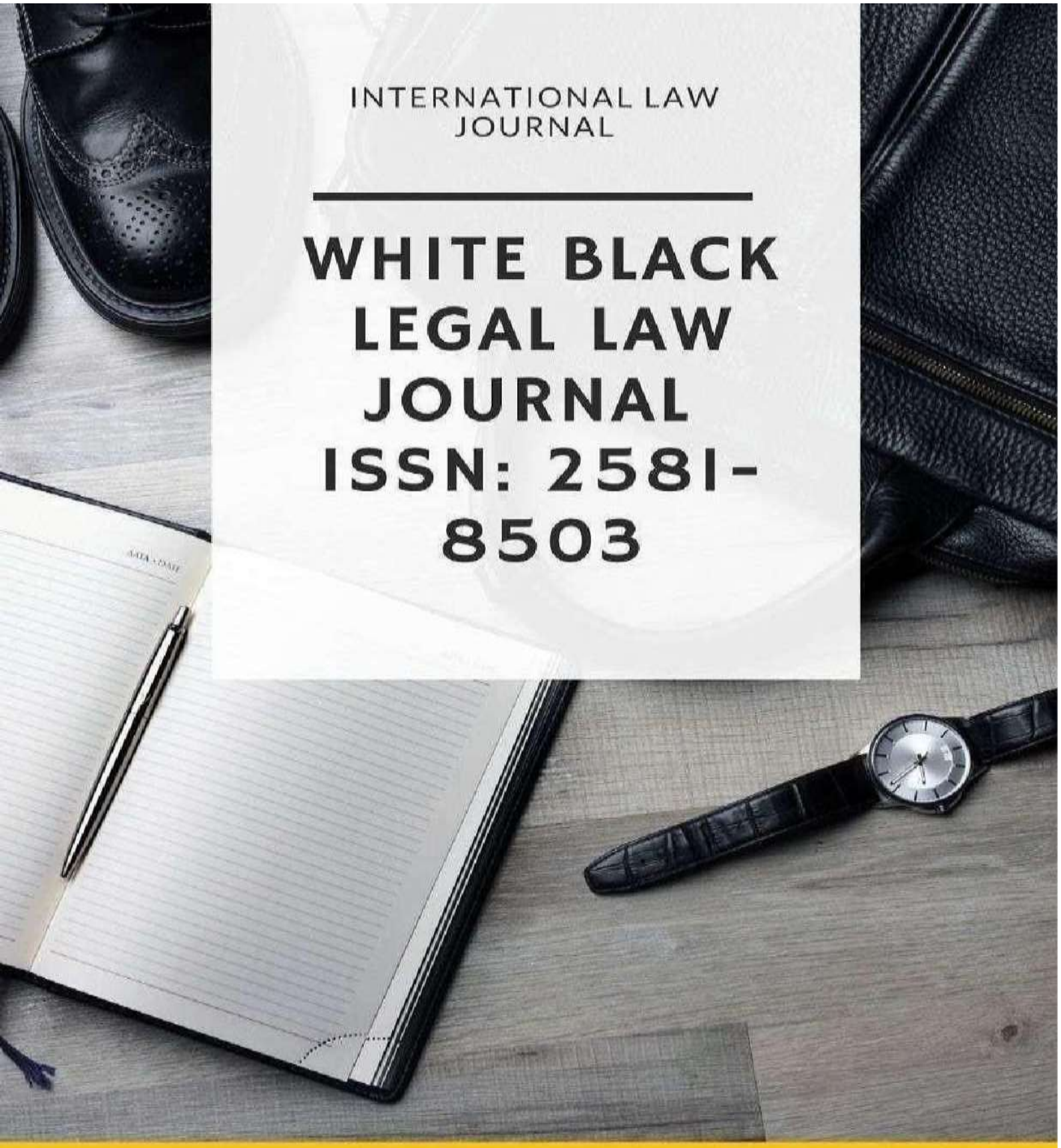

INTERNATIONAL LAW JOURNAL

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

No part of this publication may be reproduced or copied in any form by any means without prior written permission of Editor-in-chief of White Black Legal – The Law Journal. The Editorial Team of White Black Legal holds the copyright to all articles contributed to this publication. The views expressed in this publication are purely personal opinions of the authors and do not reflect the views of the Editorial Team of White Black Legal. Though all efforts are made to ensure the accuracy and correctness of the information published, White Black Legal shall not be responsible for any errors caused due to oversight or otherwise.

