DOI: 10.53477/1841-5784-21-18

EXTENSION OF INTERNATIONAL HUMANITARIAN LAW ORDER IN THE INFORMATION AREA THROUGH DIGITAL DIPLOMACY

Daniel DUMITRU, PhD*
Cristina BODONI**

Hybrid threats cover the whole spectrum of fake news, cyber/information warfare. They periodically impose the multimedia agenda in all known spaces to man. If for the Earth's natural spaces, we have norms and customs respected international, the navigation in the digital space does not confer to the user the same protection given by a code of laws accepted worldwide, although we have a new set of instruments with shield role against dangers called cyber security. In order for this cyber security to be accepted by as many (non) state actors as possible, we need international norms, built by professionals with expertise and proactive thinking. The people with specific responsibilities for negotiating such rules are diplomats, in this case we have the digital diplomats. What is their purpose? What is the connection between hybrid warfare, digital diplomacy and humanitarian law? These are questions that we answer through this research. In the structure of the paper we used concepts from International Humanitarian Law (IHL) norms that can be adapted to cyber operations and hybrid threats. In the case of the use of aggressive cyber actions and cyber capabilities, the competence of current international law is the objective of the article for the emergence of the right to self-defence. Then, we look at aspects of military actions involving cyber-attacks, designed on the spectrum of the cyber operation, and these cyber actions will be examined applying principles established by existing laws.

**** Daniel DUMITRU, PhD, is Professor and PhD advisor in the field of Information and National Security within "Carol I" National Defence University, Bucharest, Romania. E-mail: daniel_dumitru64@yahoo.com***
***** Cristina BODONI is PhD Student in the field of Information and National Security, "Carol I" National Defence University, Bucharest, Romania. E-mail: cristina_bodoni@yahoo.co.uk***

Keywords: *hybrid threats; cyber-attacks; international humanitarian law; military operations; cybercrime; digital diplomacy.*

Argumentum

"Change is the law of life. And those who look only to the past or present are certain to miss the future".
John F. Kennedy

Our study begins with this quote because it maintains its validity. It is more current than ever whereas it warns law enforcement about an uncertain future, in which individuals have entered a vortex of change produced by technological innovation, simply amoral. Here we really need new rules or the adaptation of the old ones to new requirements. Thus, the involvement of law enforcement in the reformulation of the national and international legislative code is permanent, they must be aware that law is not a system of abstract logic, it is the result of a negotiation between world's legal and jurisdictional professionals.

This is a network of arrangements with deep historical roots and current new branches promoted in the hope that old practices that are proportionately integrated into current (inter) national security rules, especially national security. Regardless of the state of affairs, peace or war, in all natural spaces and artificial information, we need a competent diplomacy for using all possible tools to succeed in obtaining international norms useful for as many users of digital tools. These rules have become necessary in a world where the number of hybrid threats has grown exponentially because they cause vulnerability in security systems and the most powerful states, the risk of escalation increases proportionally, and can turn into cyber war at any time. This sector of activity has become one of the main security threats facing all types of (non) state actors, in which we have not yet accepted adequate and legitimate mechanisms in the management of new types of war through transferable rules in cyberspace.

Nowadays we face an anarchic yet functional world society, which does not eliminate conflict, it can act preventively in order to change the form of conflict, placing more emphasis on non-violent forms of coercive activity[11].

The aim of this study is to present digital diplomacy as a promoter of innovative approaches to war law. To achieve the objective of this study, we shall present some examples. These are given by underlining relevant articles of the Four

[1] A.J.R. Groom, André Barrinha and William C. Olson. *International Relations Then and Now Origins and Trends in Interpretation.* Second Edition. Routledge, Taylor & Francis Group, New York, USA, 2019, p. 117.

Geneva Conventions (Humanitarian Treaties) of 1949, Two Additional Protocols of 1977 and Protocol III of 2005, in the process of adapting to the requirements of the globalized information system.

The working hypothesis for this approach is a syllogism that starts from the premise that the horrors of war had led to diplomatic negotiations for the initiation of international rules that could come into operation in times of war. These conventions and protocols are currently an integral part of International Humanitarian Law (IHL). If negotiations belong to diplomats and diplomacy has entered the information age, then digital diplomacy can bring forward diplomatic negotiation in the IHL plan in order to have new rules adapted to the new requirements of the information space.

This research is empirical and exploratory. Being enunciated through a syllogism, the hypothesis introduces us to the transdisciplinary study, built on the principle of causality with the help of the inductive method[2].

The article contains three sections. In the first, *Digital Diplomacy and Cyber Diplomacy, Hybrid Threats and Information Warfare*, we have defined the main concepts related to diplomacy and security in the information age. In the second section, *Updating Traditional Warfare and Its Extension in Cyberspace,* we have included the terminology for cyber warfare and cyber incidents through factual examples of borderline situations that states may face and that have reinterpreted state security. In the third section, *Cyber hostile actions and politico-diplomatic responses*, limits for war and international humanitarian law, in which we have correlated the factors and concepts described with relevant aspects of the war-adapted IHL in the information age.

