The Challenges raised by the application of International Humanitarian Law to Information Warfare

Glasgow Student Number: 2567058K

Trento Student Number: 225062

Charles Student Number: 79452457

Presented in partial fulfilment of the requirements for the Degree of

International Master in Security, Intelligence and Strategic Studies (2020-2022)

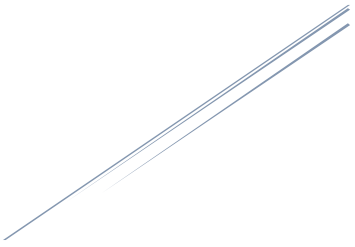
Word Count: 21 212

Supervisor: Professor Marco Pertile

Date of Submission: 10/08/2022

'We must remember that in time of war what is said on the enemy's side of the front is always propaganda, and what is said on our side of the front is truth and righteousness, the cause of humanity and a crusade for peace.'

- Walter Lippmann, American writer,



Abstract

In wartime, information is essential and decisive for the conduct of hostilities. It is the foundational element of intelligence, the basis of the war narrative galvanising the society but also, a weapon. International humanitarian law acknowledged the strategic importance of information, regulating the involvement of spy and journalists in armed conflicts. Information has gained an increasing place in the military strategy and in the academic debates because of various factors, including the development of new information technologies, the emergence of the phenomenon of 'information warfare', the growing interest of the political analysts for 'hybrid warfare' after the Crimean crisis in 2013 and the sociological context of 'post-truth'. In a context of ever-changing technological environment, the application of the current international humanitarian legal framework to information warfare is full of challenges and raises unanswered questions. Hence, this dissertation aims at answering the following question: how do the specificities of contemporary information warfare challenge the application of international humanitarian law? This question is particularly relevant now for several reasons. First, one has gained hindsight on marking events of information operations, including the attack on the radio and television tower in Serbia in 1999, and the entry into the digital age during the Second Lebanon war, specifically with numerically modified imagery. Second, one can now appreciate the evolution of information warfare practices with new information and communication technologies, illustrated by the Russo-Georgian war and the Russo-Ukrainian war, and the growing use of disinformation, deep fakes and other techniques manipulating information. This master's thesis will analyse the applicable rules to information warfare and the problems related to the application to the relevant conducts identified in several case studies before examining the opportunities and challenges of regulation.

Keywords: armed conflicts, international humanitarian law, information and communications technologies, information operations, information warfare, media.

Acknowledgements

I would first like to express my gratitude to my thesis supervisor Prof. Marco Pertile of the School for International Studies at the University of Trento. He remained patient throughout my long process for settling upon a final topic and steered me in the right the direction whenever he thought I needed it.

I would also like to thank my superiors and colleagues at Universal Rights Group. Despite the great workload we endured for the 50e session of the Human Rights Council, they were always sympathetic and accommodating for me to succeed and gave me great opportunities to work on topics related to this thesis.

I would also like to acknowledge Ms Beatrice Godefroy from the Centre for Civilians in Conflict, who took the time to exchange views with me.

I must express my very profound gratitude to my parents and my sister for providing me with unfailing support and patience throughout this challenging year. Finally, this accomplishment would not have been possible without the continuous encouragement of my classmates and friends, their precious advice and attempts to answer my metaphysical questions and doubts late at night.

Thank you.

Table of contents

Introduction

In 1943, the MI5-led Operation Mincemeat enabled the invasion of Sicily by the Allies. This deception operation relied on the fabrication of a scenario displaying a dead officer, with fake British correspondence to mislead the Axis force on the Allies' military strategy in the Mediterranean Sea.[1] The British military intelligence decrypted German messages showing that the Axis forces fell for the ruse. This operation gave an undeniable military advantage to the Allies, who successfully invaded Sicily on 9 July 1943, and eventually won World War II. This is an example of the use of information as a strategic military tool. It shows how decisive and essential information can be in wartime. Information is the heart of intelligence and is fundamental for military decision-making. Indeed, the military strategy relies on available information so the conflict parties seek for the best knowledge of the situation to take advantage of it. Already in the 19th century, von Clausewitz coined the concept of 'fog of war' to refer to the uncertainty of combatants regarding their adversaries and their capability.[2] Reducing this uncertainty is essential for the military, making information and intelligence even more important for the military strategy. The chaotic information environment exacerbates this uncertainty of situational awareness.