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 provide dedicated 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 2 | Sep 2025 ISSN: 2581-8503

PROTECTION OF CIVILIANS IN CYBERSPACE: A LEGAL ASSESSMENT OF CYBER WARFARE

AUTHORED BY - DR. RAMESH PARAJULI[1]

Abstract

Cyber warfare is a newly emerged form of warfare not explicitly indoctrinated by international legal theory. Assessing the humanitarian impact of cyber warfare within the framework of international law is a complex and evolving field. A legal assessment of cyber warfare involves examining the application of existing international legal norms to use cyber aptness in armed conflicts and considering the implications for civilians and civilian infrastructure. The application of legal principles to cyber operations is challenging but essential to protect civilians and minimize harm during armed conflicts. Legal experts, governments, and international organizations continue to work on developing and clarifying the legal framework for cyber warfare. The international community has yet to reach a concession on how international humanitarian law applies in this new form of conflict. In studying cyber operations and their respective legal regimes, one should consider the importance of the contexts in which these operations occur. In practice, cyber operations do not unfold from and in repudiations. Two situations must be distinguished: whether cyber operations occur in peacetime or during an ongoing armed conflict. Subsequently, whether the cyber operations reach a threshold that changes the situation can be analyzed, transforming the applicable legal framework. This paper will be based on the cyber attack and its impact on humanity. Therefore, I tried to explore how international humanitarian law views the cyber warfare and its impact on humanity.

Keywords: Cyber Warfare, International Humanitarian Law, Emerging issues in International legal order

[1] Assistant Professor at Faculty of Law, Tribhuvan University, Nepal.

Background

International Humanitarian Law (hereafter IHL) limits how limiting or prohibiting certain means and methods of warfare is conducting hostilities. Art 22 of the Hague Regulations 1907 states, "The right of belligerents to adopt means and injure the enemy is not unlimited." The norms of IHL limit or prohibit the use of specific means and methods of weaponry. The law of weaponry contains both general principles and specific rules[2]. The principle refers to the prohibition of weapons that are by nature indiscriminate or cause unnecessary suffering, while the specific rules refer to the limitation or prohibition of certain means and methods of warfare. Cyber operations by its nature fall into specific rules of law and weaponry. It is said that state-sponsored cyber operations, namely recourse to cyber means by one state generally against another, are usually labeled cyber-warfare[3]. For further understanding, it is constructed from the prefix 'cyber,' which refers to the relationship between the internet and computer technology, and the term 'war.' Put simply, it amounts to war that involves employing the internet and computer technology[4]. In the case of IHL, the term ‘war’ or ‘warfare’ can be defined as an armed conflict between States or non-state actors to impose by force a determined will. Its view is that the current UN Charter and the existing law of armed conflict, as well as the basic principles of International Humanitarian law that relate to war and the use of threat of force, all still apply to cyberspace, specifically, the no use of force and peaceful settlement of international disputes decrees as well as the principles of distinction and proportionality[5]. It stated the expression 'cyber warfare' is also narrower than ‘cyber operations’ and technically refers only to the conduct of hostilities in armed conflict using cyber technologies.

From a legal point of view, it is essential to distinguish between cyber warfare in the sense of cyber operations conducted in the context of armed conflicts within the meaning of IHL. IHL could only be attributable, if cyber operations are orderly and conducted in the context of and related to an armed conflict[6]. Thus, it should be fairly uncontroversial that when cyber operations are conducted in the context of an ongoing armed conflict, they are subjugated by the same IHL rules as that conflict. In military doctrine, the state’s cyber operations fall within

[2] Dan-Iulian Voitasec, *MEANS AND METHODS OF CYBER WARFARE*, CHALLENGES OF THE KNOWLEDGE SOCIETY 555 (2016).
[3] FRANÇOIS DELERUE, CYBER OPERATIONS AND INTERNATIONAL LAW (2020).
[4] Johann-Christoph Woltag, *Cyber Warfare: Military Cross-Border Computer Network Operations under International Law* (2014).
[5] Li Zhang, *A Chinese Perspective on Cyber War*, 94 INTERNATIONAL REVIEW OF THE RED CROSS 801 (2012).
[6] Cordula Droege, *Get off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians*, 94 INTERNATIONAL REVIEW OF THE RED CROSS 533 (2012).

the broader category of information operations[7]. what characterizes cyber operations and makes them unique, however, is that information can also be used to inflict disruption or damage on an adversary[8].

“"information operations' have been defined as "the integrated apply of the essential potentialities of electronic warfare, computer network operations, psychological operations, military deception, and operations security in concert with specified supporting and related capabilities, to influence, disrupt, corrupt, or usurp adversarial human and automated decision making while protecting our own"[9].

