

HYBRID WARFARE – A CHALLENGE TO MODERN INTERNATIONAL LAW

GUERRA HÍBRIDA – UM DESAFIO AO DIREITO INTERNACIONAL MODERNO

Article received on: 7/4/2025

Article accepted on: 9/5/2025

Nguyen Linh Giang*

*Institute of State and Law, Vietnam Academy of Social Sciences, Viet Nam

Orcid: <https://orcid.org/0009-0002-6983-5076>

lgiang77@gmail.com

Abstract

In the context of a rapidly changing and volatile global security landscape, hybrid warfare has emerged as a new form of conflict, combining traditional military means with non-military tools such as cyberattacks, trade warfare, environmental warfare, and many other forms. Hybrid warfare, while recently a frequent topic in international political science and military science, is not a legal term. Therefore, it is impossible to apply conventional methods of definition and international legal norms to address activities in the form of this type of warfare. This term poses many challenges from the perspective of international law and the national laws of states in fields such as human rights law, the law of armed conflict, information security law, and international trade law. This article analyzes the concept and characteristics of hybrid warfare and examines some typical cases to highlight the challenges that it is posing to the international legal system. The article emphasizes the current legal gaps and proposes directions for the future development of international law and the strengthening of international oversight mechanisms.

Keywords: Hybrid Warfare. International Law. New Conflicts.

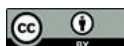
Resumo

No contexto de um cenário de segurança global volátil e em rápida mudança, a guerra híbrida emergiu como uma nova forma de conflito, combinando meios militares tradicionais com ferramentas não militares, como ataques cibernéticos, guerra comercial, guerra ambiental e muitas outras formas. Guerra híbrida, embora recentemente um tópico frequente na ciência política internacional e na ciência militar, não é um termo jurídico. Portanto, é impossível aplicar métodos convencionais de definição e normas jurídicas internacionais para abordar atividades na forma desse tipo de guerra. Este termo apresenta muitos desafios da perspectiva do direito internacional e das leis nacionais dos Estados em áreas como o direito dos direitos humanos, o direito dos conflitos armados, o direito da segurança da informação e o direito comercial internacional. Este artigo analisa o conceito e as características da guerra híbrida e examina alguns casos típicos para destacar os desafios que ela representa para o sistema jurídico internacional. O artigo enfatiza as lacunas jurídicas atuais e propõe direções para o desenvolvimento futuro do direito internacional e o fortalecimento dos mecanismos internacionais de supervisão.

Palavras-chave: Guerra Híbrida. Direito Internacional. Novos Conflitos.

1 INTRODUCTION

In the context of globalization and the digital age, conflicts between nations have become increasingly complex, multi-layered, asymmetrical, and difficult to identify. The concept of *hybrid warfare* emerged to describe a phenomenon that combines traditional



military means with non-military tactics. It is a new form of warfare that is difficult to recognize and can have consequences and impacts on national security that are no less severe than traditional military conflict.

Hybrid warfare is waged across military, diplomatic, economic, cultural, and social domains using various forms and means, including new technological environments. Furthermore, hybrid warfare is not always an activity of one state against another; it can be conducted by multiple states against one or more others, or even initiated and carried out by non-state actors. Hybrid warfare can affect many sectors and all societal platforms.

Particularly in the era of digital technology, issues of hybrid warfare related to cybersecurity have become extremely complex and difficult to prevent, highlighting the danger of this new type of conflict.

From a theoretical standpoint, hybrid warfare is a new term that has recently emerged in military and international political science. However, this concept has not yet appeared in international law. To this day, while scholars, researchers, and strategists from many countries around the world have named and provided various definitions for hybrid warfare, the term remains undefined in international law.

In this context, the question arises: Is the modern international legal system, including regulations on the use of force in international law (*Jus Ad bellum*), international trade law, and international human rights law and humanitarian law, capable of addressing this issue?

This article analyzes the concepts and characteristics of hybrid warfare, the legal challenges it presents, and proposes some trends for improvement to ensure the effectiveness of international law in this new context.

2 METHODOLOGY

This article is conducted on the basis of an interdisciplinary research approach, drawing from legal and international relations sciences.