International humanitarian law acknowledged the strategic importance of information in 1907 with the Hague Convention. Articles 29 and 31 provide a definition of a spy and its status under international humanitarian law as part of the regulation of people working for the collection and the circulation of information. These two articles specifically regulate the conduct of persons acting clandestinely or on false pretences to obtain information in the zone of hostilities, with the intention of communicating it to the hostile party.[3] Similarly, international humanitarian law seeks to protect people who enable information

[1] Ben Macintyre. Operation Mincemeat: The True Spy Story that Changed the Course of World War II. London: Bloomsbury. (2010).
[2] von Clausewitz, C. *Vom Kriege*, Book 1, Chapter 3. « Nebel des Krieges". (1832).
[3] Convention (IV) respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land. The Hague. Annex to the Convention: Regulations respecting the laws and customs of war on land - Section II: Hostilities - Chapter II: Spies - Regulations: Art. 31. (1907).

to circulate among the military and the population. Even though the legal corpus distinguishes war correspondents and independent journalists, both benefit from a strong legal protection so they can investigate and report information from armed conflicts' battlefield. War correspondents is a legal category, which emerged from the practice in World War II and the Korean War.[4] It refers to accredited journalists, who are under the protection of the armed forces. Journalists should be considered as civilians and yet, they enjoy the status of prisoners of war if captured.[5] The protection of independent journalists falls into the scope of Article 79 of the First Additional Protocol as well, which ensure the protection of 'journalists engaged in dangerous professional missions in zones of armed conflict' within the meaning of Article 50 (1).[6] Thus, they enjoy the full scope of protection granted to civilians under international humanitarian law. Because of their essential role in documenting armed conflicts and holding parties accountable for violations, the United Nations Security Council adopted two resolutions in 2006 and 2015 as a response to intentional attacks against journalists while the United Nations Human Rights Council adopted a resolution on the safety of journalists in 2020.[7] In this resolution, member states underlined the crucial function of journalists and media workers in times of crisis, recognised the importance of the credibility of journalism, "in particular the challenges of maintaining media professionalism in an environment where new forms of media are constantly evolving and where targeted disinformation and smear campaigns to discredit the work of journalists are increasing", and the importance of the ability of investigative journalism to work without fear of reprisals. Most importantly, the resolution was the opportunity of member states

[4] Alexandre Balguygallois, « Protection des journalistes et des médias en période de conflit armé ». *International Review of the Red Cross*. Vol. 86, No. 853. (2004). pp. 37-68; https://casebook.icrc.org/case-study/protection-journalists.

[5] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts. Art. 79 (1977); Third Convention (III) relative to the Treatment of Prisoners of War. (1949). Art. 4 (a) para 4.

[6] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts. Art. 50(1) (1977).

[7] United Nations Security Council resolution 2222 (2015). *On protection of journalists and associated media personnel in armed conflict.* S/RES/2222; United Nations Security Council resolution 1738 (2006) S/RES/1738; Human Rights Council resolution 45/18 (2020) . *The safety of journalists*, A/HRC/RES/45/18.

to express serious concerns at attacks and violence against journalists and media workers in relation to their work in situations of armed conflict and to recall that

> "journalists and media workers engaged in dangerous professional missions in areas of armed conflict are civilians under international humanitarian law and shall be protected as such, provided that they take no action adversely affecting their status as civilians".

Although information has always been an important part of armed conflict strategy, it has gained an increasingly significant place in the strategy and in the academic debates with the development of new information technologies.[8] It is important to note that information warfare has always existed, with propaganda and war narratives, to demonise the adversaries and galvanise the population during armed conflicts. As such, the second Lebanon war is particularly interesting as the spark of the armed conflict was light up by a meticulous management of information. Hezbollah kidnapped two Israeli soldiers to proceed to negotiations to free some of their own prisoners. However, it was revealed later on that these kidnapped soldiers were dead from the capture, which constitutes a deceptive operation.[9] Information was used as part of the strategy as a support of military operations. However, a shift occurred with the development of new technologies. The narrative is important as influencing the adversary to erode social cohesion is now a goal of the strategy *per se*. The analyst Murray called this phenomenon the sixth military revolution, bringing buzzwords such as 'information warfare' or 'cyber war'.[10] In 1994, the US Congress created the Commission on the Roles and Capabilities of the US Intelligence Community, which defined information warfare as follows:

> "Information warfare" refers to activities undertaken by governments, groups, or individuals to gain electronic access to information systems in other countries either for the purpose of obtaining the data in such systems,

[8] Nunes, Paulo. "Impact of New Technologies in the Military Arena: Information Warfare." *Air Power.* Vol 2. No 2. (2007).
[9] France24. Echange de prisonniers entre Israël et le Hezbollah, *France24.* 16 July 2008 https://www.france24.com/fr/20080716-echange-prisonniers-entre-israel-le-hezbollah-liban-israel
[10] Williamson Murray, *America and the Future of War.* Standford: Hoover Institution Press. (2017). pp 47-49.

> manipulating or fabricating the data, or perhaps even bringing the systems down, as well as activities undertaken to protect against such activities."[11]

As information is political and the field evolves rapidly, definitions of 'information warfare' are relative to their context and complex to agree upon. However, one can agree that the term refers to information operations aiming at obtaining a decisive advantage in the information environment involving the battlespace use and management of information and communication technology.[12]

Although there are similarities between information warfare and cyberwarfare, both phenomena should be distinguished. Cyberwarfare has emerged with the invention of the internet, computers and related technological developments whereas information operations are an older practice with the use of the press or radio networks.[13] Cyberwarfare targets software and computers, using hacking, malware, viruses, while information warfare aims at demoralizing or manipulating the adversary or the public, using disinformation, propaganda, denial-of-service attacks on command and control systems, etc. Information warfare has a bigger scope as it covers the dissemination of information through different types of media, including non-digital ones. The analyst Janis Berzins talks about people's minds as the centre of gravity or the battlefield of information warfare.[14] Information warfare is closely linked to psychological warfare as it also aims at triggering a psychological reaction in the adversary's mind.

---

[11] George Curtis. *The Law of Cybercrimes and their investigations.* CRC Press, Taylor & Francis Group. (2012). p.27

[12] NATO. ″Information warfare″. Available at: https://bit.ly/3OTwHMc; Fecteau, M. (2019). 'Understanding Information Operations & Information Warfare'. *Global Security Review.* 7 January 2019. Updated on 22 June 2022.; Maria Luisa Nardi, 'Origin of Cyber Warfare and How the Espionage Changed: A historical Overview' in Luisa Dall'Acqua, Irene Maria Gironacci. *Transdisciplinary Perspectives on Risk Management and Cyber Intelligence.* (2020).

[13] Brunetti-Lihach, N. (2018). 'Information Warfare Past, Present, and Future'. *The Strategic Bridge*. November 14, 2018. https://thestrategybridge.org/the-bridge/2018/11/14/information-warfare-past-present-and-future.

[14] Janis Berzins. "Russia's New Generation Warfare in Ukraine: Implications for Defense Policy", Military Operations. Vol 2. No. 4. (2014). Available at: https://www.tjomo.com/article/47/Russias_New_Generation_Warfare_in_Ukraine_Implications_for_Defense_Policy/

As the Crimean crisis developed in 2013, the interest of analysts and scholars for information warfare was renewed with the growing topic of 'hybrid warfare' in the debates.[15] Indeed, looking at the occurrence of the search of 'hybrid warfare' in the news on the Internet, the term became increasingly searched after 2015 and mostly associated with the Russian Federation (See figure 1). In 2010, the North Atlantic Treaty Organisation (NATO) Supreme Allied Commander of Europe and the Supreme Allied Command Transformation Office defined this concept as a situation including 'adversaries with the ability to employ simultaneously conventional and non-conventional means adaptively in pursuit of their objectives'.[16] Information is one of the major tools of these non-conventional means of war.[17]

Today, information warfare takes place in a particular technological environment and sociological context. Although an old phenomenon, the development and the democratization of new and emerging technologies has changed the face of information warfare. It makes information immediate, widely spread and louder leading to an even more chaotic information environment, where reaction can be just as fast under the cover of anonymity. People are more likely to use cognitive shortcuts and confirmation bias.[18] Information is therefore omnipresent and inescapable in the daily life. Information technology is cheap and easily accessible making social malicious use of information even easier, slowly moving the battlefield to the internet. The interactions between politics and media have also evolved, leading to a post-truth politics era. This concept means that political leaders shape public opinion relying on emotions and personal belief, rather than objective facts.[19] In this context, hate speech and fake news are more numerous and less detectable, undermining one's ability to form an opinion.[20] This shift could be explained by