The US DoD *Dictionary of Military and Associated Terms* defines ‘cyberspace operations as ‘[t] he employment of cyberspace potentialities where the primary aim is to achieve objectives in or through cyberspace[10]. The *Tallinn Manual on the International Law Applicable to Cyber Warfare*, published in 2013 by a Group of Experts at the invitation of NATO’s CCDCOE,[11] slightly modifies this language. It defines cyber operations as ‘the employment of cyber capabilities with the primary purpose of achieving objectives in or by the use of cyberspace[12]. More descriptively, the International Committee of the Red Cross (ICRC)’s definition refers to ‘operations against or via a computer or a computer system through a data stream. Such operations can aim to do different things, for instance, to infiltrate a system and collect, export, destroy, change, or encrypt data or to trigger, alter, or otherwise manipulate processes controlled by the infiltrated computer system. Thomas Wingfield, in his book *The Law of Information Conflict: National Security Law in Cyberspace,* gives a more plain language definition. "Cyberspace is not a physical place - it defies measurement in any physical dimension or time-space continuum. It is a shorthand term that refers to the environment created by the confluence of cooperative networks of computers, information systems, and telecommunication infrastructures commonly referred to as the World Wide Web[13]. In a Detail form Kevin Coleman, a Senior Fellow and Strategic Management Consultant at the Technolytics Institute, an independent executive think tank, defined "cyber war" as "a conflict

[7] The Oxford Compact English Dictionary, (2003). Oxford: Oxford University Press, p 268.
[8] Daniel J Ryan et al., *International Cyberlaw: A Normative Approach*, 42 GEO. J. INT’L L. 1161 (2010).
[9] *Id.*
[10] US DoD, *Dictionary of Military and Associated Terms*, p 70.
[11] The CCDCOE is a think-tank based in Tallinn that was created after the 2008 DDoS attacks against the Baltic state.
[12] Tallinn Manual, p 76.
[13] Thomas C Wingfield, *The Law of Information Conflict: National Security Law in Cyberspace*, (NO TITLE) (2000).

that uses hostile, illegal transactions or attacks on computers and networks in an effort to disrupt communications and other pieces of infrastructure as a mechanism to inflict economic harm or upset defenses.

The particular definition of the word itself is not a suffix to determine the applicability of law in cyber operations. One of the most challenging aspects of cyber war is the concept of attribution. This refers to the difficulty of ascertaining who was responsible for a particular cyber action. This might be the logical target for any retaliatory action the victim might wish to undertake, whether in the cyber or physical domain. Cyber attribution includes determining the cyber attack's originating network address, which is a relatively straightforward process from a technical standpoint. A Cyber attack, as defined above, that is attributable to one state and directed against another state triggers the applicability of the IHL of IACs. Suppose an armed group that is not under the control of a state against a state or another armed group launches such an attack. In that case, IHL only applies if the group has a sufficient degree of organization and the amount of violence is sufficiently high. It is accepted that Rule 20 of the Tallinn Manual, in which '[c]yber operations executed in the context of an armed conflict are subject to the law of armed conflict,' whether or not the operations amount to resort to armed force themselves[14]. The Manual, however, fails to explain what 'in the context of ' means, and the commentary limits itself to note that it could refer to either the fact that the operations are conducted by a belligerent against an adversary or that they are carried out to contribute to a belligerent's military effort[15]. This write up shall be followed by cyber operation and its impact to the humanity, applicable international legal norms, potential use of means and method of cyberwarfare, cyber attribution and state responsibility with the concluding remarks to assess the protection of civilians in cyber space. The researcher will rely on doctrinal and analytical method within the existing literature available in the primary and secondary sources including experts' opinion, institutional reports and data available on the government websites. The researcher limits this research on how the cyber operation has impacted the civilian and civilian infrastructure and applicable legal norms from humanitarian law perspectives.

[14] MICHAEL N SCHMITT, TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (2013).
[15] Tallinn Manual, p 76, *supra* note 11.

Cyber Operation and Humanitarian Impact

Information technology increasingly affects all aspects of human life. It is used to control not only data but the physical world, too. The interconnected nature of the internet and the high dependence of modern societies on computers make it difficult but possible to respect the normal rules on the conduct of hostilities in cyber attacks[16] The main problem with applying the rule of IHL is that the military and civilians in most countries use the same internet and communication software and most of their components. The principle of distinction, as per the international practices, requires that parties to a conflict always differentiate between civilians and combatants and between civilian objects and military objectives[17] In the words of the ICJ, it is a cardinal principle of IHL. Attacks may only be conducted against combatants or military objectives. In planning and carrying out cyber operations, the only targets permissible under IHL are military objectives, such as computers or computer systems that effectively contribute to concrete military operations. Attacks via cyberspace may not be directed against computer systems used in purely civilian installations.