First, the *analysis and synthesis method* is used to systemize the theoretical foundations and current international legal frameworks, including the United Nations Charter, the 1949 Geneva Conventions and their 1977 Additional Protocols, as well as

academic literature on hybrid warfare. This allows for an analysis of the development of the "hybrid warfare" concept and an identification of its basic characteristics.

The *comparative legal method* is also applied to contrast modern international legal norms with the real-world practice of hybrid warfare that has occurred in many places around the world, such as the 2014 Crimea event, the 2023 Israel-Hamas conflict, and the current Russia-Ukraine war. This comparison helps to identify the gap between legal provisions and the reality of modern warfare, thereby highlighting the challenges for international law.

The *case study method* is also employed with several typical cases to illustrate the diversity and complexity of this new form of warfare.

Finally, the *secondary sources analysis method* is used to analyze the theoretical underpinnings of the article while staying close to practical realities, thereby proposing feasible legal solutions.

3 DISCUSSIONS

3.1 Concept and characteristics of hybrid warfare

"Hybrid warfare" is a term that has been widely used in recent years globally (Robert, 2018; Bettina, 2018; Erik and Patrick, 2016; Waseem, 2020; Ofer, 2018). This term describes modern conflicts in which state or non-state actors use a combination of conventional and unconventional tactics and strategies to achieve their objectives. Although the term has become popular in recent years, U.S. military scholars have been discussing similar concepts for decades, laying the groundwork for the development of hybrid warfare theory.

In the late 1990s, Thomas Huber (Thomas, 2022) wrote about the theory of *Compound Warfare*, a concept related to shaping the understanding of hybrid warfare. This concept refers to combining the use of both conventional and irregular forces, such as guerrillas or militias, to fight an enemy. In compound warfare, irregular forces play a vital supporting role for the regular army by providing intelligence, logistics, and even soldiers, while also denying the enemy access to these resources (Thomas, 2022).

It is important to emphasize that Huber and other proponents of the compound warfare concept do not see it as an entirely new phenomenon (Ofer, 2018). Instead, they

view it as a strategic model that has existed throughout history, where conventional and irregular forces work together. Through studying the history of warfare, Huber has shown that this combination often provides a significant advantage, allowing the weaker side to confront and even defeat an enemy that is militarily stronger in conventional terms (Ofer, 2018). Therefore, he believed that compound warfare would continue to be a popular strategy in the future, especially in asymmetric conflicts.

In addition, while not directly mentioning the term "hybrid warfare," the U.S. National Defense Strategy (NDS) of 2005 also played an important role in shaping its content. The NDS emphasized the need to adapt to a world where state and non-state actors use a combination of conventional and unconventional tactics and strategies to achieve their goals. Although it did not use the specific term, the NDS recognized the complex and diverse nature of modern conflicts, laying the groundwork for the development of hybrid warfare theory in the following years. The NDS acted as a crucial catalyst, driving the development of hybrid warfare theory. By acknowledging that the lines between different forms of warfare were blurring and that adversaries with the ability to combine various tactics and strategies were emerging, the NDS laid the foundation for building a new framework to understand and counter the complex challenges of modern warfare.

Although Hoffman was the first to widely use the term "hybrid warfare" in military circles starting in 2006, the origin of the term is older. In fact, Thomas R. Mockaitis used the term "hybrid warfare" as early as 1995, albeit with a slightly different meaning from the context and manner in which Hoffman later redefined it (John and Martijin, 2021). According to Hoffman, hybrid warfare is the combination of different forms of warfare, including conventional capabilities, irregular tactics and formations, terrorism, and criminal acts (Hoffman, 2006). This concept was shaped by various influences, including theories of unrestricted warfare, fourth-generation warfare, compound warfare, and the 2005 U.S. National Defense Strategy, as well as the influence of other scholars (Hoffman, 2006). Nevertheless, the concept of hybrid warfare developed by Hoffman also shows significant differences, creating its unique character in military theory. Hybrid warfare does not describe a completely new phenomenon, but it provides a feasible approach to the cognitive aspects of the increasing complexity of combat operations, thereby offering practical solutions that can be applied depending on the circumstances. Unlike previous theories that could be abstract or highly theoretical,

Hoffman's approach focuses on practicality. It defines hybrid warfare and complex threats as military problems that can be solved with military measures, with appropriate doctrine, training, and equipment.