[15] Fridman, Ofer (2018) Russian 'Hybrid Warfare', Resurgence and Politicisation, Hurst & Co. p.106
[16] NATO (2010) BI-SC Input to a new NATO capstone concept for the military contribution to countering hybrid threats, 25th August 2010, p. 2
[17] *Ibid.*
[18] Herbert Lin "The existential threat from cyber-enabled information Warfare". Bulletin of the Atomic Scientists. Vol 75, No. 4 (2019). pp 187-196.
[19] Oxford's Learners Dictionary. "Post-Truth". Available at: https://www.oxfordlearnersdictionaries.com/definition/english/post-truth
[20] Vergely, B. (2019) « Vers des fakes de plus en plus nombreux et de moins en moins détectables : comment vivre à l'heure de la post-vérité ? » *Atlantico*, 6 janvier 2019.

the digital revolution and several factors, including the de-professionalization of journalism, the emergence of alternative media and the algorithms of search engines, which reduce the diversity of opinion and the critical spirit.[21] Next to this, the coronavirus has led to an 'infodemic'.[22] All these elements have accelerated the study of information. The reality of the battlefield is important only to the extent that it delimits what can be reasonably claimed.[23] The narrative has become an unescapable political element of the armed conflict and its outcome. The relationship between armed forces and mass media is complex. Indeed, mass media are essential to the military, and yet, the military must deal with both the search of transparency of media and the secrecy of the military apparatus and operations. This may conflict with mass media work, as they would tend to verify and trace the sources of information.[24]

As Captain Nunes rightfully noted "the real problem concerning the information warfare concept lies in the fact that we have a set of old concepts dressed in new clothing."[25] Indeed, in a context of ever-changing technological environment, the application of the current international humanitarian legal framework to information warfare is full of challenges and raises unanswered questions. Hence, this dissertation aims at answering the following question: how do the specificities of contemporary information warfare challenge the application of international humanitarian law? This question is particularly relevant now for several reasons. First, one has hindsight on marking events of information operations, including the attack on the radio and television tower in Serbia in 1999, and the entry into the digital age during the Second Lebanon war, specifically with numerically modified imagery. Second, one can now appreciate the evolution of information warfare practices with new information and communication technologies, illustrated by the Russo-Georgian war and the

---

[21] Viner, K. (2016) « Comment le numérique a ébranlé notre rapport à la vérité », *Courrier international*, 9 septembre 2016.
[22] World Health Organisation. "Infodemic". Available at: https://www.who.int/health-topics/infodemic#tab=tab_1
[23] Paul Goble. "Defining Victory and Defeat: The Information War between Russia and Georgia". in Svante Cornell & Frederick Starr. *The guns of August 2008: Russia's War in Georgia.* (Armonk, New York. 2009). p.195.
[24] Lorenza Fontana. "Hezbollah vs Israel: Confronting Information Strategies in the 2006 Lebanese War". *University of Glasgow.* (2010).
[25] Nunes, Paulo. "Impact of New Technologies in the Military Arena: Information Warfare." *Air Power.* Vol 2. No 2. (2007).

Russo-Ukrainian war, and the growing use of disinformation, deep fakes and other techniques manipulating information.

This master's thesis will analyse the applicable rules to information warfare and the problems related to their application to the relevant conducts identified in several case studies. The first part compares the confrontation of the traditional understanding of war, which is reflected in the established rules of international humanitarian law, with contemporary information warfare practices raising questions when it comes to the principle of distinction, the definition of an attack and the assessment of the damages (Part I). The second part explores how international humanitarian law covers some of the information warfare practices in the conduct of hostilities, notably the prohibition of perfidy and terror as well as incitement to violence (Part II). The third part questions the need for regulation and looks into the current debates on the diverse options for this regulation, as contemporary practices of information warfare become intrusive in the civilian sphere with large-scale consequences (Part III).