1. Digital Diplomacy and Cyber Diplomacy, Hybrid Threats and Information Warfare

Diplomacy has been gradually defined according to the context of the times, the environment and by the people who influenced the foreign policies of the states, and afterwards within the international organizations. One of the definitions that remains valid for almost two centuries belongs to Baron Ferdinand de Cussy. He defined diplomacy in 1846 as "all the knowledge and principles that are necessary to conduct well public affairs between states."[3]. In 1975, Mircea Malița considered diplomacy a professional nucleus around which four distinct elements revolve[4]:

[2] Marcel T. Djuvara, *Metoda inductivă și rolul ei în științele explicative*, Noua Tipografie Profesională Dimitrie C. Ionescu, Bucharest, 1910, p. 6.

[3] Ferdinand de Cussy, *Dictionnaire ou manuele-lexique du diplomate et du consul,* Tipographie de F. A. Brockhaus, Leipzig, 1846, p. 256.

[4] Mircea Malița, *Diplomația. Școli și Instituții*, Didactică și Pedagogică Publishing, Second Edition, Bucharest, 1975, p. 44.

"history, international relations, conflict theory and international law". In the 21st century, Corneliu Bjola and Markus Kornprobst consider that diplomacy is made up of four components[5]: "Institutionalized communication, double recognition, focus on the provision of public goods and productive capacity (e.g. global decision-making, relationships and rules)". It has officially mastered the established tools of the information age, which has led to the connection of technical terms in the field of technology, information and communications with diplomacy. After many attempts to link diplomacy with the information space, to impose it on independent platforms, social networks and internet search engines, as well as a specific type of activity undertaken at a given time, digital and cybernetic are the two adjectives that remained representative of the diplomacy practiced in the 1920s. We often explain them as synonymous[6]. Sometimes, we can find in articles, manuals or official documents "different prefixes, the same meaning: cybernetic, digital, net, online, virtual, e-"[7] alongside diplomacy.

In recent official documents of the European Union, cyber diplomacy appears more often than digital diplomacy. In "Revisiting the EU Cybersecurity Strategy: A Call for EU Cyber Diplomacy" published in February 2021, Annegret Bendiek and Matthias C. Kettemann do not mention digital diplomacy under no circumstances. They place cyber diplomacy in tandem with digital foreign policy as a form of style, so as not to repeat the terms. They highlight the role of diplomacy and propose an extended mandate for the European External Action Service (equivalent to the Foreign Ministry of the European Union) in building a normative code through negotiations for cyberspace and information and for which it must be empowered for this task of diplomacy cyber[8]. For Barrinha and Renard, cyber diplomacy is an "emerging international practice that seeks to build an international cyber society, linking the national interests of states with the dynamics of world society – the predominant realm in which cyberspace has evolved over the past four decades"[9]. It should be noted that even here, the term digital diplomacy never appears. Ilan Manor argues that digital diplomacy is "digitization of public diplomacy"[10], and

[5] Corneliu Bjola, Markus Kornprobst, *Understanding International Diplomacy Theory, Practice and Ethics,* Second Edition, Routledge, Abington, Oxon, UK, 2018, p. 238.

[6] André Barrinha, Thomas Renard, "Cyber-diplomacy: the making of an international society in the digital age", *Revue Global Affairs*, No. 3:4-5, pp. 353-364, 2017, URL: https://doi.org/10.1080/23340460.2017.1414924, accessed on 25.10.2021.

[7] Jovan Kurbalija, *An introduction to internet governance*, Published by DiploFoundation, Geneva, Switzerland, 2016, p. 14.

[8] Annegret Bendiek, Matthias C. Ketteman, *A revising the EU Cybersecurity Strategy: A call for EU Cyber Diplomacy,* SWP Comment, No. 16, 16 February 2021, p. 3, URL: https://www.swp-berlin.org/publications/products/comments/2021C16_EUCyberDiplomacy.pdf, accessed on 21.10.2021.

[9] André Barrinha, Thomas Renard, *op. cit.* p. 353.

[10] Ilan Manor, *The Digitalization of Public Diplomacy*, Palgrave Macmillan Publishers, Basingstoke,

Corneliu Bjola attributes the main role in "the use of social networks for diplomatic purposes"[11]. For Brian Hocking and Jan Melissen, digital diplomacy is often equated with public diplomacy, but also includes:

a) changing foreign policy agendas;

b) cyber agendas for issues and negotiation scenarios;

c) knowledge management in the issue of efficient data management;

d) the provision of digitized consular services and crisis management[12].

From the above definitions an idea emerges: that diplomatic practice in the 21st century indicates that diplomacy has entered the information age, it is in an accelerated process of hybridization in the "virtual environment, generated by cyber infrastructures, including processed information content, stored or transmitted, as well as the actions performed by users in it"[13].

Thus, in order to manage threats and risks, to exploit hybrid threats and cyber warfare, we have at our disposal coercive and non-coercive means (in the fields of diplomacy, security and defence) to choose between multiple approaches and meanings according to them, even if the new definitions of hybrid threats are not few.