Currently, a number of international organizations and countries have begun to address and study hybrid warfare, especially following the complex events in the Crimean Peninsula and Russia's actions since 2014. Russia's moves have awakened Western nations and sparked debates about the future of European security and how to counter various threats. In the same year, the North Atlantic Treaty Organization (NATO) used the term hybrid warfare to describe Russia's actions in Crimea (NATO, 2015).

In the national defense strategies of many countries around the world, such as the UK, the US, Singapore, and Australia, there is also a trend of states using military, paramilitary, and non-military measures to threaten the security of other nations (Nguyen, 2023).

International organizations like NATO, the European Union (EU), and the United Nations (UN) are also paying attention to hybrid warfare issues. However, to date, the UN has not taken an official stance on hybrid warfare. Although some discussions related to hybrid warfare have taken place at the UN Security Council since 2016, many experts still believe that the UN maintains an outdated approach to conflict and that "hybrid warfare is a threat to international peace and security" (Michele, 2017).

It is evident that the understanding of hybrid warfare has changed the world's perception of war and the battlefield. In the past, when people thought of war, they often imagined bombs, casualties, and armed conflict between nations and military forces. To speak of war was to speak of violence and the military. The battlefield was a specific, physical location where military combat occurred. However, with the development of various forms of hybrid warfare, the concepts of war and the battlefield have clearly changed significantly.

Although the concept of hybrid warfare still involves armed conflict, military activities, and a battlefield that may be a specific location, war can also encompass non-military and non-violent actions, such as the trade war between the United States and China. The definition of war today is considered a "gray zone" due to its ambiguity. "Gray zone warfare" is understood as using political influence, economic coercion, cyberspace, information operations, and even a military posture to affect an adversary, their allies,

and their partners. War today is many times broader than the concept found in dictionaries (Australian Army Research Centre).

According to the understanding that the battlefield is where war takes place, it is clear that as the concept of war changes, the concept of the battlefield changes as well. In multi-faceted, multi-force warfare, the battlefields are also diverse. In addition to physical battlefields in the traditional sense—on the ground, in the air, and at sea—the battlefield can be in cyberspace, a borderless battlefield that is not confined to any national territory (e.g., information warfare, trade warfare). In other words, in hybrid warfare, sometimes it is not a matter of defining the battlefield but rather of defining the means by which the war is conducted.

At the same time, it can be seen that when the battlefield becomes borderless, issues related to national sovereignty in hybrid warfare also become vague and difficult to define. Typically, national sovereignty is understood as a state's power over its territory and population. However, in the modern world, under the multifaceted impact of international relations, national sovereignty is also understood as the ability to control and manage a nation's affairs such as security, economy, and the environment. Under the impact of hybrid warfare, such as information warfare, economic warfare, cyber warfare, and environmental warfare, the concept of national sovereignty has clearly expanded beyond how it was previously defined.

From the above analysis of the concept of hybrid warfare, it can be seen that hybrid warfare has some commonalities but also many differences from traditional warfare. It can be observed that, because they are both forms of warfare, they share some common characteristics: In terms of *objectives*, both types of warfare aim to achieve certain political, military, or economic gains or to seize a piece of land or a certain population. In terms of the *use of force*, while traditional warfare is purely about the use of force, hybrid warfare combines the use of force with other forms to achieve its goals, but overall, both forms of warfare involve force. In terms of *causing damage to the opponent*, both forms of warfare cause damage to the opponent; both traditional and hybrid warfare can result in damage to people and property. In addition to these common characteristics, hybrid warfare has its own distinct features compared to traditional warfare in terms of its methods, the time and space it takes place, the actors involved, and the strategies, tactics, and means used.

Based on the research by Thomas Huber and Hoffman, we can summarize some key characteristics of hybrid warfare:

First, *its diverse nature*. Hybrid warfare can involve a variety of forces and nations, combining different methods of warfare and shifting between traditional and unconventional means and vice versa.

Second, *the actors can be state or non-state entities*. The actors carrying out hybrid warfare are very diverse. The enemy attacking one or more states could be a single country, multiple countries, or even non-state/transnational groups and organizations like Hezbollah or the Islamic State (ISIS).

