Armed Hostilities: Addressing the Evolving Policies, Regulations and Challenges of Information Warfare

***Uche Nnawulezi*[1], *Jacques Kabano*[2] , *Robert Turyahebwa*[3]**

[1] *Assoc.Prof., Faculty of Law, University of Lay Adventists, Kigali, Rwanda*
email: uche.augustus@unilak.ac.rw , ORCID: 0009-0004-0625-2775
[2] *Dr., Faculty of Law, University of Lay Adventists Kigali, Rwanda;*
email: j.kabano@unilak.ac.rw ; ORCID: 0000-0002-0248-9204, Corresponding author
[3] *Faculty of Law, University of Lay Adventists of Kigali, Rwanda;*
Email: rturyahebwa@gmail.com ; ORCID: 0009-0002-9650-1899

Received Date: 17/06/2025 *Accepted Date: 03/10/2025* *Published Date:30/10/2025*

Abstract

In today's rapidly advancing world, armed hostilities have taken on a new dimension with the emergence of information warfare. This conceptual paper examines the evolving landscape of IW through a normative legal lens. It argues that with technological advancements, information warfare has become a prominent tool in modern conflict, creating additional challenges to the unity and security of nations. Through a normative research method, the paper examines existing policies and regulations governing information warfare and emphasizes the necessity of adhering to the principles of necessity and proportionality, as applied to other forms of military conflict under the Law of Armed Conflicts. Against this backdrop, the paper investigates the issues associated with information warfare. It unveils that as technology continues to advance, so do the challenges and risks linked to information warfare. Therefore, it is crucial for authorities and agencies to establish comprehensive guidelines and policies capable of addressing these emerging threats. Ultimately, the paper concludes that there is a pressing need to educate and train individuals on cyber warfare in order to raise awareness, prevent, and respond to potential cyber-attacks. By implementing these measures, governments and organizations can create a secure and resilient environment in the face of information warfare.

Keywords: *Armed Hostilities; Policies; Regulations; Challenges; Information; Warfare*

1.0 Introduction

In recent years, issues of armed hostilities and information warfare have become increasingly complex and challenging in this era of internet. As the world experienced advancement in technology, States along with non-state actors now involved in cyber-attacks, disinformation campaigns, and other forms of information manipulation that can have devastating consequences [1]. As a result, policymakers and governments around the world are grappling with the need to develop comprehensive policies and regulations to address this evolving threat. Be that as it may, the challenges of information warfare are numerous and multifaceted. However, IW remained an application of several techniques aimed at undermining an adversary's reputation or informational infrastructure [2]. This strategy can be used in both peace and conflict and this form of warfare has become increasingly prevalent in recent years as technology has advanced and the internet has become a crucial battleground. The information warfare tactic, in particular, is heavily dependent on hybrid warfare players.

In this regard, government as well as non-government actors engaged in hybrid warfare using IW strategies to demonize their adversaries through the distributions of fake news, misleading information and propagandas,

e-ISSN 2821-3394

or to undermines their adversary's internet security systems. It should be noted that IW applies several tactics in its operations, for example, sudden and covert on-line attacks on an adversary's cyberspace through interceptions of confidential information, theft; or using social media campaigns to disseminate rumours against the adversaries [3]. To put it succinctly, information warriors rely on obtaining information before harming their opponent intangibly. Sometimes, the intangible harm also results in material harm. For example, a viral attack on an enemy's jet fighters' command and control systems can make it more difficult for pilots to manoeuvre their aircraft, which could lead to crashes and even human losses [4]. As damage has changed from being intangibles to tangibles which suggests that the Law of armed Conflict (LOAC) would apply in this situation. However, there seems to be some difficulties in enforcing global regulations on IW when the likely effects of the activities resulting from IW are intangible harm [5].

Furthermore, the paper takes the position that freedom of thoughts, expressions, common heritage of mankind as well as requirements of Outer Space Treaty (OST) significantly imposed constraints on global laws in the regulations of IW activities. However, these constraints are essential for maintaining ethical standards and preventing the misuse of IW. It is of foremost importance to note that this constraint contributes to the challenges in the legal placement of IW under international law's norms, rules, and principles [5]. As a result, activities on the operations of information becomes unfettered in its scope and operations, thereby posing global threats to safety and tranquility. Therefore, it is worthy of mention that absence of regulations is capable of allowing competitor States to utilise information warfare techniques unrestrictedly against each other, which can lead to escalating conflicts and destabilizing international relations. When militant terrorists and anti-state groups develop information operations, the hazards to peace and security increase. As a result, it becomes instructive that the global community should collaborate on enacting relevant laws that will govern State behaviours and non-state actors anytime they employ information warfare methods and technologies against any state or entity [6]. The underlying difficulties can be addressed by convening a new convention on the subject and having conversations amongst government regulating the uncontrolled field of passage of information. Thus, this approach required cooperation and collaboration between nations to establish comprehensive guidelines and frameworks for managing the complexities of information warfare [5].

This paper aims to examine the ever-evolving landscape of information warfare and the policies and regulations that need to be put in place to address its challenges. With the advancement of technology, information warfare has become a prominent tool in modern warfare, creating several challenges to the unity and safety of the Nation. In this regard, it is crucial to explore how governments and international organisations can adapt their strategies to effectively counter and mitigate the risks associated with this form of warfare. Additionally, the paper will analyse the ethical implications of information warfare and discuss the importance of establishing ethical guidelines to govern its use. Ultimately, the paper will analyse the current landscape of information warfare and propose strategies to mitigate its impact.

2.0 Research Methodology

This paper is a conceptual study that employs normative legal research methodologies to analyze the theoretical and regulatory challenges posed by IW. Firstly, the statutory legal methodology is dependent on positive legal guidelines, principles, policies; findings along with regulatory frameworks. Also, through statutory approach, the paper examined the strength and weakness of the regulatory frameworks in place, and what should be done to strengthened it. Statutory methodology becomes necessary here as it is used to examine the norms in information warfare as well as its inadequacies in terms of safety measures. Secondly, the conceptual approach is used to examine the phenomenon of information warfare as emerging technology of warfare, and what should be put in place to handle the challenges and threats associated with it.