We have an impressive number of definitions that involve generic terms of security, protection and safety, especially for those related to security threats in situations arising from the behaviour of (non) state and individual actors, and not to complicate the framework. For our national security, we have chosen the following working definition: in its broadest sense, national security is a situation of normalcy of a state, "a country in which every citizen lives in a safe environment and trusts that the institutions, which he supports, defends and protects"[14]. This definition introduces hybrid threats because they "encompass the mixture of coercive and subversive activities, conventional and unconventional methods (e.g. diplomatic, military, economic, technological) that can be used in a coordinated way by state or non-state actors. to achieve specific objectives, without exceeding the officially declared threshold of a state of war"[15]. Thus we have a reference to attack and armed conflict.

UK, 2019, passim.

[11] Corneliu Bjola, Markus Holmes, *Digital Diplomacy: Theory and Practice*, Routledge New Diplomacy Studies, Abington, UK, 2015, p. 4.

[12] Brian Hocking, Jan Melissen, *Diplomacy in the Digital Age.* Clingendael Report. Netherlands Institute of International Relations Clingendael, Netherlands, 2015, pp. 3-4.

[13] ***, *Strategia de securitate cibernetică a României,* p. 4, URL: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/roncss.pdf, accessed on 20.10.2021.

[14] ***, *Strategia Națională de Apărare a Țării pentru perioada 2020-2024. "Împreună, pentru o Românie sigură și prosperă într-o lume marcată de noi provocări"*, Monitorul Oficial, I[st] Part, No. 574, from 1 July 2020, p. 5.

[15] ***, *Comunicare Comună către Parlamentul European, Consiliul European, Consiliu, Comitetul Economic și Social European și Comitetul Regiunilor din 5 decembrie 2018, Plan de acțiune împotriva dezinformării,* p. 2, URL: https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:52018JC0036&from=RO, accessed on 04.06.2021.

An armed attack is one "committed by a person with a firearm or with objects, devices, substances or animals that may endanger the life, health or bodily integrity of people"[16]. In our case, the extended war in cyberspace, "an extension of a nation's attack surface"[17]. In order to better understand the polemological practical meaning of this new field we have the following definition: with internet access, from mobile phone to smart refrigerator[18]; and, Henrotin defined information warfare as a set of information-driven actions and attacks that result in the destruction or incapacitation of enemy infrastructure, where automation of information collection has become fragmented due to the multitude of sensors used in automation of retaliation, especially through the use of "smart" mines capable of determining whether they should explode near a particular vehicle[19]. All these definitions introduce us to the real-virtual world of cyber warfare, the one that would transform all the other fields that are directly or indirectly assimilated to war, to polemology.

2. Updating the Traditional War and Extending It to Cyberspace

For practical purposes, in order to be able to highlight different situations in the information space, we need some distinctive elements that differentiate between hostile cyber operations that support military operations in theatres of operations and hybrid threats.

In this sense, we have the cyber-attacks in the ex-Soviet states which, through their mode of action, have set precedents in the field of (inter) national security. As a first example, the 2007 cyber-attacks on Estonia included botnet attacks by zombie computers. For three weeks, the hackers targeted the country's digital infrastructure, regardless of the level of users, public or private. Distributed Denial of Service (DDOS)[20] attacks have caused the collapse of services of all kinds, starting with online banking, multimedia or e-government services, implemented using digital tools built on algorithms, which, in turn, were transformed into platforms that included artificial intelligence. The problems arose during a political dispute between the Russian state and Estonia, over the relocation of the Bronze Soldier monument on April 26; pro-Russian demonstrations had locally intensified, warnings were also received from the Kremlin, and the next day, for three weeks, the

[16] ***, *Legea nr. 192 din 25 octombrie 2019 pentru modificarea şi completarea unor acte normative din domeniul ordinii şi siguranţei publice*, Monitorul Oficial, No. 868, 28.10.2019, p. 14.
[17] Jacob G. Oakley, *Waging Cyber War. Technical Challenges and Operational Constraints*, *Apress Publications*, New York, USA, 2019, p. 8.
[18] *Ibidem*, p. 20.
[19] Joseph Henrotin, *The Art of war in the network age. Back to the future*, John Wiley & Sons, Inc. Publications, New Jersey, USA; 2016, p. 5.1.
[20] Scott Augenbaum, *The Secret to Cybersecurity. A Simple Plan to Protect Your Family and Business from Cybercrime*, Forefront Books, New York, USA, 2019, kindle e-book, p. 34.

country was effectively blocked[21]. Then, Estonia was followed by a wave of similar cyber-attacks in other former Soviet states. They integrated and synchronized cyber activity with classic actions to defend automated systems and included unique measures, algorithms in virtual space, in physical space−drones or other types of military equipment with unmanned autonomous systems, as well as other cyber capabilities; economic and diplomatic pressure was no exception[22]. The result was an increase in strategic effects in Lithuania (June 2008) and Kyrgyzstan (January 2009)[23]; The five-day Russian-Georgian war with integrative coordination, started with cyber-attacks launched by Russia on July 29, 2008[24] and intensified by military operations on 8 August 2008.

All these attacks could be compared with simple exercises compared to the Russian-Ukrainian War from 2014, following which the Russian Federation had annexed the Crimean Peninsula. This type of armed conflict has set a precedent in proving that international treaties, conventions and protocols on IHLs are outdated, that hybrid warfare incorporates different modes of warfare conducted through conventional strategies, tactics and means integrating irregular formations, terrorist acts and crimes, including violence and coercion, without distinguishing between civilians and combatants.

