ISSN-Print: 2079-3901
ISSN-Online: 3005-396X

Navigating Legal Challenges in Drone Cyber-attacks: The Case of the Kurdistan Region of Iraq

Asst. Prof. Dr. Sanh Shareef Qader
Department of Law, Faculty of law, Political Sciences and Management, Soran University, Kurdistan Region, Iraq
Email: sanh.qadir@soran.edu.iq

ID No. 2753	Received: 13/10/2024	Keywords:
(PP 1 - 30)	Accepted: 09/12/2024	Drone Cyberattacks, Sovereignty, Countermeasures, Responsibility of States for Internationally Wrongful Acts(RSIWA).
https://doi.org/10.21271/zjlp.23.38.1	Published: 04/06/2025	

ABSTRACT

This paper provides an international law perspective on the complexities of addressing drone cyberattacks against the KRI. It seeks to explore how drone cyber-attacks intersect with established principles such as state sovereignty, the prohibition of intervention, and the prohibition of the use of force under international law. It applies relevant frameworks like the Tallinn Manual, the Articles on Responsibility of States for Internationally Wrongful Acts (RSIWA), and the UN Charter. This paper examines the legal foundation of countermeasures, including diplomatic, economic, and cyber responses, within the context of the KRI's cooperation with the Iraqi federal government. Additionally, it explores how ICJ and the United Nations Security Council (UNSC) can respond to such attacks. Based on a qualitative research method, this study incorporates a review of legal documents, case studies, and expert opinions to assess drone cyberattacks in the framework of international law. The research also emphasizes the issues of proportionality and necessity in countermeasures, while highlighting the political and diplomatic constraints faced by the Kurdistan Region due to its relationship with the Iraqi state. The findings indicate that while the KRI is capable of implementing defensive strategies, determining appropriate international responses requires careful consideration of both legal norms and geopolitical factors.

ISSN-Print: 2079-3901
ISSN-Online: 3005-396X

List of Abbreviations

UN	**United Nations**
RSIWA	**Responsibility of States for Internationally Wrongful Acts**
UNSC	**United Nations Security Council**
U.S.A	**United States of America**
ICJ	**International Court of Justice**
IHL	**International Humanitarian Law**
ICCPR	**International Covenant on Civil and Political Rights**
LOAC	**Law of Armed Conflicts**
IBA	**International Bar Association**
KRI	**Kurdistan Region of Iraq**
KRG	**Kurdistan Regional Government**

ISSN-Print: 2079-3901
ISSN-Online: 3005-396X

1. Introduction

The Kurdistan Region of Iraq (KRI) has been facing myriad, complex legal and geopolitical problems, especially in respect to the position it maintains in view of drone cyberattacks and the greater standing within the framework of international law. The paper accordingly will attempt to give a critical analysis of the legal frameworks and responses by the international community relevant to drone cyberattacks targeting the KRI, with a prime focus on the interlinkages between sovereignty, state responsibility, and the role played by countermeasures under international law. Consequently, the central aim of this research is to assess the applicability of international legal principles, which include the Articles on the Responsibility of States for Internationally Wrongful Acts(RSIWA)[1], the Tallinn Manual[2], and the UN Charter, to the unique problems created by drone cyberattacks. Moreover, this paper analyses consequences of these legal frameworks for the Kurdistan Region, considering its status as the federated region part of the Federal Republic of Iraq and practical difficulties this region faces when trying to prevent such attacks. The importance of this study is underscored by its comprehensive approach to comprehending the legal and practical aspects of managing drone cyberattacks in a region characterized by political intricacy and regional tensions.

---

[1]**The Responsibility of States for Internationally Wrongful Acts (RSIWA) is a set of draft articles developed by the International Law Commission (ILC) that outlines the principles governing the responsibility of states for breaches of international law. Adopted during the ILC's fifty-third session, these articles serve as a framework for understanding how states can be held accountable for actions that violate their international obligations. However, its status as a draft means it is not legally binding on states unless they choose to incorporate its principles into their national law or international agreements. The UN General Assembly took note of these draft articles in its Resolution A/RES/56/83 on December 12, 2001, recognizing their significance in international law. See further International Law Commission. Responsibility of States for Internationally Wrongful Acts, [Online]. Supplement No. 10 (A/56/10), 2001. Last Accessed 19 November 2024 at: https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf .**

[2]**Tallinn Manual 2.0 expands on the highly influential first edition by extending its coverage of the international law governing cyber warfare to peacetime legal regimes. The product of a four-year follow-on project by a new group of 19 renowned international law experts, it addresses such topics as sovereignty, State responsibility, human rights, and the law of air, space, and the sea. Tallinn Manual 2.0 identifies 154 'black letter' rules governing cyber operations and provides extensive commentary on each rule. Although Tallinn Manual 2.0 represents the views of the experts in their personal capacity, the project benefited from the unofficial input of many States and over 50 peer reviewers. See further Schmitt, M.N. (2013) Tallinn Manual on the International Law Applicable to Cyber Warfare. {Online}. Vol. 141. Cambridge: Cambridge University Press.https://www.penncerl.org/wp-content/uploads/2021/12/6481-tallinn-manual-on-the-international-law-applicable.pdf. And Schmitt, M. N. (2017), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*(Cambridge University Press).https://assets.cambridge.org/97811071/77222/frontmatter/9781107177222_frontmatter.pdf.**

ISSN-Print: 2079-3901
ISSN-Online: 3005-396X

The study presents, with much clarity, how the Kurdistan Region and Iraq will go through these violations smoothly, whether in the realms of diplomacy, economics, or cyberspace, which is the epitome of this work. It highlights that well-defined international norms of behavior and mechanisms to guide responses to cyberattacks become imperative. This, in turn, will be a contribution to the wider debate on cyber-sovereignty and state responsibility. This work provides valuable insight into the application of international law to modern-day cyber threats and puts forward some recommendations to improve legal and policy frameworks in better protecting vulnerable areas, like that of the KRI, against newly arising security challenges. A basic research question that orients this study is: How can international legal frameworks and countermeasure mechanisms be effectively utilized with respect to the challenge posed by drone cyberattacks in the Kurdistan Region, given its semi-autonomous nature within the Federal Republic of Iraq? The value of this research extends beyond the context of the Kurdistan Region of Iraq, adding as it does to the broader debate on cyber sovereignty and international law. The research demonstrates the existing gaps and limitations of current international norms and practices in respect of how governments address drone cyberattacks through a review of practical and legal issues. In this respect, the study underscores that clear and enforceable legal thresholds become imperative for guiding state responses with a view to limiting any potential escalation of conflict into the cyber domain. This in-depth analysis aims to feed the quest for clues with regard to the problems faced by Kurdistan Region and Iraq when dealing with the complex modern-day problem of cyber warfare. In this regard, the research question will investigate the assessment, effectiveness, and efficiency of countermeasures involved to further advance international legal mechanisms and enhance our understanding of state responsibility for drone cyberattacks.

2. Research Methodology

This paper employs a qualitative research methodology to examine international legal frameworks and countermeasure mechanisms related to drone cyberattacks on the KRI. The study carefully conducts a critical literature review of key legal texts, including RSIWA, the Tallinn Manual, and the UN Charter, establishing the foundational theoretical framework for the paper. It explores specific case studies of drone cyberattacks on the KRI, analyzing their impacts and the region's responses within both Iraqi federal and international legal contexts. Additionally, the research includes a comparative analysis of international practices and legal responses to similar attacks, drawing on scholarly arguments and existing literature to identify effective countermeasures. By synthesizing these elements, the study aims to offer actionable recommendations for enhancing the KRI's legal and policy responses to drone cyberattacks. The methodology emphasizes qualitative analysis and the evaluation of scholarly perspectives to provide a comprehensive examination of the topic. However, this study is limited by a lack of essential academic resources, such as articles, books, and scientific and legal research on drone cyberattacks specific to the KRI. As a result, data collection on this topic occasionally relies on journalistic and media sources.

3. Drone Cyberattacks on the KRI: A Concise Overview of Key Events and Implications

The Kurdistan Region, being a federal region within the unity of the Iraqi sovereign state, has been a part of much geopolitical tension and conflict for many years. The KRI,

ISSN-Print: 2079-3901
ISSN-Online: 3005-396X

under Iraqi sovereignty and with a degree of autonomy, is supposed to be integrated within the wider Iraqi state framework (Iraqi Constitution, 2005). One of the most important and modern threats with which the region faced over the last years are drone cyberattacks. Among the wide range of state and non-state actors, these drone cyberattacks have been used, further complicating the security landscape. The section below will reflect a historical background of drone cyberattacks on KRI, relating to main events, considering actors and wider implications for regional security and international law.

The use of drones in the KRI can be traced back to the early 2000s. Initially, most of the drones were employed for surveillance activities by the U.S. and its allies throughout the Iraq War. The strategic situation of KRI, being next to the powers of Iran, Turkey, and Syria, made it a very pivotal place to gather intelligence(Sadeghi,2016). In these years, also, the Kurdish Peshmerga forces, in coalition with the United States of America, began to understand the potential use of drones, not only for reconnaissance but also to engage in combat (Iddon, 2024 & Doyle,2013).

The rise and subsequent defeat of the Islamic State-ISIS-from 2014 until its defeat marked a turning point in the use of drones in the Kurdistan Region of Iraq, and saw a significant increase in the production and purchasing of drones by various militant groups (Doski, 2023). In 2021, five drone cyberattacks or attempts were reported in Iraq and the Kurdistan Region. The first major incident involved a series of drone cyberattacks at Erbil airport. The various attacks were attributed to several groups, including the Islamic State, commonly referred to as ISIS, and also the Iranian-backed militia known as Kataib Hezbollah (Sirwan, 2021).

In addition, neighboring countries of the KRI for various reasons, including the threat of terrorism launched drone cyberattacks on their target areas in the KRI. One of the most prominent actors in the drone warfare landscape of the KRI is Turkey. It is on record that, as of the year 2020, Turkey had more than 40 documented military bases in the Kurdistan Region of Iraq. These bases have been used by the country in the execution of drone cyberattacks against the Kurdistan Workers' Party, considered by Turkey a terrorist organization. The drone operations over KRI became part of the overarching regional strategy of Turkey in projecting influence to restrict Kurdish autonomy and have been expanded since 2018(Isamel, 2022). As recently as this April 2020, a Turkish drone cyberattack targeted the Makhmour refugee camp in northern Iraq, killing three civilians-two of them women-and wounding several more (Washington Kurdish Institute, 2020). The incident drew international condemnation, with the US ambassador to the UN Linda Thomas-Greenfield opposing airstrikes in civilian housing areas. Iran has also employed drone warfare over the KRI (Frantzman, 2021). Iranian drones attacked the headquarters of Iranian Kurdish parties and also civilian areas in September 2022, a factor that has instilled some sort of panic among the locals (Sirwan, 2021).