3.0 Results and Discussion

3.1 Evolving Concept of Armed Hostility in Digital Age

According to an online source, the term hostilities mean the physically armed clashes with a hostile party. A situation of armed hostilities gave rise to the emergence of comprehensive legal frameworks that regulates the manner in which parties to armed hostilities can apply or limit the applications of force against the hostile

e-ISSN 2821-3394

States during the armed hostilities [7]. From this expressions, armed hostilities can be understood as the actual use of weapons and force in a conflict between opposing parties. These hostilities are not only limited to traditional warfare but also encompass the growing field of information warfare. As technology advances, new challenges arise in regulating applications of force in the cyber realm, thereby making it necessary to re-examined the evolving policies and regulations meant to address these challenges. The concept of armed hostilities is constantly evolving to encompass the changing nature of warfare in the digital age. From the foregoing, the LOAC appears to be a regulatory framework designed to control and lessen the adverse effects of the conduct of armed hostilities [8]. The advancement and protection of the civilian populations in situations of armed hostilities is this thus the primary objective of LOAC, and basically it seeks to create a balance between military necessities and humanitarian protections [9]. The whole essence of this regulatory framework is rooted in the believe that since armed hostilities cannot be completely eradicated, then, it should and must be controlled [10].

Basically, the above position is, no doubt, informed by the fact that the acceptance and rejection of a particular means or methods of armed hostilities remained a major concern aimed at ensuring that the extent of measures to be applied in situations of military hostilities is proportionately in line with the military necessities designed to be accomplished [11]. This position is reinforced by the decisions that it is only an acceptable means of weapons of warfare that has passed the test of military objectives may be applied, and not the type that has adverse effects on the civilian populations [12]. On the contrary, the implications of this inclusion of prohibited techniques or procedures of armed hostilities is to ensure that those weapons that are capable of causing unnecessary sufferings or injuries to the civilian populations along with the violations of the rules of IHL are restricted [11]. It is noteworthy that these prohibitions placed on the techniques or nature of warfare is dependent on the guidelines that in situations of armed hostilities, the rights of the parties to agree on certain techniques or nature of warfare is not limited, only a desired method of warfare may be applied to suppress the hostile forces; unnecessary injuries or sufferings should be prevented, and a level of fairness and respect to human dignity should take precedence [11]. Indeed, the above position has raised several arguments either from those advocating for the complete prohibitions of certain means of warfare, and those saying that sustenance of injury during armed hostilities is a common thing, irrespective of the nature of weaponry used [13].

There have been criticisms on the notion that non-lethal types of warfare like compromise of the hostile forces' computer setup does not amounts to 'applications of forceful measures', and therefore, are not within the contemplation of LOAC. It is the contention of the authors that advocates of the above position, should be able to demonstrate that such actions are legitimate even in peaceful conditions under the Law of Nations. This cannot be established easily.

3.2 Deconstructing Information Warfare: Definition and Core Concepts

First of all, it is crucial to begin by clarifying an important misconception that has seeped into the public discourse on the subject matter. Information Warfare has been publicly confused and conflated with Command-and-Control Warfare or C2W, but they could not be more different. While C2W aims to use physical and electronic means to attack communication infrastructures and equipment to isolate the enemy forces on the field from the command off the field, IW aimed at exploring true or untrue messages to damage the mind and will of the enemy. It is not just a distinction without difference, as some would say, but goes to the root of the subject matter of this discourse. It should be noted that IW is different from all other forms of warfare. It is insidious, often subtle, and very difficult to defend against. The definition of IW has evolved over time as new technologies and communication platforms emerged, and because of the misconceptions about the subject matter. However, IW may be construed as the use of technology to gain an advantage in military conflicts, while others view it as a broader strategy that encompasses psychological operations and propaganda. Regardless of the definition, it is clear that information warfare has become a critical component of modern warfare, with governments and non-state actors alike utilizing various tactics to manipulate and control information flow to achieve their objectives. As technologies continue to advanced and new threats emerge, policymakers and regulators must adapt quickly to address the evolving challenges posed by IW.

From the foregoing, the USDD uses the definition of IW preferred by the Joint Chief of Staff. In this regard, the JCS, in Joint Publication (JP)3-0, Joint Campaigns and Operations, defines IW as:

e-ISSN 2821-3394

a form of information used in addition to other similar lines of activities to compelled, distort, changed, or took the policy-making process of the hostile powers or their likely enemies while safeguarding their own equipment.

Nonetheless, it has been argued that the difference between C2W and IW is not merely to separate "EC" from "EF", but to compelled, distort; destroyed or assumed the policy-making process of the EC itself. However, in view of the above arguments, it can rightly be said that things like propagandas, misinformation campaigns; smear tactics, or actual destructions to information facilities comes within IW. According to the New York Times in an article titled, "How Russia Took Over Ukraine 's Internet in Occupied Territories", it is stated that one of the Russia's key activities in occupied Ukrainian territories has been to take over the local Internet service providers, control the internet traffic through Russian Networks or either block access to social media sites, and UNA, or turn off the internet in its entirety [14]. This is a typical example of how IW can take myriad forms. IW, despite the tendencies of recent generations to assumed it as a recent development, but it may be construed as a non-recent form of warfare as the US Air Force has had IW squadrons since 1980s. Currently, its mission has been transformed into "to fly, fight, and win in air, space and cyberspace".