Third, *a heavy reliance on technology and a close link to information and propaganda operations*. The weapons used in hybrid warfare can be modern military arms, or they can be non-military methods that rely on technology, such as internet propaganda, spreading fake news, and influencing domestic and international media. Often, these non-military actions are more successful and have a more profound impact in modern warfare.

Fourth, *it is often quiet, subtle, and sometimes difficult to detect*. Hybrid warfare activities are often carried out covertly. Unlike traditional warfare with declared hostilities and gunfire, hybrid warfare is sometimes quiet and smokeless. Many countries may not even realize they are under attack until they suffer serious damage.

Fifth, *the difficulty of establishing a legal basis to classify non-military actions as an attack*. It is often very difficult to define an attack because it's hard to determine what happened first, what happened later, and who is responsible. This highlights a gap in international law and a challenge to international legal frameworks, raising questions about the validity of the rules of international law and modern international relations.

In the context of modern security, traditional warfare methods are rarely used in isolation and are more often combined with various forms of hybrid warfare. A clear understanding of the differences, similarities, and unique characteristics of hybrid warfare compared to traditional warfare will help policymakers and military strategists develop more suitable strategies for national security.

3.2 The current international legal framework for regulating hybrid warfare activities

Hybrid warfare has profound and lasting impacts. It not only causes physical and human damage but can also leave deep and long-term social, economic, and psychological consequences. Hybrid warfare can aim to weaken an enemy's military strength, destroy critical infrastructure, and gain territorial control. Additionally, it can target non-military objectives, influencing the psyche and will of the populace, undermining their support for the government, and causing social division and instability. This instability, division, and loss of trust can persist for years after the conflict ends. In a constantly changing world, hybrid warfare is a multidimensional threat, causing severe consequences and profound impacts on global peace and security. However, the international legal basis for regulating hybrid warfare activities is not yet clear or unified.

3.2.1 The united nations charter and fundamental principles

The UN Charter, particularly the provisions in Article 2(4) on the prohibition of the threat or use of force, is applied to prevent aggressive acts in hybrid wars. This prohibition applies not only to traditional wars but also includes acts that violate national security through non-military means like cyber or information warfare. Furthermore, Article 51 of the Charter outlines the right of states to self-defense in case of an armed attack. This presents a challenge when dealing with hybrid warfare, as it is difficult to clearly define what constitutes an "armed attack" when non-military actions are carried out below the threshold of an armed conflict. The fundamental principles of international law, including the principle of non-interference in internal affairs, the principle of respect for sovereignty, and the principle of peaceful dispute resolution, play a crucial role in responding to hybrid warfare.

3.2.2 International humanitarian law

The provisions of International Humanitarian Law (IHL), including the 1949 Geneva Conventions and their Additional Protocols, are key to protecting civilians and other vulnerable groups in hybrid warfare. The application of IHL in this context aims to

protect civilian objects and limit unnecessary human casualties and material damage. Fundamental principles such as the distinction between military and civilian targets, proportionality in attacks, and the prohibition of indiscriminate weapons are all applicable in hybrid warfare, helping to limit the impact of the conflict on civilians and reduce unnecessary suffering.

3.2.3 International human rights law

The application of International Human Rights Law (IHRL) in the context of hybrid warfare is a crucial area because hybrid warfare doesn't just affect military aspects—it also deeply impacts fundamental human rights and freedoms. In hybrid warfare, unconventional methods like cyber warfare, information warfare, and psychological or economic influence can violate the human rights of civilians without an official armed conflict taking place.

Unlike International Humanitarian Law, which applies only in situations of armed conflict, IHRL applies at all times, in both peace and war. This gives IHRL a broader scope when applied to the actions of hybrid warfare, especially since these actions often don't trigger a full-scale armed conflict but still affect civilians and their basic rights. In hybrid warfare, many fundamental human rights can be seriously impacted or violated. The right to life and personal safety can be threatened by social instability or violence from indirect forms of influence. Additionally, the right to privacy is often violated through cyberattacks aimed at collecting personal data. The rights to freedom of information and expression are also threatened by misinformation campaigns that obstruct people's access to accurate information.

3.2.4 International environmental law

Applying International Environmental Law (IEL) to hybrid warfare requires protecting the environment in situations where the impacts are more indirect and difficult to identify than in traditional warfare. IEL sets rules for environmental protection in conflict situations. However, because hybrid warfare often takes place below the threshold of an official armed conflict, applying these regulations is a major challenge.