Frequency and intensity of the drone cyberattacks were intensified in the year 2023 and 2024. On December 30, 2023, a drone cyberattacks occurred on a Peshmerga base near the headquarters of a ruling political party in Pirmam, a city of Kurdistan region. Although no group claimed responsibility, the attack was seen as a significant escalation in the region's security dynamics. However, the December 30, 2023 attack on the Peshmerga base was seen as a significant escalation, possibly aimed at opposing the policy of the Kurdistan Regional Government (KRG) ("Rare attack near heart of Iraqi Kurdish power, 2024"). The drone cyberattacks have targeted several critical infrastructure spots within the KRI in the year 2024. Erbil International Civil Airport located in the capital of the Kurdistan Region has been attacked most recently on 16-01-2024 and it was hacked by drone bombers, out of which three bombers have been

ISSN-Print: 2079-3901
ISSN-Online: 3005-396X

neutralized by the KRG's counter-terrorism unit (Aydogan, 2024). On January 25, 2024, another drone cyberattack on the Khor Mor gas field in Sulaymaniyah city led to a temporary suspension of production, resulting in major power cuts across the KRI. While no group has officially claimed responsibility for most of the attacks, they are suspected to be carried out by Iran-backed Shiite militias: The Islamic Resistance in Iraq, an umbrella group of hardline pro-Iran militias, has claimed some of the attacks (Azhari, 2024).

Nevertheless, KRG categorically, referring to it as an excuse to attack Erbil and to violate the sovereignty of Kurdistan Region as well as Iraq. These attacks have also been outlawed by the international community, where the U. S described them as 'reckless and imprecise 'while the United Kingdom described the attacks as 'an unjustifiable infringement of the Iraqi sovereign immunity and jurisdiction. 'France fully rejected the attacks on the Kurdistan Region demanding that the attackers be brought to book. The attacks have also caused escalated political tension between Erbil and Baghdad as the later has recalled its ambassador to Tehran and threatened to sue in the UN Security Council (Human Rights Watch, 2024 & Ministry for Europe and Foreign Affairs, 2024).

As a result of the above, it is clear that the KRI has been facing an increasing trend of various forms of cyberattacks by drones from various state and non-state actors with remarkable impacts on its security landscape. From the first instances in the area for surveillance, this later advanced to more sophisticated forms of cyberattacks as they targeted major infrastructure and civilian areas. Neighboring countries, such as Turkey and Iran, have used drone warfare to pursue their regional interests, often under the pretext of countering terrorism. The international community has strongly condemned these violations of sovereignty, urging accountability and the protection of the KRI's territorial integrity. Despite this, the ongoing drone cyberattacks continue to strain relations between Erbil and Baghdad, presenting serious challenges to regional stability and international law.

4. Modern International Conflicts and the Evolution of International Law: Addressing the Challenges of Drone Cyberattacks

The actors and motivations, methods, and implications of drone Cyberattacks sharply diverge from traditional warfare on many aspects. These attacks typically reach civilian infrastructures and populations, where remote and anonymous perpetrators make use of advanced technologies such as unmanned aerial vehicles and hacking techniques. In this aspect, the transcendence of geographical boundaries and the nonlocalized nature of damage become incomprehensible within the conventional notions of territory and conflict. These factors would, therefore, suggest that drone cyberattacks signal a new paradigm in international conflict-one where prevailing approaches are going to be revised and/or replaced by newer ones.

The use of drone cyberattacks adds a new dimension to international law challenges. Among these, the most important are issues defining what constitutes sovereignty and state responsibility in the context of such an attack and under what circumstances effective counter-measures, including the invocation of the right to self-defence, would be legally justified. The resolution of these complex questions is at the heart of ongoing relevance and effectiveness of international law against the evolving gamut of security threats.

The nature of the cyberattack erases the lines of traditional sovereignty. Traditional war identifies the attacker and its origin. Cyberattacks are different in that non-state actors or states leveraging proxies are conducting them. This alone masks attribution-the sine

ISSN-Print: 2079-3901
ISSN-Online: 3005-396X

qua non of responsibility under international law. The Tallinn Manual on the International Law Applicable to Cyber Warfare calls for due diligence whereby states should ensure that their territory is not used for acts which adversely affect the rights of other states (Schmitt, 2013). However, this principle has been subject to much controversy in application to drone cyberattacks.

The principle of sovereignty represents a cornerstone of international law in that it represents the ability of a state to govern itself without interference from the outside. New drone cyberattacks present new challenges to this doctrine in ways never before realized by conventional military operations. This is because drone cyberattacks differ from traditional military operations in that they are capable of anonymous facilitation or obscuration of origin attribution by their perpetrators. One of the most central problems in trying to define state responsibility with respect to drone cyberattacks revolves around the issue of attribution. The technical complexity of cyber operations, combined with the anonymity of the attackers, allows them to mask their identities and use proxies or botnets when conducting attacks. That sets a very high evidentiary threshold for proving that a state is responsible for a cyber-operation. Attribution typically involves a number of technical indicators, intelligence assessments, and, in many cases, circumstantial evidence; thus, this is often very contentious and politically sensitive as well (Rid & Buchanan, 2015).

Under international law, states are under due diligence obligations not to allow their territory to be used to cause injury to other states. The Tallinn Manual views this principle as meaning that states will have to take reasonable measures to prevent cyber operations that adversely affect other states if such operations are conducted from or within their territory (Schmitt, 2013). What counts as "reasonable measures," however is uncertain and likely to be a matter of interpretation. States cannot, or perhaps are unwilling to, control and regulate the cyber activities within their borders.

This means that, under international law, states are liable for a variety of wrongful acts attributable to themselves, to which drone cyber operations will also pertain. The RSIWA provides a framework through which the responsibility of a state can be determined. For instance, Article 8 of RSIWA provides that the conduct of individuals or groups acting under the direction or control of a state will be attributed to that state (RSIWA, 2001). In the context of drone cyberattacks, this kind of control or direction is hard to prove but it is an integral part of accountability. More importantly, according to Article 11, the state for sure will be considered attributable "under international law if the state acknowledges and adopt the conduct."

These principles are illustrated with historical examples. A 2019 drone cyberattack against Saudi Aramco, blamed on Iranianbacked Houthi rebels, highlighted some of the problems of attribution and state responsibility (Connell, 2019). While there was good evidence of state sponsorship, it would be hard under international law to prove that Iran was directly involved. Similarly, a wave of drone cyber operations against Israeli water facilities in 2020 was attributed to Iran; this, again, brings forward the difficulties surrounding the issue of the attribution of State responsibility and actually reacting efficiently to such an incident under the prevailing legal regime (Merman, 2022).

The doctrine of self-defense has been well enshrined in the international law and most especially in the UN Charter Article 51. This grants state the right for self-defense where there is an armed attack. The issue lies in the fact that, translating this doctrine into drone cyberattacks is more of a challenge. The first major controversy relates to the meaning of the term 'armed attack' in the context of a drone cyberattack, which shall be elaborated in far greater detail in the subsequent parts of this paper. For the Tallinn Manual, it was deemed that causing significant injury or physical damage might be armed attacks by cyber operations (Schmitt, 2013). However, this is not an agreed

ISSN-Print: 2079-3901
ISSN-Online: 3005-396X

threshold by the international community, however, and its meaning may vary greatly. For instance, the 2007 cyberattacks against Estonia were poorly responded to by the international community because it was divided on how to act towards the situation. According to Haataja and Herzog, while some viewed such an attack as aggression in the manner in which they implicated nation-state infrastructure, others openly debated that they did not constitute an armed attack within the meaning of international law (Haataja, 2017 & Herzog, 2011). In the same vein, the 2020 cyberattack on the US government, attributed to foreign actors, called into question whether such actions warranted a military response or were simply espionage (Coco, Dias, and van Benthem ,2022).

The two principles that are important in assessing the action of self-defense are the principles of necessity and proportionality as attributed by the Caroline Test (O'Meara, 2021). To recall, the Necessity principle means that the state must intervene and counter aggression that cannot be mitigated by other means while the Proportionality equates the defenders' actions to the level of aggression from the side of the aggressor. When it comes to drone cyberattacks these principles become quite nuanced. For instance, the appropriate response to a drone cyberattack could be counter cyberattack but deciding on what constitutes as proportional response may not be easy. Further, the imminence is not always clear since cyber threats can constantly or semi-continuously exist and threaten organizations.

Self-defense use in cyberspace also creates a number of ethical and legal issues. The possibility of causing collateral damage when undertaking cyber operations is high since any cyberattack may affect civilian infrastructure and that of third-party states. In conducting such cyber operations, principles from International Humanitarian Law(IHL), such as distinction and proportionality, need to be seriously taken into consideration in planning and execution with a view to limiting harm to civilians in theaters of war (Schmitt, 2013).

For this reason, effective strategies to prevent and respond to drone cyberattacks must be developed through international cooperation and legal innovation. It is important that states collaborate in establishing a clear set of norms that prescribe the use of cyber technologies in warfare. To be sure, this includes prohibition of any cyber intrusion into the drone systems of another state without explicit consent from the latter, which would amount to a violation of sovereignty and aggression. It is also necessary that norms must demand from states to declare the development and deployment of cyber capabilities in drones to an international body for transparency and accountability. States should be clear, based on the same rules, what proportional responses to drone cyberattacks are, with countermeasures against such an attack measured and thoroughly calibrated so as to prevent unnecessary escalation of conflict.

With the considerations above, drone cyberattacks pose quite a challenge to the current international legal framework. In this respect, it is relevant to consider that since drone cyberattacks had peculiar characteristics, international law needs further development to tackle such characteristics, on one hand, and on the other, that the analysis of drone cyberattacks in terms of current norms of international law may mean interference in the internal affairs of the state, violation of state sovereignty, and even the use of force against the state, which we will discuss more in further sections.

ISSN-Print: 2079-3901
ISSN-Online: 3005-396X

5. Drone Cyberattacks and KRI Sovereignty: Assessing Legal Violations and International Law Challenges

The growing intensity and complexity of the drone cyberattacks against the KRI constitute not only a serious threat to regional security but also a violation of the sovereignty of Iraq under international law, as the Kurdistan Region is part of Iraq. These attacks, perpetrated by state and non-state actors, constitute a violation of the territorial integrity of Iraq and the autonomy of the KRI through some of the cardinal principles of international law inhibiting the use of force and respecting state sovereignty. This section discusses the legal frameworks that classify drone cyber-attacks as acts of sovereignty violations and wrongful acts under international law with respect to their implications for the KRI.

Some scholars argue that drone cyberattacks does not constitute violation of sovereignty in international law. Of particular note, Michael Schmitt in his work regarding the Tallinn Manual on the International Law Applicable to Cyber Warfare avails that states could engage in cyber operations below the threshold of armed conflict that may not violate the sovereignty of the other state or amount to an armed attack (Schmitt, 2013). From Schmitt's perspective, ideals of sovereignty are now shifting to gray area, given that cyber operations do not require physical presence or even fighting.

Furthermore, the advocates of this notion pointed that that the ambiguity in international law as far as the question of cyber operations goes enables states to circumvent what could be called their national security. They claim it is in self-defense of states' rights to act to counter certain perceived threats, which may well include cyberattacks, thus recasting such operations as rightful responses to violations of sovereignty, rather than violations themselves. Likewise, other scholars, such as Catherine Lotrionte, have discussed cyber operations within state sovereignty and indicate that the evolution of the threat in cyberspace adds to the legal complication(Lotrionte,2012). Lotrionte's work further illustrates how states need to evolve their interpretation of sovereignty and self-defense in light of technological advancement, while the lack of an agreed definition on both allows for a great deal of latitude in state actions that could not normally be considered a violation of sovereignty.