Initially, IW was referred to as the use of propaganda and mental activities in creating an impressions or perceptions about a hostile power. However, with the emergence of ICT and advanced internet facilities, the scope of IW has grown to includes cyber-attacks, misleading campaigns, and the manipulations of public opinions through the dissemination of false information. As a result, governments and organisations around the world are grappling with how to address the evolving policies, regulations, and challenges posed by information warfare in order to protect national security and safeguard democratic processes. Inclusively, many have used the phrase synonymously with "info war," "cyberwar," and "netwar." Drawing from the above, the paper however, examines the concept of IW according to the Congressional Report as follows:

> *Information now operates in a realm as a weaponry against its target. In this case, an information-based attacks comprised of an unapproved step made in copying data, or to alter data indirectly through a command. IW are more deeply involved in ICT along with internet application systems. It encompassed several activities targeted at any pattern of information, transferred to any platform which includes activities on the content of the information, other systems attached to it; software; physical hardware devices that stores data or commands, along with individual activities or understandings.[15]*

This term, however, is too wide for the purposes of this study. While certain information warfare capabilities, such as deception and psychological operations, are primarily the domain of state actors, similar ones like computer network attacks are carried out by hackers or internet fraudsters known for non-compliance with arms control regime or adhere to international norms and regulations [16]. As a result, for the purposes of this article, IW actions are restricted to some of the activities carried out by State actors in situations of military warfare between a particular State and another. Sometimes, the reason may be that state actors have the resources, capabilities, and political motivations to engage in systematic and organized information warfare. State actors can leverage various tactics, including cyberattacks, disinformation campaigns, and propaganda dissemination, to manipulate public opinion, disrupt enemy communications, and gain a strategic advantage.[1]

IW is the term used to describe nation states' pursuit of a strategic advantage through dominance of the infosphere. This includes such target at on information infrastructures so as to weakened the capacity of a hostile party in order to counter or mitigate the actions, as well as manipulating information thereby creating an erroneous impression. According to NATO in 2022, IW is defined as:

[1] *This definition is intentionally restrictive to limit the discussion to address only those activities that may fall under the purview of the Department of Defense, the State Department, or their equivalent in other states. Under normal circumstances neither the Armed Forces nor the State Department will be called to remove a crowd that was preventing customers from entering a bookstore. Similarly, they should not be expected to respond to computer hackers that were conducting denial of service attacks against e-commerce websites. In both cases, these activities are the responsibility of local law enforcement officials, such as campus police or the FBI.*

e-ISSN 2821-3394

> *Such activities executed in order to access relevant information against the interest of an adversaries. This comprised of the control of one's information space, protection of one's access to his information, in the course of acquisition along with the application of the enemy's information; destructions of the information networks and obstruction of the flow of information. IW is not a new concept, but comprised of technological particles that enhanced the effects of innovative growth that oftentimes leads to information being circulated speedily to a large extent.[16]*

In order words, infosphere consists of both the physical infrastructure of information systems and the virtual space where information is stored, accessed, and shared. Information warfare is a strategic approach that focuses on manipulating and exploiting this infosphere to gain an advantage. It involves several techniques like hacking, dissemination of misinformation, along with leveraging on internet platforms in manipulating public opinions. It is to be noted that the primary concern of IW basically, is to ignore an opponent's decision-making processes, weaken their reputation, and ultimately gain a strategic advantage in conflicts, both on the battlefield and in the realm of public perception [17]. As technology continues to advance, the importance of information warfare will only grow, making it crucial for nations and organisations to develop robust defences and countermeasures to protect their information space. In relation to the subject matter of IW, it is noteworthy that 'IW' in the 1980s, different highly rated technologies were assessed by its ability to be of adverse effects to the hostile forces information flow and disabled its powers of retaliations, as this is today forming part of IW [18]. In the context of the applications of innovations in the destructions or incapacitation of the communication facilities of the hostile forces during hostilities, under the LOAC, it may be contended that the basic guidelines upon which any aggressive attacks could be evaluated is based on the fundamental guidelines on necessities and proportionalities.

The combined effects of necessities and proportionalities of such attacks must be seen to be necessary for military objectives, while the destructions incurred in such situations should be more advantageous as expected. In any case, risk control is the prime reason for LOAC in the sense that weapons of IW are more dangerous, and no amounts of military advantage could be proportionate to the deaths of civilian populations. Therefore, it is submitted that any applicable test used in LOAC should be equally applicable to methods of IW. Consequently, it is contended that " any formulations or executions of IW strategic plans, it must be in compliance with local, global regulations, treaties; LOAC along with other known regulations governing armed hostilities [19].

Above all, IW is construed as a determined efforts made to destabilized enemy's Command and Control (C& C) operational facilities in order to safeguard and control the activities of the C& C facilities of friendly military forces [20].

3.3. Understanding the Battlefield of Information Warfare

In this segment of the paper some key terms will be discussed that will give useful analysis of IW. These includes, but not limited to popular buzzwords like disinformation, misinformation; cyberattacks and psychological manipulations.

- **i.** *Disinformation* - According to the Merriam-Webster Dictionary, disinformation is defined as "false information deliberately and often covertly spread in order to influence public opinion or obscure the truth". A popular example would be the massive Russian disinformation campaign on TikTok, designed to discredit Ukrainian officials using narratives tailor-made for Western audience that was discovered last month by the BBC and the Digital Forensic Research Lab at the Atlantic Council.
- **ii.** *Misinformation* - Misinformation is defined as "false or inaccurate information". Unlike disinformation, misinformation is oftentimes ignorantly spread by members of the society who do not know any better. In this case, a typical example is the wild theories related to COVID-19 pandemic that was spread on social media.
- **iii.** *Cyber Attack* - This is defined as any malicious attempt to gain unauthorized access to a computer, computing system or computer network with the intent to cause damage [21].

e-ISSN 2821-3394

iv. *Psychological Manipulation*- This is defined as a type of social influence that aimed at changing the behavior or perceptions of others through abusive, deceptive; or underhanded tactics [22].

v. *Kompromat*- The Merriam-Webster Dictionary defines Kompromat as compromising information used to either blackmail or discredit a public figure or group, usually for political purpose. It has been theorized by various sources on the web that the Russian Government had a Kompromat on former US President, Donald Trump.

Beyond these terms, to properly understand the complex battlefield of IW, one must also understand the various participants on the battlefield. This is by no means an exhaustive list, but the most popular participants in the battlefield of IW are as follows:

a. Nation-state like Russia, the United States, and Saudi Arabia with large and robust information and disinformation networks,
b. Non-Governmental Organizations;
c. Private individuals can range from hacktivists to social media influencers;
d. Politicians who spread information or Kompromat for political purposes;
e. Security agencies and Terrorist Organizations.

It is to be noted, however, that these parties are constantly embroiled in a shadow war in order to control the flow of information to both their enemies and allies, as well as the various populations of the globe to see who would emerge victorious. In a digital age like ours, the control of information is priceless. But the question that often comes to mind is 'how?'. How exactly do so (comparatively) few individuals influence and manipulates the flow of information and the discourse of the majority of people? How would something like this work in a thinking society with access to more information than ever? These questions bring us to the next segment of the paper.