To address hybrid warfare, the international community is seeking to expand the scope of environmental protection rules to include indirect forms of attack. For example, the UN and environmental protection organizations have issued guidelines on the responsibility of states to protect the environment from cyberattacks and to enhance monitoring of environmental impacts from other hybrid warfare activities. IEL in the context of hybrid warfare may need to be adjusted to ensure that states have an obligation to protect the environment even during these unconventional forms of conflict.

3.2.5 International law on state responsibility

The attribution of State Responsibility in hybrid warfare is a complex issue due to the unconventional and multifaceted nature of this type of conflict. Under international law, a state is held legally responsible for its actions when it violates its international obligations, which include respecting human rights, protecting sovereignty, and maintaining international peace. However, in hybrid warfare, attacks often occur through non-military means, such as cyber or information warfare, making it difficult to identify the direct actor and, consequently, to attribute responsibility and identify the violation.

States engaged in hybrid warfare often use non-governmental actors or individuals, acting anonymously or through indirect means, to avoid legal responsibility. International law on state responsibility requires states to be held accountable for the actions of individuals or organizations acting under their direction, control, or with their permission. This means that if a state can be shown to have participated in or supported acts that violate rights or cause instability in a hybrid war, that state may be held responsible.

In this context, the international community is faced with the need to update and adjust the rules of international law on state responsibility to meet the challenges posed by hybrid warfare. This could include establishing clearer criteria for responsibility for cyberattacks, misinformation, and other non-military acts to ensure transparency and accountability for states in maintaining international peace and security.

Recently, some international organizations have also issued guidelines related to hybrid warfare. A prime example is the NATO-sponsored Tallinn Manual on the International Law Applicable to Cyber Warfare, which provides recommendations and analysis on how humanitarian law and international principles apply to cyberattacks.

Similarly, the International Committee of the Red Cross (ICRC) Guidelines on cybersecurity and the protection of civilians in cyber conflicts set out principles for protecting civilians and civilian infrastructure during cyberattacks. The EU has also issued cybersecurity framework guidelines that address the responsibility of member states to protect cyberspace and build resilience against destabilizing external activities. These soft-law documents, although not legally binding, help to establish international norms of conduct and raise awareness of states' responsibilities when conducting or preventing hybrid warfare.

The application of international law to hybrid warfare still faces many challenges, including the ambiguous nature of this type of conflict, the rapid development of technology, and the lack of international consensus. However, the international community is striving to improve the international legal framework to meet these new demands. Strengthening international cooperation, developing soft law, and increasing awareness of international law are all crucial solutions to counter the challenges of hybrid warfare and protect global peace and security.

3.3 Challenges of hybrid warfare to international law

3.3.1 Challenges to the principle of "prohibition on the use of force or threat of force" in international law

International law has always affirmed the restriction on the use of force to protect peace. There are two parts of international law that regulate the use of force: The first legal framework addresses when the use of force between states is permissible (*Jus ad bellum*). The second legal framework regulates how a state uses force in an armed conflict (*Jus in bello*). However, modern warfare is becoming increasingly complex with the emergence of hybrid warfare, which combines various tactics such as cyberattacks, legal warfare, and the use of irregular armed groups. This creates new challenges for international law in regulating the use of force in international relations.

Article 2(4) of the UN Charter is a key provision that prohibits not only war but all forms of illegal use of force between states. This principle is specified in the 1970 Declaration, which emphasizes the prohibition of aggressive war, the prohibition of using force to resolve disputes, the prohibition of retaliation with force, the prohibition of

infringing upon states' right to self-determination, and the prohibition of supporting terrorism (UN General Assembly, 1970). However, this rule also has exceptions, allowing the use of force in cases of collective action by the United Nations or legitimate self-defense as set forth in Chapter VII and Article 51 of the UN Charter. Furthermore, the legality of humanitarian intervention within the international legal framework on the use of force remains a controversial issue among both academics and policymakers (Christine, 2014).