According to Article 52(3) of Additional Protocol I, objects generally dedicated to civilian purposes shall be presumed not to be used to contribute to military action effectively. So, for instance, if some susceptible civilian infrastructure, such as most chemical plants, relies on a closed computer network, this network must be presumed to be civilian. Article 52(2) clarifies that there must be a close nexus between the potential target and military action. The term 'military action' denotes the enemy's war-fighting capabilities. This nexus is established through the four criteria of nature, location, purpose, and use. Nature refers to the intrinsic character of an object, such as a weapon. Objects that are not military in nature may also contribute effectively to military action under their particular location, purpose, or present use. As said, the fact that most cyberspace can be considered dual use will likely make it difficult to separate military from civilian infrastructure. However, even where military and civilian infrastructure can still be separated and distinguished, another risk is that attacks will be

[16] MARCO SASSÒLI, INTERNATIONAL HUMANITARIAN LAW: RULES, CONTROVERSIES, AND SOLUTIONS TO PROBLEMS ARISING IN WARFARE (2019).

[17] Eloisa Newalsing, *Jean-Marie Henckaerts and Louise Doswald-Beck (Eds.), Customary International Humanitarian Law, Geneva and Cambridge, International Committee of the Red Cross and Cambridge University Press (2005), 2 Volumes, ISBN 9780521539258, 4,411 Pp.,£ 320.00 (Boxed Set, Hb); Volume I Available Separately, ISBN 9780521005289, 621 Pp.,£ 32.00 (Pb).*, 21 LEIDEN JOURNAL OF INTERNATIONAL LAW 255 (2008).

indiscriminate because of the interconnectedness of cyberspace[18]. Cyberspace consists of innumerable interwoven computer systems across the world. Even if military computer systems are separate from civilian ones, they are often interconnected with commercial civilian systems and rely on them in whole or part. Thus, it might well be absurd to discharge a cyber attack on military infrastructure and restrain the attack or its effects to just that military objective. Viruses and worms are examples of methods of computer network attack that could fall into this category if their creators do not limit their effects. The use of a worm that reflects itself and cannot be under control, and might therefore cause considerable catastrophic situation to civilian infrastructure, would be a violation of IHL Whether a cyber-attack respects the proportionality rule requires foresight into its actual effect due to the interconnectivity of computer networks[19]. The principle of proportionality is formulated in Article 51(5b) of Additional Protocol I, which reflects customary international law[20]. An attack is prohibited if it 'may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated'[21]. Some Computer Network Attack (CNA-style) Offensive Cyber Operations (OCOs) provide insight into the emerging customary practice of states and related emerging norms regarding this most serious type of hostile cyber operation. Consciously or unconsciously, early cyber actors act as the early norm leaders as they help establish customary practices for hostile cyberspace operations. Many small CNA-style operations involve Distributed Denial of Service (DDoS) attacks to degrade website access, such as the Code Red attack in 2001, which involved malware that launched a DDoS attack against White House computers[22]. It is believed that approximately 100 million to 150 million botnets are utilized to conduct these frequent DDoS attacks[23]. However, there are few examples of major OCOs. Some major cases are summarized to evaluate the norms and contemporary state practice of OCOs: the purported attacks on a Siberian gas pipeline in 1982, the DDoS attacks on Estonia in 2007, the Israeli Operation Orchard attacks on Syria in 2007, the attacks on Georgia in 2008, the notorious Stuxnet attack on Iran disclosed in 2010, the Shamoon virus attack on Saudi Aramco in 2012, North Korea's attack on Sony Corp. in 2014, and the Russian

[18] Knut Dörmann, *Applicability of the Additional Protocols to Computer Network Attacks*, 76 IN COMPUTER NETWORK ATTACK AND INTERNATIONAL LAW: WAR STUDIES (2004).
[19] SASSÒLI, *supra* note 15.
[20] Newalsing, *supra* note 16.
[21] Droege, *supra* note 5.
[22] CHRISTOPHER WHYTE & BRIAN MAZANEC, UNDERSTANDING CYBER-WARFARE: POLITICS, POLICY AND STRATEGY (2023).
[23] *Id.*

attack on Ukrainian power utilities in 2015[24].

Most of the cyber attacks collectively provide some insight into the emergence of international norms through the customary practice of OCOs. There are three main conclusions from the attacks. First off, the bulk (seven of the nine assaults) was directed at civilian targets, demonstrating the lack of a norm restricting targeting to overtly military targets or aims. Second, assaults that did target just military targets were thought to have been carried out by Western countries (Israel and the United States)[25]. According to whatever country is associated with it, there may be rivalry and, in certain cases, more lenient standards surrounding OCOs. This is in line with the anticipated atmosphere of competition during the early stages of norm development. Third, current OCO experience may be lot better. Cyber-attacks have not yet been known to cause any lives or casualties, although they have caused physical harm to some strategically important objects.