3.3.1. *Tactics and Techniques*

As previously stated, the participants in the battlefield of IW are legion. In the same vein, the tools that they employed in their ever-shifting combat are similarly numerous. Even more, they are not just numerous but ever -evolving and changing. It would be manifestly impossible to attempt an exploration of all the tactics and Techniques employed in IW. This paper focused on exploring and analyzing four of the most common and relevant tools in our present digital landscape such as:

i. *Fake News*: UNESCO defined News as verifiable information within the public interest. This makes the phrase above, the subject of this segment of the paper, a bit of an oxymoron. Fake news, as it is, is news that fails to live up to its true definition. The information is never verifiably true, and based on that is not in the best interest of the public. In a similar note, it is defined as misleading content found on the internet, especially on social media (National Endowment for Democracy). Desai and Oehrli, in an article contained in the University of Michigan Library had the following to say about fake news:

> *The world of misleading information is greater than simply concocted stories. Certain stories tend to have iota of truth in it, but are not factual. It may not contain a cogent facts or sources. Some may contain cogent facts, but are designed in such a manner that it appears provocative leaving salient points and presents a one-sided story. False information exists amongst a large ecosystem of mis-and disinformation [23].*

While this understanding of the concept seems appreciable, it is to be noted that fake news is one of the tools made and used by the actors within IW to spread false information for a variety of purposes. A good example would be the well-documented spread of fake news around the 2016 United States Presidential elections. A cursory look at the surrounding stories about the 2016 United States Presidential elections suggests that an average American adults saw at least one fake news story during the three months preceding the election, that half of those who recalled seeing fake news stories at the time believed them, and that some fake news stories were reported and shared over as much as thirty million times on the internet [24].

ii. *Cyberwar:* Cyberwar is defined as a cyberattacks or series of cyberattacks launched against a country or state to gain a strategic or military advantage [25]. Cyberattacks are a cornerstone of modern information w, wielding the power to disrupt critical infrastructure, manipulate

e-ISSN 2821-3394

public opinion, and sow discord. Cyberwarfare is also a key component of information warfare in that it is one of the means for information to be stolen and transferred from one place to another. The paper noted that several United States Federal Agencies were hit in a global cyberattacks by Russian criminals [26]. More importantly, cyberattacks can be aimed at a variety of targets, including but not limited to, critical infrastructures like financial services, hospitals; power grids; media outlets for the sake of spreading misinformation and stealing of sensitive information as well as disrupting crucial services and functions.

iii. *Social Media Manipulation:* This is, perhaps, one of the more insidious means of IW, as rather than making use of sophisticated technology to hijack communication platforms to misinform and deceive the public, this merely manipulates platforms by allowing them to run as they already do and taking advantage of this to mislead the public. This, it is clear that this is done primarily through the use of Algorithms. Sprout social defines Algorithms as rules, signals and data that govern the platform's operation. They go on to explain that algorithms determine how content is filtered, ranked; selected and recommended to users. It is through the manipulation of this algorithm that participants in IW spread misinformation, disinformation, or misinformation to the users of these social media platforms.

iv. *Deepfakes*: This is another aspect of IW worth noting in light of its possible negative effects around the globe. In 2023, a post went viral on internet with a picture of the Pope in a Balenciaga outfit. This picture was not real. That is to say, it was an AI deepfakes made of the Pope. Since then, several similar deepfakes have been released on the internet with viewers struggling to separate facts from fiction. With the use of AI, any person with more than three photographs on the internet can be made to say, or do anything. All of this suggests that deep flakes are photos or videos created using a form of AI called Deep Learning that depicts fake events. Therefore, it can be argued that the use of deepfakes in IW is a fairly recent innovation, while it has existed since as far back as 2017. This can be noted from its usage which was originally limited to pornography because it was easy to differentiate a deep fake from reality, and with the development in AI, it is no longer the case. Thus, while the essence of deepfake' is associated with fake events, a notable example of it is the one being utilized in IW with a video spread on social media of Ukrainian President, Vladimir Zelensky, asking his troops to surrender to the invading Russian forces back in 2022.

4. Security Dilemma of Information Warfare

IW is a dilemma that governments and organisations around the world are grappling with. On one hand, the rapid advancements in technology have made information warfare a powerful tool for achieving strategic objectives. On the other hand, these advancements have also made it easier for malicious actors to carry out cyberattacks and manipulate information for their own gain. Policymakers and security experts are, therefore, faced with the challenge of developing policies and regulations that can effectively address the evolving nature of information warfare while also safeguarding national security and individual privacy. Furthermore, the interconnectedness of the digital world means that no country is immune to the potential threats posed by information warfare, making international cooperation and collaboration crucial in finding effective solutions.

In addition to the self-referential nature of security practices, IW are found to have threatened the national security of a State because it's contributions to the security dilemma, which is a central tenet of realism, the preeminent theory of international relations. Realists assert that each state is in charge of ensuring its own security and that security is a self-help system inside the anarchic framework of the international order. The security issue in this self-help system arises from the possibility that, to strengthen its security, one state's activities may weaken those of other states [27]. This leads to a vicious cycle where states continuously engage in a competitive race to enhance their security, often at the expense of others. Information warfare exacerbates this dilemma by enabling states to manipulate information and disrupt the security measures of their adversaries. By spreading misinformation or conducting cyberattacks, states can undermine the integrity of their rivals' security systems, creating a sense of insecurity and further escalating tensions between nations [13]. Consequently, information warfare not only threatens national security but also fuels a perpetual cycle of mistrust and aggression among states.