The concept of "force" in international law is often associated with military force, meaning the use of military weapons and equipment. Some views suggest that "force" should be interpreted more broadly to include political and economic measures such as sanctions, political pressure, etc. However, this approach has not yet gained widespread support (Ofer, 2018). Instead, the use of non-military measures like economic sanctions or political pressure to influence another state is usually examined under the principle of non-interference in internal affairs, rather than as a prohibited use of force under Article 2(4) of the UN Charter (Yoram, 2011).

Thus, while the UN Charter aims to prevent the use of force, this does not mean that all acts of force are considered illegal. The crucial issue lies in the intent of the state using force. For example, if a military unit accidentally crosses a border or a missile is launched by mistake, it may be a violation of another state's sovereignty, but it is not necessarily considered an illegal use of force in the spirit of Article 2(4) of the Charter (Andrew, 2021). Determining whether an act violates international law on the use of force depends heavily on the context and the severity of the specific action.

3.3.2 Challenges to the right of self-defense and its limits

While Article 2(4) of the UN Charter prohibits the use of force in general, Article 51 of the Charter permits states to use self-defense in case of an armed attack. However, Article 51 also places limits on this right. It can only be invoked until the UN Security Council intervenes. Furthermore, states have an obligation to immediately report any acts of self-defense to the Security Council. Failure to report does not automatically nullify the right to self-defense, but it could put the state at a disadvantage in a later legal dispute, as it may be considered evidence that the use of retaliatory force exceeded the bounds of legitimate self-defense (Christine, 2014).

So, what form of "armed attack" can justify an act of self-defense under international law? This question involves three controversial issues in academic research (Dinstein, 2011): First, what type of force constitutes an armed attack? Second, does providing support to an armed group fighting in another country constitute an armed attack? And third, what is the legal difference when an attack is carried out by a state versus a non-state actor? In the context of hybrid warfare, the question arises whether a cyberattack can be considered an "armed attack." This issue becomes even more complex in the modern era, as armed conflicts are increasingly seeing the involvement of non-state armed groups (NSAGs). How should we handle cases where NSAGs in one state launch an armed attack against another state?

3.3.3 Challenges to the role of the UN security council

In terms of preventing hybrid warfare, the Security Council plays a key role in maintaining international peace and security under Chapter VII of the UN Charter. The Council's authority is often used to prevent hybrid wars through sanctions. According to Article 41 of the Charter, the Security Council has the right to impose necessary provisional measures (such as economic embargoes, asset freezes, or travel bans) on states or individuals whose actions create instability or a risk of war. These measures are intended to weaken the resources of the actors and exert political pressure to prevent the escalation of a conflict (Andrea, 2011). For example, in many conflicts in the Middle East and Africa, the Security Council has imposed arms embargoes on armed groups to limit their ability to carry out attacks. Additionally, the Security Council can dispatch peacekeeping or special missions to prevent the outbreak of conflict, especially in areas of high tension (Håvard *et al.*, 2019). These missions can monitor ceasefires, protect civilians, and build a stable environment, thereby preventing the escalation of complex conflicts (Lise and Anjali, 2017).

In cases of ongoing conflict, the Security Council's authority plays a vital role in resolving the conflict through forms of intervention like authorizing the use of force. According to Article 42 of the UN Charter, the Security Council can authorize member states or international coalitions to use force to maintain or restore peace. This is often applied in complex conflicts where armed intervention is necessary to protect civilians, prevent escalating violence, or defeat armed non-state groups. However, a major issue is

that in many cases, the Security Council fails to reach a consensus in resolving global conflicts, and the permanent members of the Security Council frequently use their *veto power* to override resolutions. For instance, since the conflict between Russia and Ukraine began in 2014 and escalated in 2022, Russia has repeatedly used its veto to block Security Council draft resolutions (Anne, 2023). Similarly, many resolutions calling for a resolution to the Syrian conflict since 2011 have been vetoed by either Russia or China (Saira, 2012). This shows the deep disagreements among the major powers in the Security Council when it comes to resolving issues related to war, including hybrid warfare. It reflects how conflicts of national interest and geopolitical influence can overshadow international legal principles.

3.4 Recommendations for improving international law

First, Hybrid warfare has become a common term for international conflicts today. Instead of only using military force like traditional warfare, it combines various methods, both military and non-military (such as cyberattacks, information warfare, and economic warfare), to achieve political goals without a formal declaration of war. However, hybrid warfare is very difficult to define clearly, which makes applying international law complicated. For example, when one country attacks another's power grid, is that considered an act of war? This ambiguity creates loopholes that states can exploit, making it difficult to prevent and address violations of international law. Therefore, there is a need for a clear legal definition of hybrid warfare. This could be established in an international treaty adopted by the United Nations in the future.