Chapter 1 - Literature Review

Cyberwarfare and information warfare should be distinguished. Although they both rely on intangible methods, they exploit different means and target different audiences as explained above. In 1995, Alvin and Heidi Toffler affirmed that a third wave in the military history was occurring, characterised by digitalisation and information technologies.[26] At the same period, some authors such as Professor Greenberg or Major Kushner, in the late 1990s and at the beginning of the 2000s, provided a valuable overview of legal challenges and constraints raised by information warfare. However, this part of literature is dated while technology has importantly evolved and so has information warfare.[27] The academic work mainly focused on the military strategy of the United States of America (US) when new actors of information warfare emerged in the past twenty years. Information and communication technologies

[26] Alvin and Heidi Toffler, *War and anti-War: Survival at the Dawn of the 21 st Century.* New York: Warner Books. (1995).
[27] Lawrence Greenberg. Information Warfare and International Law. *National Defense University Press*. (1998); Karl Kushner. "Legal and Practical Constraints on Information Warfare" *The United States Naval War College*. (1996).

have not stopped evolving with the mainstreaming of the Internet and smart phones, the emergence of social media with fast and widespread possibilities of communication and the disruptive technologies of manipulation of information.

In 2008, NATO established the Cooperative Cyber Defence Centre of Excellence. It is an international military hub which was created to enhance the capability, cooperation and information sharing among NATO, its member states and partners in the field of cyber defence through research and consultation. The Centre notably published the Tallinn Manual on the International Law Applicable to Cyber Operations, created by an international group of experts.[28] The first version was published in 2013 and the second one in 2017 (this edition is referred as 'Tallinn Manual' afterwards). Although this manual is not legally binding, it is an influential document for legal experts and policy analysts, which is based on the practice of states, examining the rules of international law governing cyber incidents. Yet, Professor Sassòli also dedicates a whole chapter of his book on the application of international humanitarian law to cyber operations, where he gives his departing opinion on diverse points of the Tallinn Manual, such as the applicability of perfidy to cyber operations.[29] Other initiatives saw the light of day after the 2014 invasion of Crimea. This event was the momentum for new research on information warfare because of the growing academic and political interests for hybrid warfare.[30] The European Union is particularly active as many organisations were created to ensure an appropriate answer to growing disinformation, such as the 'EU Disinfo Lab', the project 'EU vs Disinfo' or 'Debunk.eu'.[31]

Russian literature on information warfare is rich and evolving. The 2008 Russo-Georgian war led the development of literature on information warfare,

[28] The group was led by Professor Michael N. Schmitt, chairman of the international law department at the United States Naval War College, for both the Tallinn Manual and the Tallinn Manual 2.0. Other members of the group included academics, militaries and jurists. The drafting process was observed by NATO Allied Command Transformation, the International Committee of the Red Cross and United States Cyber Command and peer-reviewed by thirteen international legal scholars.

[29] Marco Sassoli. *International Humanitarian Law: Rules, Controversies, and Solutions to Problems arising in warfare*. Edward Elgar Publising Limited. (2019).

[30] Fridman, Ofer (2018) Russian 'Hybrid Warfare', Resurgence and Politicisation, Hurst & Co. p.106.

[31] Disinfo.eu. 2019. *EU DisinfoLab.* Fastlane https://www.disinfo.eu/about-us/; East Strat Com Task Force. 2015. *EuvsDInsinfo.* https://euvsdisinfo.eu/about/ ; *Debunk.eu*. Delfi, Digital News. https://debunk.eu/about-debunk/;

especially the Russian perspectives on the topic. Information warfare encompasses electronic warfare, psychological operations, strategic communication and influence.[32] From 2013, Colonel Chekinov and Lieutenant Bogdanov coined the 'new-generation war' referring to a conflict, which 'will be dominated by information and psychological warfare that will seek to achieve superior control of troops and weapons and to depress opponents' armed forces personnel and population morally and psychologically. In the ongoing revolution in information technologies, information and psychological warfare will largely lay the groundwork for victory.'[33] Therefore, Russian scholars and strategists foresaw an indispensable and indivisible role for information in the military strategy. Western scholars defined 'hybrid warfare' such Russian tactics, i.e. the use of hard and soft tactics, including information control and manipulation, to dissimulate intent and to create uncertainty.[34] Despite the extensive use of 'hybrid warfare' by Western analysts and scholars with the unfolding Russo-Ukrainian war, Russian scholars and militaries seem not to have made use of the term 'new-generation war' since 2013, nor 'hybrid warfare'. The political analyst Thomas wrote that 'information warfare in the new conditions will be the starting point of every action now called the new-type of warfare (a hybrid war) in which broad use will be made of the mass media and, where feasible, the global computer networks (blogs, various social networks, and other resources)'.[35] The veracity of the information does not matter as long as there is quantity. The NATO Strategic Communication Centre of Excellence talks about the 'result of a synchronous execution of messaging'.[36] Despite the evolution of information as a component of war strategy, there is a strong belief that sole resources and kinetic capabilities are not sufficient for military victory, but it requires information military strategy to subvert adversaries in addition.