Strictly speaking, the paper posted that in 1996, the NSA Report indicated that more than one hundred and twenty States owned or in the process of establishing IW technologies are likely to generate concern among

e-ISSN 2821-3394

neighbors and inspire others to acquire similar capabilities, escalating the threat [28]. Furthermore, declarations like assurances made by China to be known and recognized as the world's foremost IW Nation could give rise to arms race in IW [29]. This would lead to a heightened level of vulnerability and insecurity in the cyber realm as countries strive to outdo one another in terms of offensive and defensive capabilities. The evolving policies and regulations in response to this challenge are crucial in ensuring that a delicate balance is maintained, where nations are able to protect their own interests without escalating tensions and triggering a full-blown cyberwar. Overall, it is no longer business as usual with regards to the challenges of the contemporary armed hostilities bordering on command structure. The paper observed that in these situations, a prominent concern of the commander is to take into account the problems associated with transfer of technology and capability's exposures during the operations. This implies that issues associated with transfer of technology may be a hindrance to the extent of IW it can applied in such situations [30].

5. Applying the Legal Regime: LOAC, CHM, and ITL

Information warfare poses unique challenges for the existing legal regime. As technology continues to advance, traditional laws and regulations struggle to keep pace with the rapidly evolving landscape. One of the main challenges lies in defining the boundaries of information warfare and determining what actions constitute a violation of international law. Additionally, the anonymity and global reach of cyberattacks make it difficult to attribute responsibility, further complicating the enforcement of existing regulations. Perhaps because much of the technology involved is still relatively new, and there is lacked of existing guidelines on global regulations that expressly placed a restriction on what is currently known as IW. It should be stated that lacked of restrictions measures increase the risk and thereby endangered the interest of the State as what the global regulations does not restrict, it invariably allows that [31]. However, it may be argued that non-existence of such regulations cannot be understood as an escape route, because even if the global regulations seem not to pretend in addressing specific arms or innovations, its general guidelines may be applicable to their deployment [31]. Nonetheless, existing international law allows for a wide range of information warfare strategies in a variety of situations. From the above there, results have shown that a little aspect of the evolving IW principles attempts to appreciate the notable challenges of applying computer innovations as a means of warfare. In this case, computer programmed takes up the role of ethical spies and warriors as it aimed at disrupting hostile forces access to reliable information, and allowed friendly forces to embraced a reliable picture of hostile forces planned attacks or target. In the ongoing Russia's military hostilities in Ukraine, the applications of social media strategies have served as battle grounds for States and Non-State actors in disseminating several competitive stories about the hostilities, while giving different situations about the armed hostilities in line with their own perceptions and likeness [32]. In the same vein, IW is a fast-growing innovation even in maritime hostilities [33]. What this suggests is that even the Naval units are gradually incorporating IW systems in its physical, virtual and constructive establishments. In the same vein, the applications of cyber and IW by Russian military forces in the Ukrainian territory has really demonstrated the effects of IW [34].

5.1 *LOAC*

In military warfare, civilian populations who are not non-combatants are protected under the law of military warfare, sometimes known as the LOAC [34]. In a similar vein, the law of war also seeks to defend people against cyberattacks. In other words, parties involved in information warfare must not put the general public at risk [34]. This guideline can be used for any hacking activity or information warfare wager that disrupts any technological transmission by an enemy state. Such actions should be prohibited by IHL or the law of war if they cause harm to civilians in any way, such as by interfering with their daily lives or businesses [34]. Similar conclusions can be drawn about several different scenarios that might guarantee noncombatants' and civilians' safety. For example, if a state engages in cyber warfare by hacking into a hospital's system and disabling critical medical equipment, innocent civilians who rely on that equipment will be put in immediate danger. Additionally, if a power grid is sabotaged and millions of people are left without electricity, their daily lives and businesses will be severely disrupted, causing widespread harm and chaos. The LOAC acknowledged the importance of protecting civilians and noncombatants during armed conflicts. It prohibits targeting civilians and requires all parties engaged in military warfare to exercise precautionary measures capable of minimizing harm to them.

e-ISSN 2821-3394

5.2 Principle of Common Heritage of Mankind (CHM) and Outer Space Treaty (OST)

Legal regime of IW is a complex and rapidly evolving area, especially with regards to OST and the principle of CHM. It is clear that OST, or treaty on guidelines governing the conduct of Nations in exploring and using OS, particularly the moon along with similar celestial objects, was officially ratified in October 1967 [35]. This Convention construed the entire space and other similar celestial objects are generally regarded as a normal inheritance of mankind, while the Moon Treaty, which was ratified in 1979, established a similar idea. This Treaty states that all issues concerning the moon and corresponding resources are shared possession of all persons. As a result of these two accords, it is possible to say that space and its corresponding celestial objects, such as the moon remained free in terms of usage [36]. However, this position was further strengthened by the declaration made in accordance with the principle of CHM, that asserts as follows: " that any infrastructures or properties shared by all nations must be freely used by all nations" [37]. This suggests that as most information activities are specifically executed via broadcast of radio wave frequencies that goes via the space, the CHM concept, in conjunction with the OST remained applicable to IW as the case may be [38]. In this regard, what this implies is that it affects broadcasting of news items from radio or television channels, dissemination of information via SMP; intrusions of cyberspace via hackers' activities through online network; radio waves transmitted through artificial satellites launched in the space by recognized global telecommunications outfits or those owned by the government. As a result, anytime such situations arise, the mentioned IW occurs, the space becomes a veritable source of transmission of radio waves that facilitates the paths for information activities. According to OST and CHM principles, space is regarded as a free for all mankind to undertake any manner of activities involving IW. In addition, it is rightly observed that OST and CHM principles legally guaranteed the continuing activities of IW in a manner permissible by law.

As a result, the field of information warfare is subject to strict regulations under global law. The primary reason for this limit is that the harm inflicted by IW is intangible. Drawing from the foregoing, it has been firmly asserted that as the LOAC does not addressed intangibilities, it has become challenging on how to control the field of IW. Furthermore, it may be argued that the inadequacy of global law in the aspects of controlling some information activities arising from waging of propaganda against an adversary party via social media platforms or other related medium could be further solidified by the global protection of the inalienable rights to freedom of opinions or expressions established in the UDHR, Article 19 [39]. Furthermore, it is instructive to note that OST along with the principle of CHM permits distributions of information via radio waves frequencies carried into space by artificial satellites, notwithstanding, whether such information was disseminated or used by hackers for several information activities. Alternatively, rather than regulating and limiting information operations, global laws tend to encourage them unintentionally or indirectly. As a result, international legal experts have found it difficult to design methods for regulating information operations [2]. This difficulty arises from the fact that information activities are often conducted through non-physical means, making it challenging to enforce regulations. Additionally, the rapid advancement of technology and the global nature of information dissemination further complicated the regulations of these operations. While some argue for the need to establish international agreements and frameworks to address this issue, others believe that such regulations could infringe on freedom of speech or expression. Ultimately, finding a balance between regulating information operations and upholding fundamental rights remains a complex and ongoing challenge for the global settlers.