On the other hand, the drone cyberattacks can be as violation of sovereignty. it can be said has claimed that the practice of non-interference is a fundamental legal rule and any interference of another state's cyber space is a violation of this rule. For example, according to Peter Margulies, the dilemmas provided by cyber threats in state responsibility need reevaluation for broader interpretations that cover numerous acts of states in granting support to the non-state actor in conducting cyber operation. (Margulies, 2023). In this regard, great emphasis is given to the fact that states should be responsible for the conduct in cyberspace of entities they sponsor or support, hence reaffirming that cyberattacks can infringe on sovereignty.

However, the International Court of Justice (ICJ) has been long aware of the sovereignty of states and also the necessity of responsibility when a state uses force in an unlawful manner (Oxford Research Group, 2011). Scholars at this regard opine that drone cyberattacks, especially those causing physical harm or disruptions of a state's infrastructure should fall under the same category as kinetic attacks which are unarguably considered as a violation of sovereignty under the international law (Currier, 2013).

It can be argued that a drone cyber-attack can be qualified as internationally wrongful acts, at least in the case of a breach of an established legal obligation under international law. A so-called "internationally wrongful act" is an act infringing on a state's

ISSN-Print: 2079-3901
ISSN-Online: 3005-396X

obligations under international law and may, therefore, also cover breaches of sovereignty. From among the elements which make up a wrongful act in cyber-attacks, the question of attribution of responsibility is the most crucial for qualifying an act as wrongful. What scholars like Michael Schmitt are saying is that a cyber-operation would have to be attributable to a state-that is, under the control or influence of a state-to be wrongful. This may be hard to establish because non-state actors may be involved or because states use proxies to conduct cyber operations. The ambiguity of attribution always convolutes the legal analysis of those actions, making the state's accountability questioned (Cherry & Pascucci, 2023).

While some scholars, like Rosa Brooks, believe fuzziness enables states to manipulate legal standards in an attempt to justify their conduct, others are of the view that the existing frameworks do provide sufficient guidance in order to assess legality in cyber operations (Brooks, 2013). For instance, the Chatham House report which focuses on state practice in cyberspace under international law mentions that international law may require states to clarify how they think it should be implemented with regard to cyber activities, thereby addressing the issue that lack of clear normative frameworks may generate misunderstanding, misperceptions and the potential for escalation (Moynihan, 2019).

It is worth to note that, when focusing on the drone cyberattacks on the KRI and its institutions, the debate gets even more complicated due to the political and legal status of the region within Iraq and the international community. To this end, the consideration of such attacks as aggression against sovereignty or wrongful activity according to international law entails the study of several sources of law and norms.

Article 2(4) of the UN Charter prohibits the threat or use of force against the territorial integrity or political independence of any state. To that aspect, the drone cyberattacks that have results in such damages to threaten the sovereignty of Kurdistan Region as a part of Iraqi sovereignty will mean breaching this principle. As it has been mentioned before, since KRI is given the status of a semi-autonomous region under Iraqi constitution of 2005, the attacks on it could also be argued to violate the sovereignty of Iraq as a whole, particularly if they undermine the stability or governance of the region (UN Charter, 1945).While International Covenant on Civil and Political Rights (ICCPR) mainly covers human rights, its principles pertaining to protection against violations of self-determination and political autonomy apply. Thus, it can be said that cyberattacks via drones against KRI's self-government or impeding political processes amount to violations under Article 1 of the ICCPR, targeting peoples' right to self-determination (ICCPR, 1966).

Such kinds of drone cyberattacks, hence, are unlawful in the entire international law. The aggressors have attacked the territorial sovereignty of the Kurdistan Region in the Iraqi state by having infiltrated into its drone's cyber operations, taken control over them. These attacks have violated the political sovereignty of KRI further through violations of the rights of its citizens, especially those affecting economic infrastructure and freedom, security concerns, and claiming civilian targets, as noted above, under both national and international law. In each of these ways, the drone cyberattacks are unequivocally unlawful acts that deserve a legal response (Sayankina, 2017). The Tallinn Manual gives a detailed explanation of how international law applies to cyber operations, including those involving drones. If the drone cyberattacks on the KRI cause significant disruption or damage, then they could be characterized even as uses of force within the meaning of the principles set out in this manual, and hence as wrongful acts. The manual further provides that the cumulative effect of several cyber operations might reach the threshold of a use of force, further entrenching the possibility that such an attack might be considered a wrongful act (Schmitt, 2013).

ISSN-Print: 2079-3901
ISSN-Online: 3005-396X

Characterization of these drone cyber-attacks is, of course, critical as it dictates which legal response is relevant under international law. There are three primary categories applicable here under international law: "the threat or use of force" under Article 2(4) of the UN Charter; "the armed attack" under Article 51; and third, a category of intervention, often neglected. The last category involves actions or threats that disturb undermine the very fundamentals of state sovereignty, such as political, economic, and cultural elements. In the scope of the KRI, all three types, especially the acts of intervention that are an overt violation of international law, are discussed in detail in subsequent sections.

Based on the above, it is clear that drone cyberattacks conducted by both state and non-state actors infringe on the territorial integrity and autonomy of the KRI and therefore on basic tenets of international law, including the prohibition of the use of force mentioned in Article 2(4) of the UN Charter. Scholars differ on the issue, with some arguing that drone cyberattacks do not violate sovereignty because they do not meet the traditional criteria for armed attacks, while others contend that such interventions clearly violate sovereignty when they cause significant damage. These attacks are recognized as wrongful acts under international law, demonstrating that violations of KRI sovereignty necessitate a strong legal response for protection.

6. Drone Cyberattacks as Intervention: Legal Challenges in the Context of the KRI

Traditionally, intervention in international law has involved at least one state or an international actor violating the sovereignty or internal affairs of another, usually by military or political means. In more recent years, however, the definition has been stretched to involve other operations in cyberspace, including drone cyberattacks. Because, as stated above, qualification of such an attack as a "threat or use of force" under Article 2(4) or as an "armed attack" under Article 51 of the UN Charter is ambiguous and depends on the gravity and effect of the attack. The precise meanings of these terms and their distinctions are not well-defined, and their relationship to "aggression," as outlined in various UN declarations including the UN General Assembly's Definition of Aggression, remains vague. This general lack of clarity complicates the application of these provisions to cyberattacks, presenting a contemporary challenge in defining and understanding intervention under international legal standards, particularly with regard to drone cyberattacks on the KR.

However, the language in UN Charter's Articles 2(4), 51, and Definition of Aggression that can refer to an incident like a drone cyberattack on the KRI. Article 3 of the Definition of Aggression enumerates actions that constitute aggression in general, and almost all refer to military activities. However, paragraph (g) of the Article defines that "The sending by or on behalf of a State of armed bands, groups, irregulars or mercenaries, which carry out acts of armed force against another State of such gravity as to amount to the acts listed above, or its substantial involvement therein". It also states in Article 4 that "The acts enumerated above are not exhaustive and the Security Council may determine that other acts constitute aggression under the provisions of the Charter" (UNGA, Res. 3314(XXIX), 1974).

By contrast, the legality of drone cyberattacks is hotly debated by scholars, with arguments over whether such an attack would constitute a prohibited intervention under international law. To that end, Rosa Brooks submits that U.S. drone strikes undermine the rule of law internationally, defying easy legal categorization and muddling the principles of self-defense and armed attack. She further argues that the

ISSN-Print: 2079-3901
ISSN-Online: 3005-396X

drone operations can amount to a coercive intervention in the internal affairs of states, especially when it is directed against any state's critical infrastructure or efforts to hinder governmental operations and functions (Brooks, 2013). On the contrary, Michael Walzer views the ethical aspects of fighting war using drones and calls for the application of just war theory principles. He argues that targeted killings are to be analyzed within the framework of international law, wherein he says that not all drone operations would be illegal per se, but those which comprise of violation of sovereignty and massive destruction could be illegal under the law (Walzer, 2016). This debate is further supported by Joshua L. Cornthwaite, where he lists some points as consequences of territorial violation by drones. He states that any state is under legal commitments and duty to respect air sovereignty. He says that cyberattacks through drones, particularly those that are surveillance-based or functions, disrupt the states' functions that might also be considered violations of sovereignty and, hence, prohibited interventional actions (Cornthwaite, 2019).

However, Anders Henriksen argue, without providing legal references, that a violation of sovereignty occurs whenever one state physically enters the territory or airspace of another state without consent or legal justification (Henriksen, 2019) However, according to Goldsmith and Loomis, this assertion is overly broad and somewhat misleading. They argue that in some instances, crossing another state's territory does violate international law, but this would be in cases where a fighter jet or reconnaissance drone intrudes into foreign airspace without authorization. They have also pointed out that in some, it does not: for example, a spy secretly crossing a border without committing illegal activities, or a state spreading digital propaganda into another country. The concept of "sovereignty" alone doesn't clarify why certain border crossings are unlawful while others are not. To determine this, one must examine state practices and legal opinions (opinio juris) in specific contexts, something the manual fails to address (Goldsmith and Loomis, 2021). These scholars together give an idea of the legality of the cyberattacks by drones.

While some such actions are justified in specific circumstances, the possibility of coercive interference and violation of sovereignty puts into perspective vital questions about the legality of such interventions over the KRI and beyond. However, in cases where such autonomous functions of the region are disrupted or its governance hampered with drone cyberattacks, this would amount to intervention. For example, if such an attack were against the KRI's critical infrastructure, including economic infrastructure affecting the livelihoods of its people, interrupting the communication systems, or amount to coercion with the effect of making the KRI align with the political interests of another state, they can be seen as breaching the principle of non-interference.

It is relevant to note, however, that the inception of "force" was not defined peremptorily under the UN Charter, and the term has generally been interpreted to connote military force and not economic or political pressure. It is an interpretation that usually finds backing in the UN General Assembly Definition of Aggression, referring to military force itself (UNGA, Res. 2625 (XXV)). However, it should be remembered that both the UN Charter and the Declaration were written in a completely different time when military force referred to traditional armed conflict, not modern drone cyberattacks now targeting the KRI.

According to Resolution 2625, the Declaration explicitly acknowledges indirect intervention and differentiates between “armed intervention” and other types of interference or threats against a state's identity, including its political, economic, and cultural aspects, which are all deemed violations of international law. Building on this understanding, one of the key provisions of the Declaration relevant to drone

ISSN-Print: 2079-3901
ISSN-Online: 3005-396X

cyberattacks on the KRI states that "Every State has the duty to refrain from organizing, instigating, assisting, or participating in acts of civil strife or terrorist acts in another State, or acquiescing in organized activities within its territory directed towards the commission of such acts, when the acts referred to in the present paragraph involve a threat or use of force." Additionally, the ICJ in the Nicaragua case confirmed that this concept of indirect force falls under the prohibition of the threat or use of force outlined in Article 2(4) of the UN Charter. In the Nicaragua case, the ICJ elaborated on what comprises intervention and the use of force. The Court distinguished between the "most serious forms of the use of force, such as armed attack," and "less grave forms." It held that the supplying of arms and training to the contras was a threat or use of force, while supplying funds alone was not; nevertheless, the Court ruled that supply of funds was intervention. As the Court said, the principle of non-intervention proscribes interference in matters "whether it be with the political, economic, social and cultural systems of a state or with its foreign policy" (Nicaragua v. United States, 1986).