The cyber operations against Estonia in 2007 disrupted the state in a way that dangerously affected its operations but did not jeopardize its survival. This example has been viewed as a possible case of recourse to prohibited use of force; however, such a position was quickly ruled out. It must be noted nonetheless that it is too early to determine if such reluctance amounts to a continuous State practice or is merely a nascent custom. Stuxnet stood out as a new kind of weapon in that it was designed to cause physical damage via cyber means. Its makers wanted it to damage targets in the real world, but only through action on digital networks. This was novel enough. But what really distinguished Stuxnet from traditional weapons was how small its physical impact was, especially in light of the intense stakes[26]. The target was a nuclear bomb-making program that was already the target of diplomatic efforts and economic sanctions. Stuxnet only broke nuclear centrifuges, which Iran had illegally obtained to conduct illicit research. Moreover, it neither hurt nor killed anyone. In comparison, when Israel attempted to obstruct Iraqi nuclear research in 1981, its forces dropped sixteen 2,000-pound bombs on a research site during "Operation Opera," leveling it and killing eleven soldiers and civilians[27]. On May 7, 2021, the Colonial Pipeline, the largest refined products pipeline in the

[24] *Id.*
[25] *Id.*
[26] Colin H Kahl, *An Israeli Attack against Iran Would Backfire—Just like Israel's 1981 Strike on Iraq'*, 2 WASHINGTON POST (2012).
[27] *Id.*

United States, was targeted by a ransomware attack that encrypted critical infrastructure data[28]. This significant incident resulted in considerable fuel shortages and rising prices. In a controversial decision, Colonial Pipeline opted to pay the ransom of 75 Bitcoin (approximately $4.4 million at the time) in order to quickly regain access to their systems.

Cyber Operation and International Law

Cyberspace is a fictional territory based on real and tangible infrastructures. Computer networks and their components, which constitute the physical architecture of cyberspace and the internet, are real and are located within the territorial sovereignty of States. The question then arises: Does state territorial sovereignty extend to computer networks? In its 2013 report, the UNGGE, appointed by the UN General Assembly[29], noted that State sovereignty and international legal norms and principles derived from sovereignty apply to State conduct of ICT-related activities and to their jurisdiction over ICT infrastructure within their territory[30]. State-sponsored cyber operations can violate the territorial sovereignty of the targeted state. Territorial sovereignty grants states full and exclusive authority over their land, territory, and appurtenances, including internal waters, territorial seas, archipelagic waters, the airspace above, and subsoil below.

The equal sovereignty of States has been reaffirmed by the ICJ, which qualified States as 'political entities, equal in law, similar in form, and [. . .] direct subjects of international law[31]. A State has territorial jurisdiction over the areas under its territorial sovereignty and extraterritorial jurisdiction over natural or judicial persons with its nationality and its registered ships, aircraft, and spacecraft[32]. In light of this, a State's jurisdiction extends to cover cyber infrastructures that are present on its land, in its territorial sea, in its archipelagic waterways, in its airspace, on board ships flying its flag, and onboard aircraft and satellites that are registered in the State.

[28] Jack Beerman et al., *A Review of Colonial Pipeline Ransomware Attack*, *in* 2023 IEEE/ACM 23RD INTERNATIONAL SYMPOSIUM ON CLUSTER, CLOUD AND INTERNET COMPUTING WORKSHOPS (CCGRIDW) 8 (2023), https://ieeexplore.ieee.org/document/10181159/ (last visited Jan 20, 2025).
[29] OLIVIER CORTEN, THE LAW AGAINST WAR: THE PROHIBITION ON THE USE OF FORCE IN CONTEMPORARY INTERNATIONAL LAW (2021).
[30] Jason Barkham, *Information Warfare and International Law on the Use of Force*, 34 NYUJ INT'L L. & POL. 57 (2001).
[31] NICARAGUA (MERITS) (N 18) 106–111, PARAS 202–209., 2.
[32] SCHMITT, *supra* note 13.

The issues of which cyber operations linked to armed conflicts constitute attacks within the meaning of IHL is what is most often discussed in the jus in Bello. The Tallinn Manual defines cyber attacks as offensive or defensive cyber operations via its reasonably conventional system to cause injury or death to persons or damage or destruction to objects[33]. It explains that Violence against a target distinguishes attacks from other military operations, and nonviolent operations, such as psychological cyber operations or cyber espionage, do not qualify as attacks[34]. The rules for protecting civilians from the effects of hostilities, in particular the proportionality rule and the obligation to take practical precautions, apply to cyber operations that aim to disrupt or incapacitate an adversary's computer-controlled weapons systems, logistic supply networks, or communications networks. Cyber operations may be employed during an existing traditional international armed conflict as 'force multipliers.' The definition of 'cyber war' contained in a 2010 Report by the Italian Parliamentary Committee for the Security of the Republic, for instance, describes it as a proper conflict scenario between nations, fought by systematically destroying critical protection defenses of the adversary's security, or through the disruption or shutting down of strategic communication networks, *and the integration of such activities with the properly belligerent one*[35]'. An example of this scenario is the 2008 armed conflict between Georgia and the Russian Federation, where Georgia's governmental and media websites were taken off-line or vandalized during the initial phases of the conflict allegedly by Russian hackers, thus affecting Georgia's ability to communicate and possibly also the operability of its armed forces. Russia's responsibility, however, has yet to be conclusively established.