Russia is the first internationally recognized state to have resorted directly to the use of hybrid warfare, the spread of the conflict in Eastern Ukraine has only proved that Russia had all the means to implement its art, it could cover the whole the chain of cause and effect in the theatre of war or conflict operations with minimal material resources, no physical weapons and no loss of life, especially for the attacking party[25]. "Hybrid warfare is a mirror of the world we live in, a reflection of the society that leads it; therefore, a hybrid society will engage in hybrid warfare"[26].

3. Hostile Cyber Actions and Political-Diplomatic Retaliation, Limits to War and International Humanitarian Law

In the contemporary international system, the main rule governing the use of force in international law is the Charter of the United Nations (UN). Its legal basis

[21] Damien McGuinness, "*How a cyber attack transformed Estonia*", *BBC*, 27.04.2017, URL: www.bbc.com/news/3965541, accessed on 03 June 2020.
[22] David E. Sanger, *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age*, Crown Publishing Group, a division of Penguin Random House LLC, New York, USA, 2018, pp. xv-xvi.
[23] *Ibidem.*
[24] *Ibidem.*
[25] Brin Najžer, *The Hybrid Age: International Security in the Era of Hybrid Warfare*, I.B. Tauris Bloomsbury Publishing, London, 2020, p. 27.
[26] *Ibidem.*

is mentioned in Article 2, paragraph 4 of the UN Charter as follows: "All members shall refrain from the threat or use of force in their international relations, either against the territorial integrity or political independence of any other State or in any manner inconsistent with the objectives of the United Nations"[27].

The UN Charter also provides for the legitimate personal and collective self-defence of the State in Article 51: "Nothing in this Charter shall affect the inherent right of individual or collective defence in the event of an armed attack on a member of the United Nations until the Security Council has taken the necessary measures to maintain international peace and security. Measures taken by members not to exercise this right of self-defence shall be notified immediately to the Security Council and shall in no way affect the power and duty of the Security Council in this Charter to take such measures as it deems necessary to maintain or restore. This one. international peace and security"[28].

The main problem for our topic, which derives from this article of the Charter, is that the existing international norms are evasive, they cannot be applied effectively in the information space. Declarations of war, communiqués and diplomatic positions are put to the test in the conditions in which the parties involved in the hybrid war are no longer just the states, the primary subject of public international law.

We do not have legal criteria that can be applied to hybrid and hostile actions in cyberspace when they are carried out by the state directly or through a proxy and if these actions can be classified as an armed conflict between the state and its opponent. The hybridization of the war demonstrated in 2014 that the new military instruments can avoid the international norms signed by the 40 international conventions and protocols on IHL, the right to wage war, *jus ad bellum* or the rules to be observed during the war, *jus in bello.*

Jus ad bellum is a generic aspect in the legal analysis of cyber operations that can be performed by the armed forces. The activities carried out in cyberspace allow the state to carry out operations with lethal or harmful results in addition to those that do not use force but they can cause death, injury, material damage. Taken separately or as a whole, these types of actions can be considered armed attacks or the use of force in accordance with international law because the relevant states and Intergovernmental Organizations (OIGs) have included cybercrime in the legislative framework. This highlights a wide range of ways of breaking the law. Among them we find all kinds of attacks on private or public persons, operators and institutions. Some of the crimes are universally accepted, others are interpreted at the national

[27] ***, *CARTA NAŢIUNILOR UNITE*) din 26 iunie 1945, publicat în Monitorul Oficial din 26 iunie 1945,* p. 2, URL: http://www.anr.gov.ro/docs/legislatie/internationala/Carta_Organizatiei_Natiunilor_Unite_ONU_.pdf, accessed on 03.06.2020.
[28] *Ibidem*, p. 10.

level. For universally defined cross-border cybercrime we find[29]:

a) new type of crime, caused online (identity theft, financial or card payment data; theft and sale of corporate data, blackmail, etc.) on social networks, e-mail and the Internet;

b) conventional but reinterpreted crime, such as scams, social engineering; illegal trafficking of all kinds; money laundering, cyber harassment, incitement to hatred, etc.

The two types of crime are completed by those related to the protection of national security, where the definitions may be similar, but they are interpreted in terms of its citizens' nation, rights and obligations. More specifically, the heroes of one country can be enemies of another, regardless of the space in which they carry out their actions. Among these actions, at national legislative level, we have provisions in the Criminal Code of Romania, in the chapter Crimes against national security (art. 394-412)[30]: high treason, treason by transmitting state secret information and aiding the enemy; actions against the constitutional order and hostile actions against the state, espionage, attacks, in particular, of the one who endangers national security; diversion, communication of false information, propaganda, complicity, concealment of information regarding possible betrayal or hostile act, organization of espionage networks, etc. The espionage activity is codified in the international system in The Hague Regulations (1899 and 1907), the Fourth Geneva Convention (1949) and in Additional Act I (1977) of the Geneva Conventions.

In this case, cyber espionage can produce effects proportional to the aims and targets of these types of actions. They can affect relevant states, organizations and individuals, from simple password-breaking of emails belonging to public figures to material damage in real life or actual loss of life[31]. "Criminality in cyberspace"[32] (Cybercrime) has begun to be taken seriously at regional level through firm action. One of the first at European Union level is "Council Decision (CFSP) 2020/1127 of 30 July 2020 concerning restrictive measures against cyber-attacks threatening the Union or its Member States".