However, this approach may be applied to the KRI drone cyberattacks. The latter might be treated as intervention and impact political and economic rights of KRI, thus violating Iraq sovereignty. Drawing from the logic of the ICJ in the Nicaragua case, therefore, the drone cyberattacks by Iran and Turkey and their armed groups in Iraq were also violations of their international obligations not to intervene in the internal affairs of other states, and as such, they are responsible for any damage caused by such actions.

It is clear from the above that the evolving nature of intervention under international law, more so with regard to drone cyberattacks, has raised some acute legal obstacles. On that note, although traditional concepts of force and sovereignty remain at the center of this area of international law, the obscurity of legality that surrounds cyber operations creates significant doubts over their legal qualification. This resonates in debates among scholars and is indeed a severe obstacle in establishing just when such an attack would qualify as prohibited intervention. Accordingly, in the context of the KRI, drone cyberattacks against critical infrastructure and basic notions of governance could thus be seen to breach principles of non-intervention under international law. What this does-more importantly, when done by other states or their proxies-is reflect the need for an updated understanding of intervention within the modern paradigm, where cyber operations are likely to become more salient in conflict.

7. Drone Cyberattacks on the KRI: Legal Perspectives on the Use of Force Under International Law

Scholars and practitioners have debated whether drone cyberattacks are prohibited threats or use of force in international law. As a result of the traditional interpretation of the term 'use of force' the reference to Article 2(4) of the UN Charter has been construed to primarily mean tkinetic military actions. Nevertheless, with the emergence of cyber technologies the question arises whether cyber operations, including those with the use of drones, can reach this level. In this context, it is necessary to state that a drone cyberattack against internationally prohibited action does not have to be as dramatic as an armed attack in order to receive a reaction from a state. For example, the drone cyberattacks on the KRI in included threats of force in the form of recommending the use of force if the KRI does not accede to the attackers' acts of political leverage. This leads to the important question whether these kinds of attacks need to be regarded as use of force in terms of International Law. If they do, one moves to the next question

ISSN-Print: 2079-3901
ISSN-Online: 3005-396X

whether or not the level of threat or use of force can be considered as an armed attack within the provisions of Article 2(4) of the UN Charter and the customary international law.

As Michael Schmitt rightly pointed out, in the context of international law the term 'use of force' is often at a lower level than an 'armed attack.' It means to say that all armed attacks include the use of force but not all uses of force can be characterized as armed attacks (Schmitt, 2014). However, he argues, an effects-based approach has to be relied upon for the purposes of determining whether a cyber-operation qualifies as a use of force. Another related line of thinking is that if the consequences of a cyber-operation are of a similar character to those of a kinetic attack that creates massive physical destruction, loss of life, or interruption of a state function that is critical, then it could be assessed as a prohibited use of force according to international law (Schmitt, 2013). This view is supported by the wider understanding that an attack of this nature, through drones, causing damage to critical infrastructure and governmental operations, is a use of force. For instance, in the case of a drone cyberattack that has destroyed crucial infrastructures in KRI, leading to disastrous results for the civilian population or, respectively, for the functioning of the Kurdish Regional Government, then such an attack would reach the threshold of use of force. Thus, this attack should be qualified as a violation of international law under Article 2(4) of the UN Charter.

However, as cyber threats continue to rise in sophistication, and reliance from states in the field of digital networks related to critical infrastructure, it is increasingly relevant to reconsider what can actually amount to "significant physical damage" or "critical disruption." For instance, whether a cyber-operation which disrupts, say, a state's financial system or electoral process would amount to a "use of force" despite the absence of physical damage or human loss. The latter situation may demand consideration of "use of force" in a more extensive and subtle sense in the context of cyberspace, which could then be captured by novel interpretations under the internationally legally binding regime.

On the other hand, the argument put forward by Marco Roscini is more limited. In this respect, he underlines that not all cyber operations, including these with the assistance of drones, would qualify as uses of force. As Roscini pointed out the novelty of cyber operations, cyber effects, non-materiality, and ambiguity in respect to attribution altogether means that the attempts at encasing cyber operations into established categories of international law are not feasible. The former advocates for the view that cyber operations can only be characterized as a use of force if they indeed cause direct and significant physical damage; this would exclude most drone cyberattacks from falling under this definition (Roscini, 2014). According to this strict approach, the attack on the KRI would then not constitute a use of force, assuming it is less serious-perhaps just causing temporary disruptions without physical damage. Nonetheless, the concept of cyber sovereignty might apply, and the drone cyberattacks would be considered a violation of Iraq's sovereignty over the Kurdistan Region, whether or not it constitutes a prohibited use of force. Although such attacks by drones against Kurdistan have caused physical harm which has resulted in the killing and injuring of civilians in the region.

Matthew Waxman on the other hand, narrows down his studies to idea of 'threat of force' in Article 2(4) of the Charter of the United Nations. In this sense, Waxman has pointed out that the mere fact that drones can perform cyberattacks would constitute an act of threat of force If this capability is used to compel or threaten other states. Applying the conditions set out by Waxman, the threat to use a cyber drone attack in order to cause certain pressure on state can also be qualified as a violation of the international law (Waxman, 2011). This approach accentuates the psychological and the strategic effects of cyberspace capabilities and stresses that the allegation of such

ISSN-Print: 2079-3901
ISSN-Online: 3005-396X

operations should be considered prohibited actions in the context of international law. However, Waxman's perspective highlights that the ability to intimidate or affect the political and, or military decisions in KRI, can also be a violation of international law, even if it does not lead to physical harm. Given such operations and their capability of disturbing stability and provoking some type of fear can be considered prohibited action by virtue of Article2(4). This broader interpretation recognises that we have to consider the strategic and psychological impact of cyber capabilities in order to determine its lawfulness.

Conversely, scholars such as Mary Ellen O'Connell insist on the possibility of expanding interpretation of the phenomenon of self-defense under the international law, stating that states have the right to initiate an attack with drones against non-state actors if there is a credible threat to the state's security. According to O'Connell, modern warfare requires a new approach in terms of legal justice because of that, he suggests that the existing legal approaches to conflicts should incorporate the characteristics of asymmetrical warfare (O'Connell, 2010). As per O'Connell's line of thinking, drone cyberattacks to the KRI are not regarded as threats or a use of force in sanitized legal traditions since the sovereignty of the Iraqi state remains questionable. However, Mary O'Connell's argument faces several critical issues. Tellingly, the idea of a 'credible threat' is somewhat ambiguous and therefore when applied could allow for rampant interpretative licenses which only serve to trounce accountability when force is applied in its extreme measure. This ambiguity can lead to weakening state's authority and rules that have been set by the state, to undermine the state, and international order and to encourage the use of force. Secondly, such broad interpretations, even as intended to address asymmetric conflicts, can aggravate these conflicts by enticing retaliation and more violence in its place of solving the problems. Moreover, there is lack of specifics to recommend them that fails to capture the legal and ethical issues of drones' operation including killing of civilians and extermination of suspected persons. A less radical option could be a reinforcement of the existing codification of international law and diplomacy in reference to the challenges posed by the asymmetric warfare and non-state actors rather than the expansion of self-defense regime.

Also, the original Tallinn Manual does not give a clear meaning of what is referred to as use of force in the cyber operations. As Schmitt notes, even the International Group of Experts (IGE) that was discussing the issues for three years could not reach consensus on the definition of a cyber use of force. They only agreed that any non-injurious or nondestructive cyber operation must be addressed individually. This would contain features like operation severity, the impact time frame, intrusiveness factors and military aspects of operation (Schmitt, 2014). The legal framework for threats of force is even less developed than that for the use of force. Nonetheless, Ian Brownlie defines a threat of force as "an explicit or implied promise by a government to use force if its demands are not accepted (Brownlie, 1963). This clearly describes the nature of the threats involved in the drone cyberattacks on the KRI.

Another crucial factor to consider about drone cyber warfare attack on the KRI is the use of force or coercion not only in the type of force used but also in the target and aim of the force. According to the study Sadurska articulated this as the central question: Does a threat constrains the range of choice for the state? (Sadurska,1988). Regarding the drone cyberattacks on the KRI, the declared goals were the presence of the illegal armed groups and the supposed Israeli facilities in the region. However, these bases and groups were either nonexistent; or were not actually present in the city. The ultimate working of the attacks seems to be political, economic and or commercial harm to the region.

ISSN-Print: 2079-3901
ISSN-Online: 3005-396X

Drone cyberattacks against the KRI could be seen, arguably, to be in nature of 'use of force' within the meaning of Article 2(4) of the UN Charter and perhaps even as much as an 'armed attack' within the meaning of Article 51, more so than will be discussed below, despite no involvement of weapons or damage in such an attack. There is a reason scholars avoid characterizing this type of attack as such because of concerns of escalation and unpredictability. Still, one may argue that proper definition of the nature of such attacks might be beneficial for better responses and deterrence. The attackers take advantage of the current uncertainties in international law about cyber operations, knowing they might not face immediate consequences from the affected states (Yadron, Barrett, & Barnes, 2014). However, the KRI cannot effectively respond against these drone cyberattacks due to the absence of a clear legal framework for such attacks other than through the Iraqi state, which might fail for political reasons. In all these cases, this region remains at the mercy of incidents that make any possibility of addressing these attacks well within the bounds of international law.

In short, the legal status of drone cyber-attacks on the KRI under international law remains complex and unsettled. Whereas the "use of force" under Article 2(4) in the UN Charter traditionally referred to kinetic military acts, there are those who would argue for an effects-based approach whereby a cyberattack that gives rise to significant harm might constitute a use of force. The threats of force and coercion that may be involved in the KRI's case could also mean a violation of international law, even in the absence of physical damage. A more restrictive view, on the other hand, regards only those operations causing direct physical harm as uses of force, a stance complicating the classification of such attacks. The ambiguity inherent in the international law frameworks, in addition to the lack of a clearly articulated legal framework for cyber operations, places the KRI in jeopardy as it strives for an effective response against such attacks.

8. The Legal Challenges of Classifying Drone Cyberattacks on KRI as Armed Attacks under International Law

The concept of an "armed attack" lies at the heart of international law, especially under Article 51 of the UN Charter, entailing the inherent right of self-defense in case of an armed attack. At the same time, however, changes in technology have challenged traditional interpretations of what actually constitutes an armed attack. The newest drone cyber-attacks, especially those against the KRI, raise the question of whether such an act could constitute an armed attack under international law, as there is considerable scholarly debate.