The high contracting Party is responsible for determining whether using a new weapon, means, or method of warfare would be prohibited in some or all circumstances by the Protocol or any other provision of international law that the high contracting party is subject to. Cyber operations can also occur during an ongoing armed conflict. In this case, the pre-existing armed conflict will have rendered the law of armed conflict applicable to cyber operations occurring among belligerents. For example, during the 2008 Russo-Georgian War, Georgia faced several cyber attacks allegedly conducted or sponsored by Russia[36]. The actual armed conflict between

[33] COPASIR, (7 JULY 2010). RELAZIONE SULLE POSSIBILI IMPLICAZIONI E MINACCE PER LA SICUREZZA NAZIONALE DERIVANTI DALL'UTILIZZO DELLO SPAZIO CIBERNETICO, DOC XXXIV, NO 4, P 17.
[34] Tallinn Manual, p 76., *supra* note 11.
[35] COPASIR, (7 JULY 2010). RELAZIONE SULLE POSSIBILI IMPLICAZIONI E MINACCE PER LA SICUREZZA NAZIONALE DERIVANTI DALL'UTILIZZO DELLO SPAZIO CIBERNETICO, DOC XXXIV, NO 4, P 17, *supra* note 32.
[36] Markoff, John. (13 August 2008). 'Before the Gunfire, Cyber attacks'. The New York Times.

the two belligerents triggered the applicability of the law of armed conflict, which applies to cyber operations even if they do not qualify as a cyber-armed conflict.

International Humanitarian Law Applicable to Cyber Attacks

Modern International Humanitarian Law (IHL) attempts to govern conduct during war. Current IHL, often referred to as *jus in Bello*, embodies a mixture of treaties, customs, and foundational principles. *The jus in Bello* tradition seeks to minimize atrocities during armed conflicts. The *jus ad bellum* tradition, or the war law, complements *jus in Bello.* Whereas *jus in Bello* governs conduct once armed conflict begins, *jus ad bellum* governs nations' conduct, leading to the initiation of armed conflict. *Jus ad bellum* attempts to reduce the need for war. The terms *law of war* and *law of armed conflict* refer to the combination of *jus ad bellum* and *Jus in Bello*[37]. With the growth of cyber capabilities and cyber dependencies, experts have argued the efficacy and applicability of traditional IHL with respect to cyber-warfare. Much of the discussions regarding cyber-war centers on which cyber-attacks might constitute armed attacks in the context of IHL. The classification of an action as an armed attack, under IHL, brings with it the right of the victim state to self-defense, subject to the *jus in Bello* tradition[38].

Common Article 2(1) of the 1949 Geneva Conventions provisioned that the Conventions apply 'to all cases of declared war or of any other armed conflict which may arise between two or more of the high contracting parties, even if the state of war is not recognized by one of them[39]. It is generally accepted that this provision reflects customary international law and therefore fixes the threshold of application not only of the Geneva Conventions but also of the customary provisions contained in the Hague Conventions[40]. In the light of the first paragraph of Common Article 2, the Geneva Conventions and customary international humanitarian law would apply to cyber operations between states in three cases: (1) if they are preceded by a declaration of war made through cyber or traditional means of communication; (2) when the cyber operations occur in the context of an already existing international armed conflict and have a nexus with it; and (3) when they amount themselves to an international armed conflict, with or without the

[37] Lesley Swanson, *The Era of Cyber Warfare: Applying International Humanitarian Law to the 2008 Russian-Georgian Cyber Conflict*, 32 LOY. LA INT'L & COMP. L. REV. 303 (2010).
[38] Christopher S Yoo, *Cyber Espionage or Cyberwar?: International Law, Domestic Law, and Self-Protective Measures*, CYBERWAR: LAW AND ETHICS FOR VIRTUAL CONFLICTS (JENS DAVID OHLIN, KEVIN GOVERN, CLAIRE FINKELSTEIN, EDS., 2015), U OF PENN LAW SCHOOL, PUBLIC LAW RESEARCH PAPER (2015).
[39] Adam Roberts, *Documents on the Laws of War* (2000).
[40] NILS MELZER, INTERPRETIVE GUIDANCE ON THE NOTION OF DIRECT PARTICIPATION IN HOSTILITIES UNDER INTERNATIONAL HUMANITARIAN LAW (2009).