Extrapolating this idea, we have actions that can extend from the real environment to the virtual one, provoking rapid political-diplomatic, military, defence or attack reactions. Some may include all the possibilities for reaction in a state. This reaction represents the right of self-defence in the cyberspace of state

[29] David B. Skillicorn, *Cyberspace, Data Analytics, and Policing,* CRC Press, Boca Raton, Taylor & Francis Group, LLC, Boca Raton, Florida, 2021, pp. 15-16.

[30] *** *Codul Penal al României,* published in Monitorul Oficial of României, 1st Part, No. 575, 25 June 2004, pp. 876-879.

[31] Scott Augenbaum, *op. cit*., p. 35

[32] ***, *Convenția privind criminalitatea informatică din 23.11.2001 *) (Convenția de la Budapesta - 2001),* publicată în:Monitorul Oficial, Partea I nr. 343 20.04.2004, p. 1.

entities against interference. The types of attacks diversified, the mercenaries entered the information space, being known as hackers and differing, metaphorically, by several colours, after, initially, they were classified into three categories: white hats; grey hats; black hats (white, grey or black hats), these colour codes progressively expressing the degree of legality of activities in cyberspace, from legal (white) to illegal (black). In the IHL, the mercenaries are provided in the Protocol of 1977, art. 47, as follows: "Mercenaries are people specially recruited in the country or abroad to fight in an armed conflict; they take part directly in hostilities in order to obtain a personal advantage and which is actually promised by or on behalf of the party to the conflict, a remuneration higher than that promised or paid to the contingents of regular armies, having a similar rank and function in the armed forces of this part; and they are not members of the military forces of a party to the conflict"[33]. From time to time, we are informed by the media that various members of the diplomatic, consular or administrative bodies of some embassies are accused of espionage[34], we consider it appropriate to explain the generic term spy. In turn, it is assimilated with the intelligence activity in the information environment, that of cyber espionage. Their traditional status has been detailed in The Hague Conventions. This is explained in the articles 27-29 of Conventions II (1899) and IV (1907), in art. 29, 30 and 31 of Convention VI (1907), based on the identification of a person as a spy: "a belligerent state with the intention of communicating them to the opposing party"[35]. The clandestineness, the false pretext, the intention to communicate the accumulated information to the enemy party are found in their actions carried out at the limit (i) of legality.

Spies, mercenaries, diversionists and saboteurs are just a click away, the current threats and armed (hybrid) conflicts fall under the spectre of theft, misinformation, false information or unauthorized access to another state's network systems. Then, such actions can be protected according to The Hague Protocols. However, mercenaries and cyber espionage operations go beyond the provisions of legal acts and/or customs of international law, because they involve interference by

[33] ***, *Protocolul adiţional I la convenţiile de la Geneva 1949, adoptat la Geneva în 1977, cu privire la protecţia victimelor de război în conflictele armate internaţionale,* URL: https://lege5.ro/Gratuit/he3daojy/protocolul-nr-1-1977-aditional-la-conventiile-de-la-geneva-din-12-august-1949-privind-protectia-victimelor-conflictelor-armate-internationale, accessed on 03.06.2021.

[34] A.N.: One of the recent examples is a flagrant organized in March, in which an Italian Navy officer was involved while handed secret documents to the Russian military attaché. Source: *Italian officer 'caught selling secrets to Russia',* 31.03.2021, URL: https://www.bbc.com/news/world-europe-56588506?fbclid=IwAR3R2Whyuzk8rQaskWaBvUxdJv5rMIgj_BxQF2t419G5cGUATNw3jdbAjto, accessed on 21.10.2021.

[35] James Brown Scott, *The Hague conventions and declarations of 1899 and 1907, accompanied by tables of signatures, ratifications and adhesions of the various powers, and texts of reservations*, New York Oxford University Press American Branch, Toronto, Canada, 1915, p. 118.

state or non-state actors in the systems of another state and violate the principle of non-intervention in art. 2, paragraph 7 of the UN Charter. It prohibits states from interfering in the internal affairs of other states, and victim states can protest against these actions by reporting them to the UN Security Council, but in reality, this is not the case. Leon Panetta, former secretary of the US Department of Defense, affirms that: "We have seen first-hand how modern vehicles such as remote platforms and cyber systems have changed the way wars are conducted. They give our soldiers the ability to face the enemy and change the course of war, even if they are far away. On the right side of the cyberspace spectrum there is the use of force or armed attack in cyber operations. Pentagon officials expressly say cyber-attacks on US will be seen as a war action"[36]. Extensive actions in cyberspace directly affect international norms that provide for the right to life. Recognized worldwide by accepting the points set out in the 1948 Universal Declaration of Human Rights and in accordance with article 51 of the UN Charter, within the scope of the Geneva Conventions and their Additional Protocols. In Additional Protocol I of Geneva Conventions we find rules that can adapt the information space because here we have non-international armed conflicts without technical specifications. In this area, actions in cyberspace can be integrated into this protocol through the wide range of physical damage or death/damage to the environment, only the new environment also involves the online environment, where the impact of cyber operations can have similar results to the effects produced in following traditional military actions.