Some scholars seem to believe that a cyberattack would only be considered as an armed attack in case of more serious injury or damage. For Shiri Krebs, a revision of "drones, aerial vision and the law of armed conflict" should be considered in light of developments with new technologies like cyber-attacks(Krebs,2023). Similarly, another related argument put forward by the International Bar Association's Human Rights Institute refers to the view that "the legality of armed drones under international law" depends on whether their use, for instance, cyberattacks, can pass the test of necessity and proportionality (International Bar Association, 2017). However, Krebs doesn’t directly address the direct question of whether cyberattacks constitute armed attacks, which may render doubt in how such cyber operations by means of drones fall into her argument. While she calls for a general reassessment of the law to account for drones, it’s unclear how this extends to cyberattacks, which involve different characteristics. For instance, a drone cyberattack disrupting the critical infrastructure-like power grid of a

ISSN-Print: 2079-3901
ISSN-Online: 3005-396X

country-may not cause immediate physical damage but is able to cause immense disruption in society. Krebs' focus is much more general, on drones in conventional warfare, and for that reason alone will most likely fail to take into account problems characteristic of cyber-attacks, which fall outside the frameworks established by existing legal norms based on physical damage. On the other hand, the approach of International Bar Association applies well to conventional drone strikes but raises questions when applied to cyberattacks. Since cyberattacks don't always result in physical destruction, it's harder to assess proportionality and necessity in the same way. For example, how to evaluate the proportionality of an attack by a drone cyberattack that does not have an immediate impact on physical systems with regard to the expected military advantage of such an attack? The dependence on traditional legal criteria by the IBA might thus not take into consideration the peculiar nature of the cyberattack, operating within such gray area in the law. Therefore, the tension that exists between these two views carries the broader implication of tugging international law in two directions on how to consider the constantly changing technologies of modern warfare, especially in the realm of cyberattacks.

Some other scholars are not very sure with the way that drone cyberattacks are considered as armed attacks. Rosa Brooks as mentioned earlier believes that U.S drone attacks include what may be potential cyberattacks, 'undermine the international rule of law' due to their straightforward legal categorization (Brooks, 2013). The ambiguity in international law regarding drones and artificial intelligence may allow states to manipulate the rules to their advantage (Khan, 2023). However, Brooks' points to a large issue in international law: the potential for states to exploit legal grey areas. By not providing a clear framework for drone cyberattacks, international law may allow states to act in ways that challenge the spirit of the law without technically violating it. This law manipulation is most relevant in relation to advanced technologies, such as drones and artificial intelligence, where the existing legal rules may be outdated or ill-equipped against new forms of conflict. If states can argue that ambiguity justifies actions otherwise illegal under international law, that will set a dangerous precedent.

As Michael Schmitt points out, while some of the cyber operations can be highly disruptive and costly, they nevertheless usually do not reach the threshold to qualify as an "armed attack" under the judgment of most scholars (G. A. Res. 2625, 1970). An "armed attack" traditionally refers to a large-scale physical invasion or actual hostilities that cause significant physical destruction or or casualties, accordingly to the provisions of the international law. This raises the question: To what extent does this kind of drone cyberattacks on the KRI conform to this traditional definition of an armed attack or does it throw a different perspective to the definition?

Such an attack on the KRI-with conventional weapons, like explosives-would no doubt constitute an attack and would most probably attract international condemnation (Faidhi, 2024 & Wilgenburg, 2024). If data and digital infrastructure are considered as vital as physical assets in today's context, then drone cyber-attacks need to be looked at with equal seriousness. It needs to be understood that the KRI attacks caused well over violations of sovereignty, as included in the previous section; they were extensive in terms of damage and disruption. Considered from the perspective of modern cyberwarfare, these kinds of attacks fit into the concept of a kinetic attack, showing just how grave and debilitating this impact truly is.

However, as mentioned earlier, the issue is that cyberattacks cause losses that are not tangible, or easy to establish that there was an attack in the first place. In legal contexts there similar fashion things are assumed to be an assault only when there is clear proof of harm to the body. Current legal instruments include the Law of Armed Conflict (LOAC) and the Tallinn Manual do not adequately address the non-kinetic form of

ISSN-Print: 2079-3901
ISSN-Online: 3005-396X

warfare ("International armed conflict," 2024). The Tallinn Manual provides an understanding of the legal consequences of cyber operations, especially those that create physical damage. Under the Manual, a cyber-operation should be considered to be an armed attack under international law only if it is reasonably expected to cause injury or death to persons or damage to objects. This agrees with the principle by which cyber operations that result in tangible destruction constitute a violation of state sovereignty and could be considered an armed attack, based on its scale and impact (Check, 2023; Jarose, 2023 & Chang, 2023). However, it remains challenging to know how different operations cause intangible loss. This understand is further complicated by the fact that the legal on which it is based applies principles which were designed for a different kind of age with a different sort of threat, mostly the physical kind.

The Manual recognizes that it is the consequences of the action, rather than the nature of the target, which define whether it is an attack; however, this approach to cyber operations is seriously limited by the prerequisite for physical damage (Schmitt 2013: p.93). Where there is no non-physical harm, this framework's flexibility is undermined. Thus, the relevance of the traditional legal frameworks of international law within the context of these drone cyberattacks on the KRI is limited to not being able to cover the entire realm of damages from these, since not all of them actually do physical harm. These, though without physical damage, highly disturb the needs of the people in question and thus are continuous in the region. This is indicative of how international law needs to shift further to realize the strategic value of data and cyber infrastructure, especially in scenarios like drone attacks. It brings into focus the requirement for the definition of cyber operations as comprising potential threat to extant sovereignty and security even where it does not entail physical harm.

To summarize, it can be noted that the qualification of drone cyberattacks as 'armed attacks' under the international law remains a rather contentious question and further elaboration of this issue is needed. Traditional legal frameworks define an armed attack as one contributing to major physical damage or massive casualties. Such definitions have been challenged with the rise of cyber technologies, particularly in drone operations. Destructive drone cyberattacks, such as those against the KRI, often disrupt critical infrastructure and cause significant societal disruption but do not necessarily involve physical destruction of property. While such an attack may not be deemed to meet the strict criteria of an armed attack under existing international law, in that there is no immediate physical harm, their impact on a region suggests otherwise. These cyber operations have caused widespread damage to essential services and security in KRI, placing them within the ambit of the strategic consequences of kinetic attacks. So while such an operation may fall outside the direct realm of being defined as an armed attack, the reality imposed by drone cyber-attacks on KRI is a serious threat to sovereignty and security-one that is forging new ground on how it would be legally defined under international law.

9. Countermeasures and International Legal Responses to Drone Cyberattacks: Challenges and Mechanisms for the KRI

Under international law, countermeasures are recognized as lawful measures by states responding to internationally wrongful acts by other states or non-state actors. They are measures by which the injured state can defend its interests and urge, at the same time, the offending state to terminate its illegal activities. The principle is rooted in customary international law and codified in articles of 22 and 49 – 54 of the RSIWA (RSIWA, 2001). Article 22 defines countermeasures as actions that are typically unlawful but are

ISSN-Print: 2079-3901
ISSN-Online: 3005-396X

justified when taken in response to another state's breach of an international obligation. Article 49(1-2) further specifies that an injured state may only employ countermeasures against a state responsible for an internationally wrongful act to induce compliance with its obligations under Part Two. The second paragraph clarifies that countermeasures are limited to the temporary non-performance of the injured state's international obligations toward the responsible state.

Drone cyberattacks present unique challenges to international law because they operate in a hybrid domain combining physical hardware (drones) with digital warfare (cyberattacks). As mentioned earlier, the Tallinn Manual provides a framework for assessing cyberattacks within the broader context of state responsibility, emphasizing that sovereignty, non-intervention, and prohibitions on the use of force apply equally to cyberspace.

This would imply that upon a drone cyber-attack infringing on the sovereignty of a state or breaching any other international obligations, it can resort to non-forcible countermeasures in calling upon the responsible state to stop the commission of the wrongful act. Non-forcible countermeasures in this case can be in several forms, such as, diplomatic measures which would include the recall of diplomats, formal protest letters, or suspension of relations with the offending state. The latter may involve freezing of assets, trade sanctions, and other forms of financial penalties. Otherwise, this could be some form of cyber counter-measure that could involve offensive measures to disrupt the aggressor nation's cyber capability or disrupting its infrastructure, for instance (Marossi & Bassett, 2015). However, this argument lacks clarity on the legal constraints and potential risks associated with these actions. Whereas under international law, diplomatic and economic measures are standard, invoking cyber countermeasures does make states nervous at the possibility of escalation. If norms of restraint such as proportionality and necessity do not temper responses in cyberspace, there is a very real possibility of a mistake being made, such as impacting civilian infrastructure or an escalation of the conflict. For instance, the 2019 drone cyberattack on Saudi oil facilities, which was blamed on Iran, prompted Saudi Arabia to call for international support, ratchet up the sanctions against Iran, but refrained from direct cyber retaliation out of concerns about escalating actions in the region. (Jones, Newlee, Harrington, & Bermudez, 2019). This provide a clear example of how cyber responses must be appropriately gauged to realize objectives without offering undue escalation in the cyber theater.

Furthermore, Article 49(3) of RSIWA says any countermeasure should meet the principles of necessity, proportionality, and temporality (O'Meara, 2021). It shall be such that it should be the last resort, after having tried all peaceful means of settling a situation, such as negotiations or international adjudication. The reaction should be on the scale of the degree of harm suffered and stopped as soon as the wrongdoing state begins to fulfill its obligation under international law. Proportionality, in particular, within the cyber domain, should be an appropriately measured response so as not to escalate tensions or create any unintended collateral consequences in third-party states. For instance, if a drone cyberattack disables an energy grid, the injured state may have the right to take corresponding cyber actions to disable the attacker's capabilities, but it must avoid causing greater harm than the original attack (Boylan, 2017). In this analysis, however, it mentions only that countermeasures should be a sort of "last resort" without delimiting that under the principle of necessity, no other lawful means must indeed be available to deal effectively with the violation. Additionally, though the principle of proportionality here is mentioned, the detailed analysis about this issue is very important in light of the complexity of cyberattacks. In cyber operations, determining proportionality is far more challenging because of the unpredictable and

ISSN-Print: 2079-3901
ISSN-Online: 3005-396X

far-reaching consequences of cyber responses. For instance, if a state were to retaliate against a drone cyberattack by disabling the attacker's infrastructure, it could unintentionally impact civilian systems or third-party states, thereby violating international law. While relevant, the provided example oversimplifies the matter to imply that proportionality requires no more than causing less harm, when in fact the real difficulty is about how to assess and contain the spillover effects of cyber actions. The reference to temporality is also underdeveloped in that it should indicate not just that countermeasures shall cease once the wrongdoing state complies but also to be reversible, wherever possible, to avoid permanence of the damage.

However, while Kurdistan Region thus enjoys a great degree of autonomy, it operates nevertheless within the framework of the Federal Republic of Iraq, and as a sub-state entity, it lacks full legal capacity in order to unilaterally deploy countermeasures in the international realm (Kurdistan Region of Iraq, 2019). In situations where the KRI is the target of drone cyberattacks, its right to take defensive measures either preemptively or in retaliation, must be coordinated with the Iraqi federal government. Nonetheless, the KRI could engage in non-forcible countermeasures in the form of enhancing cybersecurity defenses, cooperating with international cyber defense organizations, and blocking the cyber capabilities of potential attackers through joint efforts with federal authorities (Best et al., 2020).