concomitant occurrence of kinetic hostilities. Here, it would be more practical to address the issue that it is useful to refer to the notion of 'belligerent nexus' developed by the ICRC in relation to the notion of direct participation in hostilities. According to the ICRC, the belligerent nexus requires that the act must be 'specifically designed to directly cause the required threshold of harm in support of a party to the conflict and to the detriment of another[41]. It is submitted that if the cyber operations are conducted by a belligerent against another and cause or are reasonably likely to cause the required threshold of harm to the adversary, the nexus is established, and the cyber operations, as acts of hostilities, would fall under the scope of the law of international armed conflict. The notion of armed force has already been discussed in Articles 2(4) of the UN Charter. The question is whether any use of armed force in the jus a bellum sense also amounts to a resort to armed forces in the jus as bellum sense also resort to armed force that determines the existence of an international armed conflict under the jus en bello or whether the former is a broader concept that the letter. Judge Shahabuddeen's Separate opinions in the Tadic Appeals Judgement contend that an armed conflict involves the use of force and, therefore, the question of whether there is an international armed conflict between two states depends on whether a state has used armed force against another[42].

Means and method of cyber warfare

Under the Rule 41 of the Tallinn Manual distinguishes between means of cyber warfare and methods of cyber warfare, stating that the means of cyber warfare are "cyber weapons and their indistinguishable associated cyber systems". In contrast, cyber methods of warfare include the "tactics, techniques and procedures by which hostilities are being conducted."[43] These definitions will apply in international and non-international armed conflict situations. In the commentary on Rule 41, the group of experts states that cyber weapons are "by design, use, or intended use capable of causing either (i) injury to, or death of, persons; or (ii) damage to, or destruction of objects, that is, causing the consequences required for qualification of a cyber operation as an attack." The cyber infrastructure used to launch a cyber attack (in this case, the internet) is not viewed as a means of warfare because it is not under the control of the attacking party. The definition of cyber warfare methods does not include communication between allies.

[41] Ryan Goodman & Derek Jinks, *The ICRC Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law: An Introduction to the Fórum*, 42 NYUJ INT'L L. & POL. 637 (2009).
[42] Judge Mohamed Shahabuddeen et al., *INTERNATIONAL CRIMINAL TRIBUNAL FOR THE FORMER YUGOSLAVIA-APPEALS CHAMBER: PROSECUTOR V. TADIC [July 15, 1999]+ Cite as 38 ILM 1518 (1999)*, PROSECUTOR (1999).
[43] SCHMITT, *supra* note 13.

Still, it is steady to refer to "more than those operations that rise to the level of an attack." Even though communications between friendly forces are not viewed as methods of cyber warfare, interfering with the enemy's communication using a Denial of Service (DoS) attack that does not reach the threshold necessary to be considered a cyber attack would constitute a method of warfare.

In the case of means and method of warfare, Rule 42 of the Tallinn Manual explicitly states that: *"It is not allowed to apply means or methods of cyber warfare that are to cause dispensable injury or unnecessary suffering."*[44] This rule reflects both treaty law[45] and customary IHL and is applicable in both international and non-international armed conflict[46]. In the Nuclear Weapons case, the International Court of Justice (ICJ) defined unnecessary suffering as "harm greater than that unavoidable to achieve legitimate military objectives."[47] In conformity with Rule 42, it applies only to injury or suffering caused to combatants, civilians directly participating in hostiles, and members of organized armed groups, while any incidental harm caused during a military operation to persons protected against attack would be governed by the principle of proportionality and the requirement to take precautions in attack[48]. Given the nature of the test, using means or methods of cyber warfare against certain targets could be more effective than conventional means or methods. Most cyber-attacks tend to neutralize or destroy a target while causing fewer casualties. However, the test is not limited just to the immediate effects of the two weapons (or methods of warfare); other factors should be taken into consideration before choosing between the two, such as the availability (including the expense) of both types of weapon, the logistics of supplying the weapon and its ammunition at the place where it is to be used and the security of the troops which employ it.

All these factors favor increasing the usage of cyber means and methods in certain situations. It should be noted that most means and methods of cyber warfare are not directed against individuals but against military materiel. Rule 43 deals only with means and methods of cyber warfare that are inherently discriminatory. Subparagraph (a) prohibits those means and methods of cyber warfare whose effects are impossible to predict. For instance, the launch of

[44] Tallinn Manual, p 76, *supra* note 11.
[45] Theodor Meron, *The Geneva Conventions as Customary Law*, 81 AMERICAN JOURNAL OF INTERNATIONAL LAW 348 (1987).
[46] ICRC Customary IHL Database – Rule 70 – Accessed on 10.03.2015.
[47] ANONYMUS AC02198766, LEGALITY OF THE THREAT OR USE OF NUCLEAR WEAPONS: ADVISORY OPINION OF 8 JULY 1996 (1996).
[48] Tallinn Manual, p 76, *supra* note 11.

malware, designed without any specific safeguards, will infect and deploy the payload component to all computer systems infected without distinguishing between military computer systems and computer systems protected by IHL. Subparagraph (b) prohibits the usage of means and methods of cyber warfare that are capable of being directed against a specific target but also will cause harmful effects on civilians or civilian objects.