5.3 International Telecommunication Law

ITL plays a crucial role in addressing the evolving policies, regulations, and challenges of information warfare. It provides a framework for states to establish guidelines and protocols for the use of information and communication technologies during armed hostilities. Moreover, examining the ITU and its Charter, it may be right to say that the ITC is specifically a convention that regulates global wire and radio communication frequencies, and sometimes may be implicated in some attacks bordering on telecommunication networks.[2] In actual sense, ITU might not be able to significantly restrict information warfare operations, especially during warfare. This is because the ITU's authority is limited to facilitating cooperation amongst contracting parties

[2] Although it was created long before the United Nations, the ITU is currently a member of the UN system.

e-ISSN 2821-3394

and promoting peaceful use of telecommunications. Also, while it can establish guidelines and regulations, it lacks the power to enforce them or take action against non-compliant contracting parties.

Interoperability and interference remained ITU's main concerns. However, the ITU, and its precursor evolved in 1865 basically to facilitates ITT within the region of Europe [40]. Following several dangerous naval incidents, one of the Union's first radio regulations mandated that maritime radio systems be interoperable. This was as a result of the MWC, had the patent right of installing along with operating radio equipment on vessels, and would not allow its agents to interact with any other stations that did not engage MWC. This lack of interoperability posed a significant risk to maritime safety, as ships were unable to communicate effectively in emergency situations. Additionally, the exclusive use of Marconi equipment created a monopoly in the radio industry, limiting competition and innovation. To address these concerns, the ITU established standards and regulations to ensure the interoperability of radio systems, promoting communication and cooperation among different operators and manufacturers.

There is some relevance between IW attacks that adopted electro-magnetic spectrum, ITN and ITU and its regulations. Firstly, broadcasting stations from one country cannot interfere with other states' broadcasts on their authorised frequencies. Secondly, the ITU's IFRB allocates ES to avoid overlapping. Thirdly, combatants' locations are meant to strictly adhered to the rules of non-interference. Fourthly, ORS are prohibited. Fifth, contracting parties are not meant to transmit unreliable and misleading signals. Ultimately, member States should strive to safeguard confidentialities of global exchanged, even though empowered to prohibit RWCs. The aforementioned measures and regulations highlight the importance placed on maintaining order and preventing chaos in the world of radio communications. By ensuring that each state has its designated frequencies and that interference is minimized, the ITU and its member states work towards creating a harmonious and efficient global communication network.

6.0 From Tangible to Intangible Harm: The IW Challenge

This segment explores the various challenges faced in effectively regulating information warfare. Understanding the challenges is crucial in order to develop effective policies and regulations to address the evolving nature of information warfare.

6.1 *Intangible Damage*

One of the difficulties in effectively regulating information warfare is the intangible damage it can cause. Unlike traditional forms of warfare that involve physical destruction, information warfare primarily focuses on manipulating and disseminating information to influence public opinion and disrupt societal systems. The intangible nature of this damage makes it challenging to quantify and address, as it often goes unnoticed or underestimated. It is noteworthy however that application of allied tactics in bombing shows the extent of how the current regulations may be construed in addressing issues of new technologies of IW. The employment of the airplane in this fashion was not prohibited by the laws of war when the first Allied forces began tactical shelling targeted at different towns in Germany and Japan during WWII. Contrarily, their effects were comparable as the subsisting LOAC for naval shelling was utilized to legitimized tactical bombings. Basically, current regulations controlling naval shelling allowed lawful bombing of places of work or equipments relevant to the hostile camps, as it permitted bombing of protected areas, and even allowed the bombing of unprotected areas notwithstanding the refusal of the native agencies on the removal of all the equipments relevant to combatant's installations [41]. It allowed allies to justify their strategic bombing campaigns as they targeted industrial areas and infrastructure that were crucial to the enemy's war effort. The existing laws of war provided the Allies with a legal framework to carry out these bombings, even if they resulted in civilian casualties. Thus, strategic bombing became an integral part of the Allies' overall war strategy, aiming to cripple the enemy's ability to produce weapons and sustain their war effort. As a result, LOW for naval bombing was found to be relevant to tactical bombings due to the impact of both activities was found to be similar unprotected weapons aimed at destroying the hostile party's war infrastructure. The SolarWinds hack (2020)[42], attributed to Russian actors, compromised thousands of organisations globally, including US government agencies. The primary harm was not physical destruction but the silent, long-term compromise of sensitive data and a profound erosion of trust in software supply chains. This 'intangible damage', including espionage and the potential for future disruption, is a hallmark of IW, and existing arms control treaties, designed for physical weapons, are poorly equipped to regulate it. However, remains that one of the difficulties noted in IW is its

e-ISSN 2821-3394

incompatibility with other weaponries now regulated under the arms' supervisory treaties. This position is reinforced by the fact that most of the intangibles impacts of IW differs from weaponries that are engaged beyond cyberspace, and has made the existing regulations on military conflicts difficult to incorporate IW. Therefore, new frameworks and regulations specifically tailored to address the unique nature of information warfare are needed.

6.2 Challenges of Sovereignty

Information is a domain in the United States [43]. According to Joint Vision 2020:

> *An understanding of this spectrum dominance connotes that the US forces are capable of conducting instant, sustainable or synchronized activities in a collaborative manner geared towards a particular situation along with access to or free to engaged in all aspects of space, sea; land; air or messages [43].*

It has been observed that one of the most dangerous aspects of IW in these aspects is its capacity to propagate as electronic signals in all global networks of coverage which is achieved through the space thereby producing the expected results, while remaining undetected through physical sight. Furthermore, all these responses may unintentionally affect Countries that are not sharing boundaries with a targeted State. A more pertinent issue however is to examine the subject of territorial sovereignty of a nation state that emphasized on the sole power of a given state sole power over issues occurring within its territorial boundaries which has remained a basic tenet of global law right from the emergence of the Westphalian Treaty in 1648. Undoubtedly, it has been observed that the challenge has always been on how to determine the mode of application of the subject matter of sovereignty in the sphere of information. Interestingly, the global regulations process has addressed such challenges before, as it was not the first occurrence of emerging technologies being called to question.