As mentioned earlier, in recent years, the KRI has increasingly come under drone-based and cyberattacks, widely assessed as the hand of non-state actors or proxy forces emboldened by regional powers. These attacks repeatedly carried out against critical infrastructure-from oil facilities and communication systems to government buildings-present a continuous threat to stability in the region. In such cases, the KRI must work within the Iraqi legal framework while also invoking its own regional laws to respond effectively. These Drone cyberattacks can be categorized as an intervention, which determines the nature of Iraq's response. For example, a methodical approach to disrupting the cyber operations of an attacking state could be used to deliver a firm warning. The action would show the offending state that their actions will not be tolerated and would also underscore Iraq's capability to strike back. However, there is a hard task ahead of Iraq in implementing this method since many of those attacks come from countries with which Iraq has strong relations, such as Iran. Besides, Iraq does not have strong cyber military capability.

In terms of international legal procedures for preventing drone cyberattacks, Iraq can hold regional countries accountable for drone cyberattacks through the RSIWA. Under Article 22 of RSIWA, Kurdistan Region, as part of Iraq, has the capacity to participate in invoking state responsibility for wrongful acts that breach Iraq's sovereignty or cause significant harm. The process begins with filing complaints. KRI, through Iraq can lodge a complaint with the RSIWA. For example, if a drone cyberattack is attributed to a regional country and breaches Iraq's sovereignty or causes substantial harm, Iraq can bring the case before the ICJ under Article 34(1) of the ICJ Statute, which states, "Only states may be parties in cases before the Court". However, Article 22 of RSIWA furnishes the legal basis upon which states may seek judicial resolution for such breaches of international obligations. Consequently, Iraq and Kurdistan Region can seek redress from the ICJ or other international legal forums. This may take the form of claims for compensation or demanding the cessation of the wrongful acts. For that to occur, Iraq and Kurdistan Region would have to prove that such drone cyberattacks are international law violations and invoke the applicable means to redress such violation.

Another way is that the Kurdistan Region, through Iraq, may also find redress through various international mechanisms for such drone cyberattacks. One avenue could be a complaint under Chapter VII of the UN Charter to the UNSC for attacks that are

ISSN-Print: 2079-3901
ISSN-Online: 3005-396X

considered to pose a threat to regional peace and security. This is, in fact, the big problem; framing such attacks specifically as a threat to international peace and security. The UNSC might not consider such attacks as destabilizing enough with spillover effects that demonstrate broader regional implications. Another complicating political factor is in Iraq's strained relations with Kurdistan Region. Given the tensions that have always existed between the federal government and the KRG, especially over territorial disputes and political autonomy, it is a question whether Iraq would be willing to take up the interest of Kurdistan Region to the international plane.

Another line could be with the UN Secretary-General, calling on a special investigation to be ordered regarding the drone cyberattacks. This would entail the taking of the form of a UN fact-finding mission for the purpose of collection of evidence and attribution to the states. It finds its competencies under Article 99 of the UN Charter, which states that the Secretary-General is competent to bring matters constituting any threat to international peace and security to the attention of the UNSC. However, Iraq might be unwilling to worsen its relations with neighboring countries like Turkey or Iran, both of which have usually been implicated in these attacks. Its economic and security links with these countries may also contribute to Iraq's reluctance toward taking the issue to the UNSC due to larger diplomatic consequences. In fact, even a fact-finding mission initiated by the UN Secretary-General under Article 99 of the UN Charter faces certain firm political resistance from powerful regional actors, making such efforts more complex in terms of international accountability. These political and diplomatic obstacles really point to a very difficult path for KRI in countering drone cyber-attacks through international mechanisms.

It is clear from the above that, countermeasures under international law do provide states suffering from wrongfulness, such as that constituted by drone cyber-attacks, with ways of legal response. While defensive measures on the part of the Kurdistan Region are possible within the Iraqi legal framework, more broadly speaking, international responses, such as the invocation of state responsibility through RSIWA or before the ICJ or UNSC, remain problematic in light of Iraq's political and diplomatic straitjacket. Finding a balance between effective retaliation and preventing escalation has been of great concern, even more so in the cyber domain.

10. Conclusion and Recommendations

10.1 Conclusion

In conclusion, this paper elaborated in detail on the complicated legal regime around drone cyberattacks in KRI, with an emphasis on the nexus of cyberwarfare and international law. The main focus was to find out how these new forms of attack are challenging the corpus of established legal principles and to assess whether current international legal regimes provide an appropriate framework for responding to such violations. It has elaborated upon how drone cyberattacks are the embodiment of a mix between the physical and digital, thus challenging longstanding conceptions of sovereignty and state responsibility. Application of the framework, such as the RSIWA and Tallinn Manual, has showed its usefulness and limits in the context of cyber operations. These frameworks, though fundamental, usually fail to consider the subtlety and the ever-changing face of cyber threats. Principles of necessity, proportionality, and temporality stand at the heart of applying countermeasures under international law and are most difficult to apply in this area of cyber warfare. The inherently unpredictable nature and wide-reaching scope of cyberattacks make proportionality assessments, and how well responses function, quite complex. This study has also highlighted the broader political and diplomatic challenges that further complicate the KRI's ability to address

ISSN-Print: 2079-3901
ISSN-Online: 3005-396X

these attacks effectively. As a sub-state entity operating within the Federal Republic of Iraq, the Kurdistan Region's capacity to unilaterally engage in international legal processes is limited. The geopolitical complexities involving regional powers such as Iran and Turkey create additional hurdles, affecting Iraq's willingness and ability to pursue international remedies or escalate the issue to bodies like the UNSC. These constraints underscore the difficulties in navigating the international legal system when addressing cyberattacks that may originate from or involve multiple states or non-state actors. The paper has also gone ahead to discuss the real-life implications of such legal and political challenges, noting that though in theory, international legal mechanisms provide avenues for recourse, but in practice, they are usually hindered due to a lack of political will and requirements of comprehensive evidence of broader regional impacts. The findings of this paper fill the gaps with regard to the legal issues surrounding the use of drones in cyber warfare and advanced warfare and they call for the establishment of adequate solutions to protect sovereignty and security in the modern digital context. Since cyber threats will continue to evolve, relevant international legal norms and practical strategies must keep adapting to cope with and mitigate the risks of such an attack effectively. This means that, in the face of continuous change in the global cyber-war landscape, further development of legal and practical responses is called for to afford resilience and security in the international order.

10.2 Recommendations

To enhance the response to drone cyber-attacks in KRI, several recommendations can be proposed:

1. Establishing a Strong Cyber Defense Mechanism: The Kurdistan Region and Iraq need to create robust cyber-security infrastructures to reduce the potential impacts of cyberattacks. This approach will include upgrading to advanced technologies, conducting regular security assessments, and fostering collaboration with international cyber-defense organizations.

2. Establish Clear Legal Standards for Cyber Operations: It is essential to create more defined and specific international legal standards that address cyber operations, including drone cyberattacks. The global community should collaborate to formulate clear guidelines and norms to guarantee that responses are appropriate, necessary, and reversible.

3. Improve International Cooperation: Iraq and the KRI should enhance their role in international forums, advocating for better norms and practices of cooperation. It orchestrates the establishment of goodwill with other international partners for aid or intervention in addition to diplomatic communications dealing with geopolitical thorns that hinder effective responses.

4. To promote political-diplomatic engagement, Iraq must navigate its regional relationships and security needs amid political constraints. This involves advocating for a consensus on cyberattacks and engaging in discussions with international partners about how political challenges hinder specific avenues for legal recourse.

5. Considering that the Responsibility of States for Internationally Wrongful Acts, 2001, represents a foundational structure in modern international law, it would be apposite that this instrument be revisited by the UN General Assembly during its 80th session in September 2025. While widely regarded as being of authoritative status, the instrument remains merely a draft, devoid of binding force to lead states uniformly in case of internationally wrongful acts. To address this gap, the UNGA could add the draft project to its agenda, encouraging discussions among member states about its potential adoption as a treaty or examining ways to further develop it. This initiative would

ISSN-Print: 2079-3901
ISSN-Online: 3005-396X

enhance international legal accountability and clarify state responsibilities in the face of emerging global challenges. Such a move aligns with the UN's broader mission to promote justice, accountability, and the rule of law on an international scale. Therefore, given the increasing complexity of state interactions and the growing reliance on the principles outlined in this draft, the 80th session offers a timely opportunity for the General Assembly to advance this important instrument within the framework of international law.

6. Establishing robust political support for the creation of a Kurdish state, with guarantees from the international community. This support would help the Kurdistan Region uphold its sovereignty as a state in alignment with the principles of international law.

References

- **Books**

Irani, P. K. (1964). International law and the use of force by states. [Online]. Oxford University Press. Last Accessed 4 September 2024 at: https://academic.oup.com/book/10823.

Marossi, A. & Bassett, M. (2015). Economic sanctions under international Law: Unilateralism, Multilateralism, Legitimacy, and Consequences. [online]. Den Haag: Springer. Last Accessed 15 September 2024 at: https://link.springer.com/book/10.1007/978-94-6265-051-0.

Roscini, M. (2014) Cyber operations and the use of force in international law. [Online]. Oxford University Press. Last Accessed 1 September 2024 at: https://books.google.iq/.

Schmitt, M. N. (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. {Online}. Cambridge University Press. Last Accessed 19 November 2024 https://assets.cambridge.org/97811071/77222/frontmatter/9781107177222_frontmatter.pdf.

Schmitt, M.N. (2013) Tallinn Manual on the International Law Applicable to Cyber Warfare. {Online}. Vol. 141. Cambridge: Cambridge University Press. Last Accessed 21 July 2024 at: https://www.penncerl.org/wp-content/uploads/2021/12/6481-tallinn-manual-on-the-international-law-applicable.pdf .

- **Theses**

O'Meara, C. (2021). Necessity and Proportionality and the Right of Self-defence in International Law. PhD thesis, University College London. [online]. Last Accessed 15 September 2024 at: https://discovery.ucl.ac.uk/id/eprint/10057299/.

Scientific Journals

ISSN-Print: 2079-3901
ISSN-Online: 3005-396X

Boylan, E. (2017). Applying the Law of Proportionality to Cyber Conflict: Suggestions for Practitioners. [online]. Vanderbilt Journal of Transnational Law, 50, pp. 217-252. Last Accessed 15 September 2024 at: https://scholarship.law.vanderbilt.edu/cgi/viewcontent.cgi?article=1127&context=vjtl.

Brooks, R. (2014). Drones and the international rule of law. [Online]. Ethics & International Affairs, 28(1), pp. 83-103.Last Accessed 26 August 2024 at: https://scholarship.law.georgetown.edu/cgi/viewcontent.cgi?article=2296&context=facpub.

Chang, C. H. (2023). How Does the Tallinn Manual 2.0 Shed Light on the Threat of Cyber Attacks against Taiwan?. [online]. European Conference on Cyber Warfare and Security, 22(1), pp. 649-656. Last Accessed 10 September 2024: https://papers.academic-conferences.org/index.php/eccws/article/view/1294.

Check, T. (2022). The Tallinn Manual 2.0 on Nation-State Cyber Operations Affecting Critical Infrastructure. [online]. National Security Law Brief, 13, pp. 1-XX. Last Accessed 10 September 2024: https://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?article=1150&context=nslb.