Cyber Attribution and State Responsibility

The term "state responsibility for cyber operations" refers to a nation-state's political and legal responsibility for its acts carried out in the cyberspace domain. This covers a wide range of actions, including cyberwarfare, cyberattacks, and cyberespionage. Identifying the responsible state actor or institution behind a cyber attack and assessing their level of culpability or liability for the attack is known as "cyber attribution and state responsibility." This idea includes the efforts and difficulties involved in identifying the source of cyber attacks as well as the potential legal or diplomatic repercussions when a state is proven to be accountable for such actions in the cyberspace. It's a crucial subject in the context of global cyber security and the creation of standards and guidelines for state conduct online.

According to the current understanding of state responsibility, a "State bears international responsibility for a cyber-related act that is attributable to the State and that constitutes a breach of an international legal obligation."[49] Because State responsibility is precluded in the absence of attribution, States should be very concerned with cyber attribution. The international law on state responsibility specifies that attribution is the operation of attaching a given action or omission to a state. Although there have been substantial improvements in the technological capacities to track cyber attacks, such as locating the precise device or IP address used by the attacker, the legal elements of attributing cyber attacks have mainly remained obscure due to a number of problems. The persistence of uncertainty and delays in gaining attributions is one factor[50]. By purposefully concealing their identities or staging their cyber attacks to look like they were the result of another party, attackers make it more difficult to attribute blame. Even with recent advancements, identifying the computers or IP addresses that were used in the hack is frequently challenging, expensive, and time-consuming, and doing so does not always reveal the State that was at fault. To prove accurate attribution, technical, on-the-ground intelligence,

[49] Scott J Shackelford & Richard B Andres, *State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem*, 42 GEO. J. INT'L L. 971 (2010).
[50] *Id.*

and police investigations are frequently required. Even significant attempts do not always result in clear-cut evidence. Aside from locating the perpetrator, attribution has struggled to agree on the standards of proof, whether or not attributions should be made public, and the repercussions of a successful attribution. More fundamentally, efforts to clarify what international legal principles apply when cyber operations target civilians and their infrastructure below the use of force threshold and outside of armed conflicts have been hampered by the lack of agreement on standards of proof, public attributions, and the legal repercussions of attribution. It can frequently take sophisticated technical research and intelligence gathering to attribute cyber operations to a particular state. Depending on the gravity and consequence of the cyber operation, attribution may result in diplomatic, judicial, or even military reactions. There is continual interest in and discussion about the creation of international rules and agreements governing state conduct in cyberspace. These initiatives seek to define the obligations of states in the area of cyber operations as well as the rules of engagement.

Conclusion

Unfortunately, we have no bottom line on cyber conflict and the future of warfare in the digital domain. Particularly, cyber conflict is a phenomenon being designed and redesigned by new technological developments. Until now, we can presume and present the fact from some major incidents that Cyber operations producing physical effects such as damage to property, loss of life, or injury are currently considered more likely to qualify as a prohibited recourse to force. In this regard, Stuxnet is one of the rare examples of a cyber operation causing physical damage and, thus, the most likely one to qualify as a use of force. However, there is a clarification and some solace to be found. We can pretend that the character of conflict is changing more rapidly and unpredictably than it ever has.

The challenges presented by this unique context include the difficulties created by the anonymousness on which cyberspace is building. Similarly, there needs to be more clarity concerning controversy about the notions of attack and the complications of applying conduct of hostilities rules to cyber warfare, particularly the prohibition against indiscriminate attacks and the rules on precautions in attacks. These challenges should be resolved by developing new treaty rules. In conclusion, it is difficult to state how IHL applies to cyber warfare. However, whether it will provide sufficient protection to the civilian population, mainly by keeping safe and protecting civilian infrastructure from harm, will depend on how IHL, whose drafters did

not envisage such operations – is interpreted with respect to them. Only if interpreted in good faith and with the utmost care will it be possible to protect civilian infrastructure from being directly targeted or suffering damage that could be catastrophic for the civilian population or non-combatants. Even then, considering the potential weaknesses of the principles of distinction, proportionality, and precaution, and in the absence of more profound knowledge of offensive capabilities and effects, it cannot be excluded that more stringent rules might be necessary.

WHITE BLACK
LEGAL