The inherent character of IW raises the Realist security dilemma in global politics [27]. Development in a state's defensive cyber capability is typically considered by adversaries to be an emerging offensive weapon, and therefore an IW technology arms race is initiated. This dynamic of rivalry and distrust creates a less secure condition for all, underlining the absolute necessity of trust establishment and open global treaties.

6.3 Ambiguous Definitional Approach in Existing International Law

The UN Charter is a crucial legal text that governs the applications of forceful measures in global system of international regulations. However, it is restricted in its efforts to combat IW as a result of inadequate definitional approach of terms that determines the basis for the authorised application of forceful measures by a particular member state or the global community as the case may be. This challenge derives largely from IW's capacity of achieving its anticipated consequences without the normal application of force. Additionally, it must be emphasized that a notable severe case was found in Article 51 that recognises state's right in application of force as a self-defense against armed attack by the hostile powers, but does not specify what an "armed attack" is [45]. Other significant omissions include the words "aggression," "force," and "intervention." Any effort to set up an arms regulation regime will be futile and unsatisfactory unless these fundamental components of international law are clearly understood. These fundamental components of international law are clearly understood and defined. Without doubt, an unclear interpretations and definition of this fundamental components of global law, or any attempt in establishing weaponry or arms regulations regime may be unsuccessful.

7.0 Conclusion

This paper examined issues of armed hostilities by addressing the evolving policies, regulations and challenges of information warfare. The paper found that the regulations under the Law of Nations provides that contemporary weapons of warfare should be reviewed on the basis of legitimacy. This will contribute in terms of decision making in respect of its applications, safety and security of the civilian populations. Furthermore, there is need to appreciate the fact that this weapons, it's legalities, practicalities or usage appears to be difficult to be separated. The exploration of IW has revealed a multifaceted and evolving battlefield where actors deployed a range of tools to influence, disorganized and manipulates online messages to suit a selfish desire. It

e-ISSN 2821-3394

is crucial to distinguished IW from traditional C&C Warfare, understanding its insidious nature and the challenges in defending it. The analysis has highlighted key terms like disinformation, misinformation, cyberattacks; mental manipulations; Kompromat and shedding light on the Complexity of the IW landscape. The participants in this digital battlefield, including nation-states, non-government organizations; private individuals; politicians; security agencies, and terrorist organizations engaged in a constant struggle for control over information flow. The examination of tactics and techniques, such as false news, cyberwarfare; social media manipulations; deepfakes, underscores the diverse strategies employed in the realm of IW. From the weaponization of fake news to the subtle manipulations of social media algorithms, these tactics posed significant challenges to mankind around the globe. When navigating the ethical considerations surrounding IW, it becomes evident that its impact extends beyond the digital realm, shaping public opinion, influencing political landscapes, and even contributing to real-world events like the Rohingya Massacre in Myanmar. The paper finds that IW is contemporary warfare under LOAC which suggests that the applicable technique of IW should not depart from the test for necessity and proportionality as applied to similar weapons under LOAC.

Looking ahead, it is imperative to remained vigilant and proactive in countering the ever-evolving landscape of IW. Furthermore, ethical considerations, international cooperation, and technological advancements will play crucial roles in mitigating the risks associated with the misuse of information. By fostering a global understanding of IW and implementing responsible Practices, the international community can strive for a more secured and informed digital future. As a result, it is crucial for policymakers to develop comprehensive policies and regulations that address the evolving nature of information warfare. This includes investing in advanced cyber defence capabilities, fostering international cooperation to combat cyber threats, and promoting public awareness and education on digital literacy and media literacy. By taking these steps, policymakers and international organisations can better protect societies from the dangers of information warfare and ensure a safer and more secure digital future.

Therefore, the paper recommends that further studies into the policies, regulations; challenges, and ethical considerations raised by the existence of IW and how the freedom of speech of individuals might be adversely affected by all attempts made to crack down on disinformation campaigns and the spread of fake news. Furthermore, as several Countries around the globe still lacks an all-embracing regulation capable of protecting their respective information, it has become necessary for a stronger regulatory framework or guidelines that addresses user privacy through the creation of safer global environment for all and sundry.

8.0 Acknowledgments

The Authors are really grateful for the valuable assistance and support from the College of Law Library, Bowen University, Iwo Osun State, Nigeria and the University of Lay Adventists of Kigali, Rwanda. The authors were provided with all relevant materials in carrying out this research work. We accept all the errors and mistakes arising from this work.

9.0 References

[1]Exploring the Landscape of Cybercrime. Available at: https://www.researchgate.net/publication/215461179_Exploring_the_Landscape_of_Cybercrime Accessed Jan 02, 2024.

[2] Lawrence T. Greenberg et al. Information Warfare and International Law (1998).

[3] Cristian, Barna, The Road to Jihad in Syria: Using Socmint to Counter the Radicalization of Muslim Youth in Romania, in Countering Radicalization and Violent Extremism Amongst Youth to Prevent Terrorism (Marco Lombardi, 2015),193.

[4] Alexander Nitu, International Legal Issues and Approaches Regarding Information Warfare, in Proceedings of the 6th International Conference on Information Warfare and Security, 2011.

[5] Phillip A. Johnson, Is it time for a Treaty on Information Warfare? in Computer Network Attack and International Law in Michael N. Schmitt & Brian T. O'Donnell (eds.) 2010, 439.

[6] M.A. Hannan Bin Azhar & Thomas Edward Allen Barton, Forensic Analysis of Secure Ephemeral

Messaging Applications on Android Platforms, in Global Security, Safety and Sustainability: The Security Challenges of the Connected World, 2017, p.27.

[7] "Hostilities | How Does Law Protect in War? - Online Casebook" https://casebook.icrc.org/a_to_z/glossary/hostilities#:~:text=The%20term%20refers%20the%20physical,on%20the%20conduct%20of%20hostilities.