Second, redefining the concept of "force" in international relations is a necessary requirement in the modern context, as forms of conflict have changed significantly since the UN Charter was enacted. Cyberattacks and hybrid warfare, with their ability to cause serious damage without the use of traditional military weapons, have blurred the line between war and peace, posing major challenges to international law in regulating the use of force. However, there is still no consensus on expanding the definition of "force" to include non-military measures. This requires discussion and agreement within the international community, especially from bodies like the United Nations and the International Court of Justice. At the same time, it is also necessary to expand the concept

of conflict in international law and recognize hybrid forms of conflict to create appropriate mechanisms for protecting victims of these conflicts.

Third, from the perspective of international law, information warfare (IW) poses significant legal challenges due to its unique nature, including its physical and invisible impacts on state and non-state actors. The complexity of IW, especially with the development of cyber technology and global connectivity, requires a legal framework that can address these new forms of conflict. Meanwhile, the current international legal framework is insufficient to regulate IW (Jason, 2001). A prime example is Russia's influence campaign on Facebook during the 2016 US presidential election. Allison Denton argues that even though Russia's 2016 Facebook influence campaign violated US national law, it is very difficult to legally conclude that it violated international law (Allison, 2019). This is due to the limitations of the current legal framework in addressing cyber and digital influence operations. Therefore, there is a need to establish international legal norms for cyberattacks. An international convention on cyberattacks is needed, rather than just relying on the Tallinn Manual.

Fourth, states, regional, and international organizations need to work to build international codes of conduct related to cybersecurity and information warfare, combined with international human rights standards. These rules should be based on international human rights norms and uphold the principles of legality, necessity, proportionality, transparency, and accountability. At the same time, principles such as non-discrimination, the protection of civilians and critical infrastructure, and respect for the digital sovereignty of states are also important principles that need to be protected.

Finally, there is a need for an international oversight mechanism and a strengthened role for the UN Security Council, the International Court of Justice, and UN investigative commissions in handling issues related to hybrid warfare. Perhaps due to the layered, ambiguous, and difficult-to-trace nature of hybrid warfare, individual states are often unable to control it, while current international law still lacks a mechanism strong enough to react in a timely manner. Therefore, an international oversight mechanism is an essential necessity at this time. These mechanisms need to operate actively and effectively to ensure that international law is not rendered ineffective by the challenges of hybrid warfare with its multi-layered oversight mechanisms. Although it is difficult, this can be seen as the most feasible path at present to both maintain the

effectiveness of international law and protect people and the rules-based international order.

4 CONCLUSION

This study emphasizes that international law plays a vital role in maintaining global order and stability, especially when facing the challenges of hybrid warfare. International legal principles, particularly the prohibition on the use of force (except in cases of self-defense or with UN authorization) outlined in Article 2(4) of the UN Charter, aim to prevent and control conflict. However, hybrid warfare's uniquely complex nature, involving non-state actors and modern technology, poses a significant challenge to international law in determining what constitutes an "armed attack" to trigger the right of legitimate self-defense.

Hybrid warfare is a new challenge for the world and for modern international law. It blurs the lines between war and peace, and between military and non-military actions, rendering traditional norms obsolete. To maintain its effectiveness and legitimacy, the international legal system must adapt flexibly while also upholding its core principles of protecting civilians and limiting the consequences of war.

Furthermore, international law still leaves some important issues unaddressed in this context, especially a legal definition of hybrid warfare. There is currently no unified definition in international law for this type of conflict due to its diverse nature and the combination of military and non-military actions by both state and non-state actors. This requires a more specific legal concept for effective regulation and management.

This study recommends the concept of "force" needs to be broadened to include unconventional forms of attack, such as cyberattacks or economic measures, when they can cause damage equivalent to military force. Issues related to information and communication technology in hybrid warfare, including information warfare and cyberattacks, require new international legal provisions to control actions that impact the morale and will of an adversary without causing direct casualties. New technologies like artificial intelligence and autonomous weapons also pose major challenges to international law, as their potential for widespread impact and the risk of damage they can cause in hybrid warfare are not yet fully regulated.