Coco, A., Dias, T. and van Benthem, T. (2022). 'Illegal: The SolarWinds hack under international law. [Online]. European Journal of International Law, 33(4), pp. 1275-1286. Last Accessed 18 September 2024: https://academic.oup.com/ejil/article/33/4/1275/6881099.

Cornthwaite, J. L. (2019) Can we shoot down that drone? An examination of international law issues associated with the use of territorially intrusive aerial and maritime surveillance drones in peacetime. [Online]. Cornell International Law Journal, 52, p. 475. Last Accessed 30 August 2024 at: https://ww3.lawschool.cornell.edu/research/ILJ/upload/Cornthwaite-final.pdf.

Currier, E.O (2023). After action: The US drone program's expansion of international law justification for use of force against imminent threats. [Online]. Vanderbilt Law Review, 76, pp. 259. Last Accessed 25 August 2024 at: https://scholarship.law.vanderbilt.edu/cgi/viewcontent.cgi?article=4842&context=vlr .

Doyle, J. (2013). Rise of the robots: Western unmanned air operations in Iraq and Afghanistan, 2001 to 2010. {Online}. Air Power Review, 16(2), pp. 10-31. Last Accessed 3 July 2024 at: https://raf.mod.uk/what-we-do/centre-for-air-and-space-power-studies/aspr/apr-vol16-iss2-1-pdf/.

Goldsmith, J. and Loomis, A. (2021) Defend Forward and Sovereignty. [Online]. Hoover Working Group on National Security, Technology and Law. Aegis Series Paper, (2102). Last Accessed 31 August 2024 at: https://www.lawfaremedia.org/article/defend-forward-and-sovereignty.

Haataja, S. (2017). The 2007 cyber attacks against Estonia and international law on the use of force: an informational approach. [Online]. Law, Innovation and Technology, 9(2), pp. 159-189. Last Accessed 18 September 2024: https://www.tandfonline.com/doi/abs/10.1080/17579961.2017.1377914.

ISSN-Print: 2079-3901
ISSN-Online: 3005-396X

Henriksen, A. (2019) The end of the road for the UN GGE process: The future regulation of cyberspace. [Online]. Journal of Cybersecurity, 5(1), tyy009. Last Accessed 30 August 2024 at: https://watermark.silverchair.com/ .

Herzog, S. (2011). Revisiting the Estonian cyber attacks: Digital threats and multinational responses. [Online]. Journal of Strategic Security, 4(2), pp. 49-60. Last Accessed 18 September 2024: https://www.jstor.org/stable/26463926.

Jarose, J. (2023). Reconsidering the definition of 'attack' and 'damage' in cyber operations during armed conflict: Emerging subsequent state practice. [online]. The Adelaide Law Review, 44(2), pp. 317-338. Last Accessed 10 September 2024: https://search.informit.org/doi/abs/10.3316/informit.514594046455151.

Khan, A. (2023) The Ambiguity in International Law and Its Effect on Drone Warfare and Cyber Security. [Online]. MA Major Research Papers, 22. Last Accessed 8 September 2024: https://ir.lib.uwo.ca/politicalscience_maresearchpapers/22/ .

Krebs, S. (2023). Above the law: Drones, aerial vision and the law of armed conflict–a socio-technical approach. [Online]. International Review of the Red Cross, 105(924), pp. 1690-1728. Last Accessed 5 September 2024: https://www.cambridge.org/core/journals/international-review-of-the-red-cross/article/above-the-law-drones-aerial-vision-and-the-law-of-armed-conflict-a-sociotechnical-approach/37559D8B9692011DD91576B07D311E28.

Lotrionte, C. (2012). State sovereignty and self-defense in cyberspace: A normative framework for balancing legal rights. [Online]. Emory International Law Review, 26, pp. 825. Last Accessed 23 August 2024 at: https://scholarlycommons.law.emory.edu/cgi/viewcontent.cgi?article=1072&context=eilr .

Margulies, P. (2013). Sovereignty and cyber attacks: Technology's challenge to the law of state responsibility. [Online]. Melbourne Journal of International Law, 14(2), pp. 496-519. Last Accessed 25 August 2024 at: https://search.informit.org/doi/abs/10.3316/INFORMIT.117621131187624 .

Mimran, T. (2022). Between Israel and Iran: Middle-East attitudes to the role of international law in the cyber-sphere. [Online]. Baltic Yearbook of International Law Online, 20(1), pp. 209-235. Last Accessed 16 September 2024: https://www.balticyearbook.org.

O'Connell, M. E. (2009). Unlawful killing with combat drones: a case study of Pakistan, 2004-2009', in Bronitt, S. (ed.) Shooting to kill: The law governing lethal force in context. [Online]. Notre Dame Legal Studies Paper, (09-43). Last Accessed 4 September 2024 at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1501144.

Rid, T. and Buchanan, B. (2015). Attributing cyber attacks. [Online]. Journal of Strategic Studies, 38(1-2), pp. 4-37. Last Accessed 19 August 2024 at: https://www.tandfonline.com/doi/full/10.1080/01402390.2014.977382?scroll=top&needAccess=true .

ISSN-Print: 2079-3901
ISSN-Online: 3005-396X

Sadeghi, S.S. (2016). Turkish strategy in the Iraqi Kurdistan and Syrian Kurdish region and Iran. {Online}. Iranian Review of Foreign Affairs, 7(24), pp. 57-84. Last Accessed 3 July 2024 at:: https://irfajournal.csr.ir/article_125139.html.

Sadurska, R. (1988). Threats of force. [Online]. American Journal of International Law, 82(2), pp. 239-268. Last Accessed 4 September 2024 at: https://www.cambridge.org/core/journals/american-journal-of-international-law/article/abs/threats-of-force/1C28A6B9CBB526C500B8CD6121504639.

Sayankina, S. (2017). Drone strikes in violation of territoriality: How are they justified?. [Online]. Journal of Territorial and Maritime Studies. Last Accessed 29 August 2024 at: https://www.journalofterritorialandmaritimestudies.net/post/2017/05/19/drone-strikes-in-violation-of-territoriality-how-are-they-justified.

Walzer, M. (2016). Just & unjust targeted killing & drone warfare. Daedalus, 145(4), pp. 12-24. Last Accessed 30 August 2024 at: https://direct.mit.edu/daed/article/145/4/12/27115/Just-amp-Unjust-Targeted-Killing-amp-Drone-Warfare.

Waxman, M. C. (2011). Cyber-attacks and the use of force: Back to the future of Article 2(4). [Online]. Yale Journal of International Law, 36, pp. 421. Last Accessed 3 September 2024 at: https://openyls.law.yale.edu/bitstream/handle/20.500.13051/6629/14_36YaleJIntlL421_2011_.pdf?sequence=2&isAllowed=y.

Yadron, D., Barrett, D. and Barnes, J. E. (2014). U.S. struggles for response to Sony hack. [Online]. The Wall Street Journal. Last Accessed 15 September 2024: https://www.wsj.com/articles/u-s-struggles-for-response-to-sony-hack-1418950806.

- **Websites**

Amwaj.media (2024). Rare attack near heart of Iraqi Kurdish power holds multiple messages. [Online]. Amwaj.media. Last Accessed 16 August 2024 at: https://amwaj.media/media-monitor/drone-strike-near-kdp-headquarters-sends-domestic-and-geopolitical-message .

Aydogan, B. (2024). Iraq's Kurdish Regional Government says it thwarted drone attack on US-led coalition base. [Online]. Anadolu Ajansı. Last Accessed 16 August 2024 at: https://www.aa.com.tr/en/middle-east/iraq-s-kurdish-regional-government-says-it-thwarted-drone-attack-on-us-led-coalition-base/3109983#.

Azhari, T. (2024). Attack on Iraqi Kurdish gas field leads to major power cuts. [Online]. Reuters. Last Accessed 17 August 2024 at: https://www.reuters.com/world/middle-east/explosive-drone-strikes-iraqs-khor-mor-gas-field-sources-2024-01-25/ .

Best, K. L., Schmid, J., Tierney, S., Awan, J. A. L. A. L., Beyene, N. M., Holliday, M. A., & Lee, K. (2020). How to analyze the cyber threat from drones. [online]. RAND Arroyo Center. Last Accessed 16 September 2024: https://www.rand.org/pubs/research_reports/RR2972.html .

ISSN-Print: 2079-3901
ISSN-Online: 3005-396X

Cherry, L.M. and Pascucci, P.P. (2023). International law in cyberspace. American Bar Association. [Online]. Last Accessed 26 August 2024 at: https://www.americanbar.org/groups/law_national_security/publications/aba-standing-committee-on-law-and-national-security-60-th-anniversary-an-anthology/international-law-in-cyberspace/.

Doski, D. (2023). Kurdistan and the United States: ISIS defeated, what happens now?. {Online}. Wilson Center. Last Accessed 12 July 2024 at: https://www.wilsoncenter.org/article/kurdistan-and-united-states-isis-defeated-what-happens-now .

Faidhi, K. (2024). Khor Mor drone attack draws international condemnation. [Online]. Rudaw. Last Accessed 8 September 2024: https://www.rudaw.net/english/kurdistan/27042024.

Frantzman, S.J. (2021). US concerned after Turkey attacks refugee camp. [Online]. The Jerusalem Post. Last Accessed 16 July 2024 at: https://www.jpost.com/middle-east/us-concerned-after-turkey-attacks-refugee-camp-670217 .

Human Rights Watch (2024). Iraq: Iranian attack kills civilians in Erbil. [Online]. Last Accessed 17 July 2024 at: https://www.hrw.org/news/2024/01/22/iraq-iranian-attack-kills-civilians-erbil .

Iddon, P. (2024). U.S.-allied Kurdish security forces face unprecedented drone attacks. {Online}. Forbes. Last Accessed 3 July 2024 at: https://www.forbes.com/sites/pauliddon/2024/02/06/us-allied-kurdish-security-forces-face-unprecedented-drone-attacks/.

International armed conflict (2024). [online]. International Cyber Law. Last Accessed 10 September 2024 at: https://cyberlaw.ccdcoe.org/wiki/International_armed_conflict.

International Bar Association (2017) The Legality of Armed Drones Under International Law. Background paper by the International Bar Association's Human Rights Institute. Adopted in May 2017. pp. 1-56. [Online]. Last Accessed 8 September 2024: https://www.ibanet.org/medias/B0B8AF88-FD20-44F8-A920-634484645113.pdf?context=bWFzdGVyfGFzc2V0c3w0Mzg3MDJ8YXBwbGljYXRpb24vcGRmfGFERmxMMmhpTWk4NE56azJNek00TVRreU5ERTBMMEl3UWpoQlJqZzRMVVpFTWpBdE5EUkdPQzFCT1RJd0xUWXpORE0TkRZME5URXhNeTV3WkdZfGYzMjdhZjRjY2RhMDM0M2Y3NmVlOTFkYzFiZjQ2ODY3OTUwYmQ1MDE0NWUyNTg4OTEzMmI5Y2Q1NmEwOTA4NTU#:~:text=Article%202(4)%20of%20the,of%20Article%202(4).