[8] Fred Aka Agwu, United Nations System, State Practice and the Jurisprudence of the Use of Force, Lagos, Malthouse 2005, p. 337.

[9] The British Manual of Military Law: Royal Warrant Governing the Maintenance of Discipline Among Prisoners of War; London, 1958.

[10] Geoffrey Best, Humanity in Warfare: The Modern History of International Law of Armed Conflicts, London, Weidenfeld and Nicolson, 1980, p. 309.

[11] Robert L. Bledsoe and Boleslaw A. Boczek, International Law Dictionary, Santa Barbara, Califf.: ABC-CLIO, 1987, p. 391.

[12] Cohen Avner et al. Nuclear Weapons and the Future of Humanity: The Fundamental Questions: Rowman and Littlefield Publishers,1986.

[13] Hays W. Parks, "Means and Methods of Warfare", (2006) 33 Geo. Wash. Int'l L. Rev. 3: 512.

[14] Alexander Satariano, "When Words Become Weapons: The Unprecedented Risks to Civilians from the Spread of Disinformation", 2022.

[15] Clay Wilson, Information Warfare and Cyberwar: Capabilities and Related Policy Issues, Washington, DC: Congressional Research Service, 2004, CRS-2.

[16] Gregory Rattray, Security in Cyberspace in Arms Control: Cooperative Security in a Changing Environment, ed. Jeffrey Larsen, Boulder, CO: Lynne Rienner Publishers, 2002, p. 312-313.

[17] NATO: Media - Disinformation - Security: Information Warfare, North Atlantic Treaty Organisation, 2022. Available at: https://www.nato.int/nato_static_fl2014/assets/pdf/2020/5/pdf/2005-deepportal4-information-warfare.pdf Accessed December 2, 2024.

[18] Tredinnick, L. Disinformation Warfare: Risks for Businesses (2023) Business Information Review, 40(3), 103-110.

[19] Douglas Waller, "Onward Cyber Soldiers", Time, August 21, 1995, pp. 38-46.

[20] Department of Navy, Policy Planning and Guidance for National Information Warfare, Command and Control, Washington DC: 16 February, 1995, 5.

[21] B. G Blair, Strategic Command and Control, Washington, D.C, The Brookings Institution, 2001.

[22] Yuchong, Li and Qinghu, Liu, "A Comprehensive Review Study of Cyber Attacks and Cyber Security: Emerging Trends and Recent Developments", (2021) 7 Energy Reports, 8176-8186.

[23] Jennifer Henderson, Psychological Manipulations and Cluster-B Personality Traits of Cult Leaders, Walden University, 2023.

[24] Angel N. Desai et al. "Misinformation and Disinformation: The Potential Disadvantages of Social Media in Infectious Disease and How to Combat Them", (2022) 74 Clin. Infect. Dis. 3:34-39.

[25] Hunt Allcott and Matthew Gentzkow, "Social Media and Fake News in the 2016 Election", (2017) 31 Journal of Economic Perspectives, 2: 211-36.

[26] Avast Business Team, What is the Cyber Kill Chain and How Does it Work? Avast Business Team, December 15, 2021.

[27] Sean Lyngaas, United States Government Agencies in Global Cyber Attacks By Russian Criminals, CNN, June 15, 2023.

[28] Robert Jervis, Cooperation Under the Security Dilemma, in Conflict After the Cold War: Arguments on Causes of War and Peace, ed. Richard Betts, New York: Pearson Longman, 2004, p. 382-384.

[29] James T. McKenna, “Tighter Security Urged for Defense Computers,” (1997) Aviation Week & Space

e-ISSN 2821-3394

Technology, 60.
[30] Michael J. Robbat, "Resolving the Legal Issues Concerning the Use of Information Warfare in the International Forum: The Reach of the Existing Legal Framework, and the Creation of a New Paradigm," (2000) Journal of Science and Technology Law.
[31] Warren Caldwell, Jr. "Promises, Promises", Proceedings, January 1996, 56.
[32] Legality of the Threat or Use of nuclear weapons, Advisory Opinion, 1996 I.C.J. July 8, 1996.
[33] Christian Perez, "Information Warfare in Russia's War in Ukraine: The Role of Social Media and Artificial Intelligence in Shaping Global Narratives", Foreign Policy, August 22, 2022.
[34] Kelly Aeschbach, Information Warfare Becoming a Critical Submarine Capability, April 8, 2024.
[35] Marie Baezner and Patrice Robin, Cyber and Information Warfare in the Ukrainian Conflicts, Centre for Security Studies, ETH Zurich, 2018.
[36] Stephan Hobe, Technological Development as a Challenge for the Development of Air and Space Law, in A New International Legal Order, Chia-Jui Cheng (ed.), 2016, p. 296.
[37] Prue Taylor, An Ecological Approach to International Law: Responding to the Challenges of Climate Change, 2008, p.259.
[38] Gillian Doreen Triggs & John Roberts Victor Prescott, International Frontiers and Boundaries: Law, Politics and Geography, 2008, p.402.
[39] Norman J. Medoff and Barbara Kaye, Electronic Media: Then, Now, and Later, 2016, p.9.
[40] Universal Declaration of Human Rights, G.A. Res. 217 (III) A, U.N. Doc. A/RES/217(III) (December 10, 1948).
[41] Harold M. White and Rita Lauria, "The Impact of New Communication Technologies on International Telecommunication Law and Policy: Cyberspace and the Restructuring of the International Telecommunication Union", (1995) 32 Cal. W. L. Rev. 1.
[42] Fisher, S. (2021, December 10). SolarWinds hack explained: Everything you need to know. WhatIs.com. Retrieved October 5, 2025, from https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know
[43] Gary M. Anderson and Adam Gifford, “Order Out of Anarchy: The International Law of War,” August 8, 2004.
[44] John P. Casciano, Address, Air Force Association National Symposia, Los Angeles, Ca., 18 October 1996. Available at: http://www.aef.org/pub/la9.asp. Accessed December 27, 2023.
[45] Department of Defense, Joint Vision 2020, Washington DC: Joint Chiefs of Staff, 2000, p. 6.

e-ISSN 2821-3394