The Tallinn Handbook on International Law Applicable to Cyber Warfare describes a similar situation for *jus ad bellum* for cyberspace, which shows that cyber infrastructures in their own countries are part of national infrastructure and that any attack on it is illegal[37], regardless of the level reached by this attack. However, not all cyber-attacks can be categorized as an armed attack that can activate self-defence structures. However, the effects of a cyber-armed attack may be equivalent to those that would result from an action qualifying as a traditional armed attack[38]; therefore, armed cyber-attacks are based on cyber-attacks, from simple incursions into private/individual information systems to unique cyber actions to achieve national security objectives against other states that give states the right to self-defence provided they respect IHL, by default, the four Geneva Conventions signed in August 1949, and their two Additional Protocols signed in 1977. The advantage of these Conventions and their Additional Protocols is that, after signing, ratifying

[36] Jennifer, Wang, *The White House and Pentagon Deem Cyber-Attacks, An Act of War, Forbes*, URL: http://www.forbes.com/sites/reuvencohen/2012/06/05/the-white-house-and-pentagon-deem-cyber-attacks-an-actof-war/, accessed on 03.06.2021.
[37] Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations,* Cambridge University Press, Cambridge, 2017, p. 15.
[38] *Ibidem*, p. 54.

and acceding to these rules, the Conventions were universally accepted. For example, Additional Protocol I has been accepted by 200 states[39] (UN has 193 state members). Becoming fundamental legal documents, the Geneva Conventions and their Additional Protocols govern armed conflicts between states, thus developing the IHL principles of armed conflict. IHL represents "the set of rules of international law, of customary or conventional origin, intended for the purpose of specifically regulating problems arising in situations of international and non-international armed conflict"[40], with two basic branches[41]:

a) The law of armed conflict (the Law of War), and

b) International Humanitarian Law (Humanitarian Law).

The 1977 Additional Protocols to the Geneva Conventions were imposed by the impact of innovations in weapons technologies and changes in the way wars are conducted, representing an adaptation of the conventions and the previous protocol to technological innovations and changes in the war of the twentieth century. The Second Additional Protocol is the first international document in which they are described without being named directly, the situations in which civilians involved in (inter)national conflicts and asymmetric combat structures can be found in which the area of applicability is specified, then we have clearly specified in Article 4 and acts of terrorism[42].

The armed attack has many valences. According to art. 49 of Additional Protocol I, "the expression attacks means acts of violence against the adversary, whether these acts are offensive or defensive"[43]. These involve violent actions taken at individual, group or (inter)national level to achieve specific objectives. The attack has two traditional forms in the field of polemology, the international armed attack and the national one, specifically in civil wars. They were joined by non-state actors, such as international organizations or other individual actors or organized in various entities with power and influence in the international arena.

In the case of international armed conflict between two or more states, the Geneva Conventions apply, in the armed conflict in the national space between a state and an organized armed group we have the possibility to monitor the extent to which the parties are respected and whether they respect civilians and goods; we also have the third joint article of the Geneva Convention[44]. Regardless of how

[39] ***, *Geneva Conventions of 1949 and Additional Protocols, and their Commentaries, By State*, URL: https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/vwTreatiesByCountry.xsp, accessed on 27.10.2021.

[40] Anatolie Bulgac, Sergiu Sîrbu, *Drept Internaţional Umanitar (Ghid)*, Centrul Editorial-Poligrafic Medicina, Chişinău, 2019, p. 8.

[41] Anatolie Bulgac, Sergiu Sîrbu, *op.cit.*, pp. 8-9.

[42] ***, *Protocolul nr. 2/1977 adiţional, op.cit.*, pp. 24-25.

[43] ***, *Protocolul nr. 1/1977 adiţional, op.cit.*, p. 24.

[44] Anatolie Bulgac, Sergiu Sîrbu, *op.cit.* pp. 8-12.

armed conflict is characterized, methods of conflict must comply with the law of armed conflict[45].

Cyber actions are used as versatile tools in armed conflict, through which attacks can reach the level of armed attacks in *jus in bello*, which can cause disruptions between the land, sea, air and telecommunications forces with the related commands; to minimize trust in government and the state in general; to terrorize the civilian population and to come to the aid of traditional military campaigns. Such situations have challenged states to make important decisions. They have started to set up cyber divisions. For example, the terrorist attacks of September 11, 2001 in the USA produced many changes, among them the creation of the first cyber division within the Federal Bureau of Investigation[46].

The IHL offers the possibility of harmonizing laws on current issues posed by hostile actions in cyberspace because most countries in the world are signatories to The Hague Conventions and Regulations, the Geneva Conventions and their Additional Protocols. Actions in the virtual space are cross-border, undertaken globally in proportion to the level of IHL acceptance in all natural spaces. Thus, the three principles of the IHL can be extended, because: we need proportionality in the choice of means, methods and numbers in war; to discriminate between civilians and combatants, between civilian and military structures; in order to avoid human suffering and material destruction[47]. These principles are assumed through humanity, impartiality, neutrality, independence, volunteering, unity and universality[48]; all the more so since, in the information age, we need a system attesting the legitimacy of freedoms in cyberspace, paraphrasing John Stuart Mill, where the freedom of one state ends on the Internet, that is where the freedom of the other begins.