REFERENCES

- Allison Denton, 2019, Fake News: The Legality of the Russian 2016 Facebook Influence Campaign, *Boston University International Law Journal*, 183.
- Andrea Charron, 2011, *UN Sanctions and Conflict: Responding to Peace and Security Threats*. Routledge.
- Andrew Clapham, 2021, *War*, Oxford University Press.
- Anne Peters, 2023, *The war in Ukraine and the curtailment of the veto in the Security Council*, *Revue Européenne du Droit*, June 2023.
- Australian Army Research Centre, *What is War? Defining War, Conflict and Competition*, [What Is War? Defining War, Conflict and Competition, Australian Army Research Centre \(AARC\)](#).
- Bettina Renz, 2018, Russia and “Hybrid Warfare”, *Contemporary Politics*, Routledge, DOI: 10.1080/13569775.2016.1201316.
- Christine Gray, 2014, The Use of Force and the International Legal Order in Malcolm D Evans (ed), *International Law*, Oxford University Press, 623–626.
- Erik Reichborn-Kjennerud and Patrick Cullen, 2016, What Is Hybrid Warfare?, Norwegian Institute of International Affairs (NUPI).
- Håvard Hegre, Lisa Hultman and Håvard Møkleiv Nygård, 2019, Evaluating the Conflict-Reducing Effect of UN Peacekeeping Operations, *The Journal of Politics*, 215.
- Hoffman, 2006, *Complex Irregular Warfare: The Next Revolution in Military Affairs*, Elsevier Limited on behalf of Foreign Policy Research Institute.
- Jason Barkham, 2001, Information Warfare and International Law on the Use of Force, *New York University Journal of International Law and Politics*.
- John G.L.J. Jacobs and Martijn W.M. Kitzen, 2021, Hybrid Warfare, *Oxford Bibliographies*, 22/9/2021), <<https://www.oxfordbibliographies.com/display/document/obo-9780199743292/obo-9780199743292-0260.xml>>.
- Lise Morjé Howard and Anjali Kaushlesh Dayal, 2017, The Use of Force in UN Peacekeeping. *International Organization*, 72 (1), 71-103, <https://doi.org/10.1017/S0020818317000431>.
- Michele J.Sison, 2017, *Remarks at a UN Security Council Open Arrria- Formula Meeting on "Hybrid wars as a threat to international peace and security"*, 31/3/2017, <https://usun.usmission.gov/remarks-at-a-un-security-council-open-arria-formula-meeting-on-hybrid-wars-as-a-threat-to-international-peace-and-security/>.

National Defense Strategy of the United States, 2005, *The United States Department of Defense*, March 2005 <<https://history.defense.gov/Historical-Sources/National-Defense-Strategy/>>.

NATO, *Wales Summit Declaration*, 13/9/2015

Nguyen Thi Lan Huong, 2023, "Hybrid Warfare" in the South China Sea: The Issue of Using Maritime Militia from the Perspective of International Law, a PhD thesis in international law, Diplomatic Academy of Vietnam.

Ofer Fridman, 2018, *Russian 'Hybrid Warfare': Resurgence and Politicization*, Oxford University Press.

Robert Johnson, 2018, Hybrid War and Its Countermeasures: A Critique of the Literature, *Taylor & Francis*, Volume 29, 2018, Issue 1, <https://doi.org/10.1080/09592318.2018.1404770>

Saira Mohamed, 2012, *The UN Security Council and the Crisis in Syria*, *American Society of International Law*, Volume 16, Issue 11.

Thomas H. Huber, 2002, *Compound Warfare: That Fatal Knot*, US Army Command and General Staff College Press.

UN General Assembly, 25th Sess. 1970, 'Declaration on Principles of International Law Concerning Friendly Relations and Cooperation among States in Accordance with the Charter of the United Nations.' <<https://digitallibrary.un.org/record/202170>>.

Waseem Ahmad Qureshi, 2020, The Rise of Hybrid Warfare, *Notre Dame Journal of International & Comparative Law*, 173,

Yoram Dinstein, 2011, *War, Aggression and Self-Defence*, 5th edn, Cambridge University Press.