Isamel, Y. (2022). Turkey's growing military presence in the Kurdish region of Iraq. [Online]. The Washington Institute for Near East Policy, 18. Last Accessed 15 July 2024 at: https://www.washingtoninstitute.org/policy-analysis/turkeys-growing-military-presence-kurdish-region-iraq .

Jones, S.G., Newlee, D., Harrington, N. & Bermudez Jr, J.S. (2019). Iran's threat to Saudi critical infrastructure: The implications of US-Iranian escalation. [online]. Last Accessed 15 September 2024 at: https://apo.org.au/node/253086.

ISSN-Print: 2079-3901
ISSN-Online: 3005-396X

Kurdistan Region of Iraq (2019). The Snapshot: KRI. Brand KR. [online]. Last Accessed 16 September 2024: https://brandkri.com/the-krg-structure/.

Ministry for Europe and Foreign Affairs. (2023). Attack in Iraqi Kurdistan (31 December 2023). [Online]. Last Accessed 18 August 2024 at: https://www.diplomatie.gouv.fr/en/country-files/iraq/news/article/attack-in-iraqi-kurdistan-31-dec-2023 .

Moynihan, H. (2019) The application of international law to state cyberattacks. Chatham House. Last Accessed 29 August 2024 at: www.chathamhouse.org/2019/12/application-international-law-state-cyberattacks/2-application-sovereignty-cyberspace.

O'Connell, M.E. (2019). Drone attacks on Saudi Aramco oil installations. [Online]. Last Accessed 22 August 2024 at: https://scholarship.law.nd.edu/ndls_news/535/.

Oxford Research Group (2011). Discussion paper: Drone attacks, international law, and the recording of civilian casualties of armed conflict. [Online]. Last Accessed 25 August 2024 at: https://reliefweb.int/report/afghanistan/discussion-paper-drone-attacks-international-law-and-recording-civilian.

Schmitt, M. (2014). International Law and Cyber Attacks: Sony v. North Korea. [Online]. Just Security. Last Accessed 31 August 2024 at: https://www.justsecurity.org/18460/international-humanitarian-law-cyber-attacks-sony-v-north-korea/.

Sirwan, D. (2021). Drone wars in Iraq. {Online}Rudaw, 25 June. Last Accessed 13 July 2024 at: https://www.rudaw.net/english/analysis/25062021.

Van Wilgenburg, W. (2024). Arab countries condemn Khor Mor gas field attack. [online]. KurdistanChronicle. Last Accessed 10 September 2024: https://kurdistanchronicle.com/b/3047.

Washington Kurdish Institute (2020) Turkey's military aggression in Iraqi Kurdistan once again targets refugees. {Online}. 20 April. Last Accessed 15 July 2024 at: https://dckurd.org/2020/04/20/turkeys-military-aggression-in-iraqi-kurdistan-once-again-targets-refugees/.

- **Legal Documents**

UN General Assembly (1970) Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations, A/RES/2625(XXV), 24 October. [Online]. Last Accessed 8 September 2024: https://www.refworld.org/legal/resolution/unga/1970/en/19494.

UN General Assembly (1970). Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations, A/RES/2625(XXV). [Online]. Last Accessed 31 August 2024 at: https://www.refworld.org/legal/resolution/unga/1970/en/19494.

ISSN-Print: 2079-3901
ISSN-Online: 3005-396X

UN General Assembly (1974) Definition of aggression (A/RES/3314(XXIX)). [Online]. Last Accessed 29 August 2024 at: https://digitallibrary.un.org/record/190983?v=pdf&ln=en .

United Nations. (2001). Responsibility of States for Internationally Wrongful Acts. [Online]. Last Accessed 19 August 2024 at: https://legal.un.org/ilc/texts/instruments/english/draft_articles/9_6_2001.pdf.

International Law Commission. Responsibility of States for Internationally Wrongful Acts. [Online]. Supplement No. 10 (A/56/10), 2001. Last Accessed 19 November 2024 at: https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf .

- **Legal Cases**

International Court of Justice (1984). Nicaragua v. United States of America, 10 September. [Online]. Last Accessed 1 September 2024 at: https://www.icj-cij.org/case/70/intervention.

گوزەرێک بەناو ئاستەنگە یاساییەکان لە هێرشە ئەلیکترۆنییەکانی فڕۆکەی بێفڕۆکەوان کەیسی هەرێمی کوردستانی عێراق

پ. ی. د. صانع شریف قادر
بەشی یاسا، فاکەڵتی یاسا و زانستە سیاسییەکان و بەڕێوەبردن، زانکۆی سۆران، هەرێمی کوردستان- عێراق
ئیمێل: sanh.qadir@soran.edu.iq

پوختە

ئەم توێژینەوەیە ڕوانگەیەکی یاسای نێودەوڵەتییە سەبارەت بە وردبینی ئەو ئاڵنگارییانەی پەیوەستن بە هێرشە ئەلیکترۆنییەکانی فڕۆکەی بێفڕۆکەوان دژی هەرێمی کوردستانی عێراق، ئامانجی لێکۆڵینەوەیە لەو ڕێگایانەی کە کارلێک لەگەڵ بنەما دامەزراوەکان دەکەن، وەک (سەروەری دەوڵەت، قەدەغەکردنی دەستوەردان و قەدەغەکردنی بەکارهێنانی هێز) بەپێی یاسا نێودەوڵەتییەکان، بە بەکارهێنانی چوارچێوە دامەزراوەکانی وەک دەستنووسی تالین، پرۆژەی بەرپرسیارێتی دەوڵەتان لە کردەوە ناڕەوا نێودەوڵەتییەکان، و جارنامەی نەتەوەیەکگرتووەکان. هەروەها ئەم توێژینەوەیە لە بنەما یاساییەکانی ڕێوشوێنی بەرپەرچدانەوە لە هێرشە ئەلیکترۆنییەکانی فڕۆکەی بێفڕۆکەوان دەکۆڵێتەوە کە پێکهاتووە لە ڕێوشوێنی دیپلۆماسی و ئابووری و ئەلیکترۆنی لە ژێر ڕۆشنایی جێبەجێکردن و هەماهەنگی هەرێمی کوردستان لەگەڵ حکومەتی فیدراڵی عێراقدا. زیاتر لەمەش، توێژینەوەکە باس لەوە دەکات کە چۆن دامەزراوە یاساییە نێودەوڵەتییەکانی وەک (دادگای دادی نێودەوڵەتیICJ و ئەنجومەنی ئاسایشی نەتەوەیەکگرتووەکانUNSC) دەتوانن ڕێگری لەم جۆرە هێرشانە بکەن. بۆ هەڵسەنگاندنی هێرشە ئەلیکترۆنییەکانی فڕۆکەی بێفڕۆکەوان لە چوارچێوەی بنەماکانی یاسای نێودەوڵەتیدا، ئەم توێژینەوەیە پشت بە ڕێبازێکی چۆنایەتی دەبەستێت کە بریتییە لە پێداچوونەوە بە (بەڵگەنامەی یاسایی، توێژینەوەی کەیسەکان، و بۆچوونی پسپۆڕان). جگە لەوەش، لەلایەک توێژینەوەکە جەخت لەسەر پرسەکانی ڕێژەیی و پێویستیی ڕێوشوێنی بەرپەرچدانەوەو دەکاتەوە، لەلایەکی دیکەشەوە ئەو دوو فاقییانەی کەڕووبەڕووی هەرێمی

ISSN-Print: 2079-3901
ISSN-Online: 3005-396X

کوردستان دەبنەوە، ئەمەش بەهۆی ئەو سنوردارکردنە سیاسی و دیپلۆماسییانەی لە ئەنجامی دەوڵەتی عێراقەوە هاتوونەتە ئاراوە. توێژینەوەکە دەریدەخات، لە کاتێکدا هەرێمی کوردستانی عێراق توانای گرتنەبەری هەندێک ستراتیژی بەرگریی هەیە بەڵام دەستنیشانکردنی وەڵامە نێودەوڵەتییە گونجاوەکان پێویستی بە ڕەچاوکردنی وردی پێوەرە یاساییەکان و فشارە جیۆپۆلەتیکییەکان هەیە.

وشە کلیلییەکان: هێرشی ئەلیکترۆنی فڕۆکەی بێفڕۆکەوان، هەرێمی کوردستانی عێراق، یاسای نێودەوڵەتی، سەروەری، ڕێوشوێنی بەرپەرچدانەوە، بەرپرسیارێتی دەوڵەتان لە کردەوە ناڕەوا نێودەوڵەتییەکان.

التعامل مع التحديات القانونية في الهجمات الإلكترونية باستخدام الطائرات المسيرة: حالة إقليم كوردستان العراق

أ. م. د. صانع شريف قادر
قسم القانون، كلية القانون والعلوم السياسية والإدارية، جامعة سوران، إقليم كردستان- العراق
ئیمێل: sanh.qadir@soran.edu.iq

ملخص

تقدم هذه الدراسة منظورًا قانونيًا دوليًا حول دقة التحديات المرتبطة بالهجمات الإلكترونية، باستخدام الطائرات بدون طيار ضد إقليم كردستان العراق. ويهدف هذه البحث الى معرفة طرق تفاعلها مع المبادئ الراسخة، مثل (سيادة الدولة، وحظر التدخل، وحظر استخدام القوة) بموجب القانون الدولي، وذلك باستخدام الأطر الراسخة مثل دليل تالين، والمواد المتعلقة بمسؤولية الدول عن الأخطاء الدولية، وميثاق الأمم المتحدة. تتناول هذه البحث أيضًا الأساس القانوني للإجراءات المضادة ضد الهجمات السيبرانية بدون طيار، والتي تتكون من تدابير دبلوماسية واقتصادية وسيبرانية في ضوء تنفيذ وتنسيق إقليم كردستان مع الحكومة الفيدرالية العراقية . فضلاً على ذلك يناقش البحث كيف يمكن للمؤسسات القانونية الدولية مثل محكمة (العدل الدولية، ومجلس الأمن التابع للأمم المتحدة) التي ينبغي ان تمنع مثل هذه الهجمات. لتقييم الهجمات الإلكترونية باستخدام الطائرات بدون طيار ضمن مبادئ القانون الدولي، ويعتمد هذه البحث على منهج نوعي بما في ذلك مراجعة (الوثائق القانونية ودراسات الحالة وآراء الخبراء) بالإضافة إلى ذلك يؤكد البحث على قضايا التناسب والحاجة إلى تدابير مضادة من جهة ، ومن جهة اخرى عن المعضلات التي يواجهها إقليم كردستان، بسبب القيود السياسية والدبلوماسية الناتجة عن الدولة العراقية. ويظهر البحث أنه في حين أن إقليم كردستان العراق قادر على تبني بعض الاستراتيجيات الدفاعية، فإن تحديد الاستجابات الدولية المناسبةَ يتطلبُ منه دراسة متأنية للمعايير القانونية ، والضغوط، الجيوسياسية.

الكلمات المفتاحية: الهجمات الإلكترونية بالطائرات المسيرة، إقليم كردستان العراق، القانون الدولي، السيادة، التدابير المضادة، مسؤولية الدول عن الأفعال غير المشروعة دوليا.