Conclusions

Throughout this article we delineated the definitions of work related to diplomacy, war, cyberspace and IHL. We highlighted theoretical concepts through real examples from natural and virtual spaces in order to emphasize the need to correlate the IHL with hostile attacks and actions conducted in the information space, as a right of war valid in all spaces known to man.

We have developed ideas through which we notice that diplomacy implemented by information media has come to the attention of public opinion with the help of public diplomacy, when established formulas of communication on social networks

[45] *Ibidem.*
[46] Nancy E. Marion, Jason Twede, *An Encyclopedia of Digital Crime*, ABC-CLIO, LLC Publishers, Santa Barbara, California, USA, 2020, p. XXIII.
[47] *Ibidem*, p. 59.
[48] *Ibidem*, pp. 15-16.

on the Internet are used. This aspect is often integrated into similar concepts, such as digital diplomacy and cyber diplomacy, but regardless of the preferred term, the complex purpose of diplomacy (negotiation, representation, denial; building, maintaining and strengthening relations between states) remains unchanged, maintaining its validity in any known space. Diplomacy has the fundamental mission of finding peaceful solutions to bi- or multilateral relations through treaties and conventions. They may include adaptations of existing or new variants, caused by the popularization of new technologies and the resizing of the approach to war, from the classical war to that in cyberspace.

The implementation of innovative systems specific to the diplomatic environment is not exceptional. The idea of using technological tools is not new either. The truly unique fact is the spiral acceptance of the set of successive transformations in the institutional and inter-ministerial environment of foreign affairs in all the states of the world; they began to bring new working techniques simultaneously. The complexity and volatility of the information environment are brought into congruence with the packages of international norms hardly accepted by international actors during the twentieth century and of diplomatic customs hundreds of years old and with thousands of years of armed conflict. Under these conditions, the war became informational and/or cyber. In the related space, the parties involved are no longer just state, private or individual actors. Here it is necessary to include new amendments in the IHL, which should be accepted by all stakeholders, state or non-state actors, private or individual; to include the legislation of tandem military practices: humans and robots, automated equipment and computerized military equipment.

The analysis of the cyber war transposed through the prism of the IHL, the Four Geneva Conventions and the Two Additional Protocols of these Conventions leads to the conclusion that the rules underlying the organization of military operations are adaptable to the cyber conflict. For this area as well as to negotiate new international normative acts, we need specialized people. But, reducing these aspects to generic terms, we already have them in the attributions of diplomats, they just have to adapt their skills to the requirements of the information age.

Therefore, the objective and hypothesis of this study are confirmed. Digital diplomacy can be a driver for innovative approaches to war law. Negotiations belong to diplomats, just as declarations of war and peace also belong to diplomacy. When diplomacy entered the information age, it also expanded its responsibilities proportionally, implicitly for the negotiations regarding the extension of the IHL for the situations produced in cyberspace. Thus, the power of material and human destruction is a click away. This fact is becoming a requirement to quickly adjust current IHL conventions to possible strategic paradigms regarding the preparation and conduct of military or hostile operations of individuals or states, all behind a computer monitor.

BIBLIOGRAPHY:

1. ***, *Carta Națiunilor Unite*, published in Monitorul Oficial from 26.06.1945.

2. ***, *Codul Penal al României*, published in Monitorul Oficial of Romania, Part 1, no. 575, 25.06.2004.

3. ***, *Comunicare Comună către Parlamentul European, Consiliul European, Consiliu, Comitetul Economic și Social European și Comitetul Regiunilor din 5 decembrie 2018, Plan de acțiune împotriva dezinformării*, URL: https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:52018JC0036&from=R

4. ***, *Convenția (de la Geneva privitoare la Protecția persoanelor civile în timp de război din 12 august 1949 (IV),* URL: https://crucearosie.ro/assets/Uploads/Conventia-de-la-Geneva-IV.pdf

5. ***, *Geneva Conventions of 1949 and Additional Protocols, and their Commentaries, By State*, URL: https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/vwTreatiesByCountry.xsp

6. ***, *Strategia de securitate cibernetică a României*, URL: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/roncss.pdf

7. ***, *Convenția privind criminalitatea informatică din 23.11.2001*) (Convenția de la Budapesta - 2001)*, published in Monitorul Oficial, Part I no. 343, 20.04.2004.

8. ***, *Legea nr. 192 din 25 octombrie 2019 pentru modificarea şi completarea unor acte normative din domeniul ordinii şi siguranţei publice,* published in Monitorul Oficial no. 868 from 28 October 2019.

9. ***, *Strategia Națională de Apărare a Țării pentru perioada 2020-2024. „Împreună, pentru o Românie sigură şi prosperă într-o lume marcată de noi provocări"*, Monitorul Oficial, Part I, No. 574 from 01.07.2020.

10. ***, *Protocolul adiţional I la convenţiile de la Geneva 1949, adoptat la Geneva în 1977, cu privire la protecţia victimelor de război în conflictele armate internaţionale*, URL: https://lege5.ro/Gratuit/he3daojy/protocolul-nr-1-1977-aditional-la-conventiile-de-la-geneva-din-12-august-1949-privind-protectia-victimelor-conflictelor-armate-internationale

11. ***, *Protocolul nr. 2/1977 adiţional la convenţiile de la Geneva din 12 august 1949 privind protecţia victimelor conflictelor armate fără caracter internaţional*)*, URL: https://lege5.ro/gratuit/he3daojz/protocolul-nr-2-1977-aditional-la-conventiile-de-la-geneva-din-12-august-1949-privind-protectia-victimelor-conflictelor-armate-fara-caracter-international

12. AUGENBAUM, Scott, *The Secret to Cybersecurity. A Simple Plan to Protect Your Family and Business from Cybercrime*, Forefront Books, New York, USA, 2019.

13. BARRINHA., André; RENARD, Thomas, "Cyber-diplomacy: the making of an international society in the digital age", *Revue Global Affairs*, No. 3:4-5, 2017, URL: https://doi.org/10.1080/23340460.2017.1414924

14. BJOLA, Corneliu; HOLMES, Markus; *Digital Diplomacy: Theory and Practice*, Routledge New Diplomacy Studies, Abington, UK, 2015.

15. BJOLA, Corneliu; KORNPROBST, Markus; *Understanding International Diplomacy Theory, Practice and Ethics*, Second Edition, Routledge, Abington, Oxon, UK, 2018.

16. BENDIEK, Annegret; KETTERMAN, Matthias C., *A revising the EU Cybersecurity Strategy: A call for EU Cyber Diplomacy*, SWP Comment, No. 16, 16.02.2021, URL: https://www.swp-berlin.org/publications/products/comments/2021C16_EUCyberDiplomacy.pdf

17. BULGAC, Anatolie; SÎRBU, Sergiu, *Drept Internaţional Umanitar (Ghid),* Centrul Editorial-Poligrafic Medicina, Chișinău, 2019.

18. DeCUSSY; Ferdinand, *Dictionnaire ou manuele-lexique du diplomate et du consul*, Tipographie de F. A. Brockhaus, Leipzig, 1846.

19. DJUVARA, Marcel T., *Metoda inductivă și rolul ei în ştiinţele explicative,* Noua Tipografie Profesională Dimitrie C. Ionescu Publishing, Bucharest, 1910.

20. GROOM, A.J.R.; BARINHA; André; OLSON, William, *International Relations Then and Now Origins and Trends in Interpretation*, Second Edition, Routledge, Taylor & Francis Group, New York, USA, 2019.

21. HENROTIN, Joseph, *The Art of war in the network age. Back to the future,* John Wiley & Sons, Inc. Publications, New Jersey, USA, 2016.

22. HOCKING, Brian; MELISSEN, Jan; *Diplomacy in the Digital Age.* Clingendael Report, Netherlands Institute of International Relations, Clingendael, Netherlands, 2015.

23. KURBALIJA, Jovan, *An introduction to internet governance*, Published by DiploFoundation, Geneva, Switzerland, 2016.

24. McGUINESS, Damien, *How a cyber-attack transformed Estonia*, 27.04.2017, URL: www.bbc.com/news/3965541

25. MALIȚA, Mircea, *Diplomaţia. Şcoli şi Instituţii*, II[nd] Edition, Editura Didactică și Pedagogică, Bucharest, 1975.

26. MANOR, Ilan, *The Digitalization of Public Diplomacy*, Palgrave Macmillan Publishers, Basingstoke, UK, 2019.

27. MARION, Nancy E.; TWEDE, Jason, *An Encyclopedia of Digital Crime*, ABC-Clio, LLC Publishers, Santa Barbara, California, USA, 2020.

28. NAJZER, Brin, *The Hybrid Age: International Security in the Era of Hybrid Warfare*, I.B. Tauris Bloomsbury Publishing, London, 2020.

29. OAKLEY, Jacob G., *Waging Cyber War. Technical Challenges and Operational Constraints,* Apress Publications, New York, USA, 2019.

30. PRITCHARD, Adam C.; THOMSON, Robert B, *Securities Law and the New Deal Justices*, URL: https://repository.law.umich.edu/cgi/viewcontent.cgi?article=2552&context =articles

31. RIORDAN, Shaun, *Cyberdiplomacy, Managing security and governance online,* Policy Press Publishing, Cambridge, UK, 2019.

32. SANGER, David E., *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age*, Crown Publishing Group, a division of Penguin Random House LLC, New York, USA, 2018.

33. SKILLICORN, David B., *Cyberspace, Data Analytics, and Policing*, CRC Press, Boca Raton, Taylor & Francis Group, LLC, Boca Raton, Florida, 2021.

34. SCHMITT, Michael N., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations,* Cambridge University Press, Cambridge, 2017.

35. SCOTT, James Brown, *The Hague conventions and declarations of 1899 and 1907, accompanied by tables of signatures, ratifications and adhesions of the various powers, and texts of reservations*, New York Oxford University Press American Branch, Toronto, Canada,1915.

36. WANG, Jennifer, *The White House and Pentagon Deem Cyber-Attacks, An Act of War*, URL: http://www.forbes.com/sites/reuvencohen/2012/06/05/the-white-house-and-pentagon-deem-cyber-attacks-an-actof-war/