---

[32] Giles, K. (2011) "Information Troops – A Russian Cyber Command?" 3rd International Conference on Cyber Conflict.
[33] Colonel S. G. Chekinov (Res.), Lieutenant General S. A. Bogdanov (Ret.), "The Nature and Content of a New-Generation War," *Military Thought* (2013).
[34] Andrew Monaghan, "The 'War' in Russia's 'Hybrid Warfare". *Parameters 45*, no. 4 (2015) pp. 65–74.
[35] Timothy Thomas. Thinking like a Russian Officer: Basic Factors and Contemporary Thinking on the Nature of War. *Foreign Military Studies*. (2016).
[36] NATO StratCom of Excellence (2015) "Analysis of Russia's Information Campaigns against Ukraine".

The contributions of Professors Henning Lahmann and Robin Geiss on information warfare are particularly interesting. Indeed, they jointly wrote a paper on the application of the principle of distinction in the interconnected cyber space in 2012. Ten years later, their research specifically evolved towards information warfare as they published an article on the need to protect information space through law and advocate for a resilient Internet.[37] Similarly, Professor Goble wrote about the virtual war in the Russian military strategy in 1999, focusing on cyber operations.[38] Ten years later, he still analysed the Russian military strategy in the Russo-Georgian war, focusing on information warfare.[39] The International Review of the Red Cross has been extensively publishing on cyber operations and information technologies since 2012 notably with articles from Massimo Marelli, the head of the Data Protection Department of the International Committee of the Red Cross.[40] This two-step work by most authors shows the rapid evolution of technology and the warfare practices that accompany it. It reveals a slight shift of interest overtime from cyberwarfare to information warfare in the military and academic literature.

As mentioned above, the study of information is more important than ever because of its growing significance in the military strategy. The Russian literature emphasised this phenomenon under diverse name before NATO gets hold of the topic.[41] The richest body of literature analysing the application of international humanitarian law to information warfare dates from the 2000s.

---

[37] Waseem Qureshi. Information Warfare, International and the Changing Battlefield*", Fordham International Law Journal*. Vol 43. Issue 4. (2020); Robin Geiss, R & Henning Lahmann. "Protecting the global information space in times of armed conflict". *The Geneva Academy*. (2021); Fabio Rugge. "MindHacking": Information warfare in the cyber age". *Istituto per Gli Studi di Political Internazionale*. Analysis n°319. (2018)

[38] Goble, P. "Russia: Analysis from Washington—A Real Battle on the Virtual Front," *Radio Free Europe/Radio Liberty*. (1999).

[39] Goble, P. "Russia: Analysis from Washington—A Real Battle on the Virtual Front," *Radio Free Europe/Radio Liberty*. (1999); Paul Goble. "Defining Victory and Defeat: The Information War between Russia and Georgia". in Svante Cornell & Frederick Starr. *The guns of August 2008: Russia's War in Georgia.* (Armonk, New York. 2009).

[40] Massimo Marelli. "Hacking humanitarians: Defining the cyber perimeter and developing a cybersecurity strategy for international humanitarian organizations in digital transformation". *International Review of the Red Cross*. No. 913. (2021). Massimo Marelli, Adrian Perrig. "Hacking humanitarians: mapping the cyber environment and threat landscape" *Humanitarian Law & Policy.* International Committee of the Red Cross. (2020).

[40] Human Rights Council resolution 49/4. Situation of human rights in the Democratic People's Republic of Korea. A/HRC/49/L.4 (2022).

[41] (2010) BI-SC Input to a new NATO capstone concept for the military contribution to countering hybrid threats, 25th August 2010, p. 2

This subject significantly lacks update as means and methods of warfare have rapidly evolved. It also lacks overview as most of the work focuses on the US military strategy in the late 1990s and on the Russian strategy starting in 2008. It is therefore in this context that this essay attempts to insert itself. This dissertation aims at analysing the information warfare practices in conflicts between 1998 and 2022 in order to get a comprehensive grasp of trends and evolution of the means and methods. This thesis also seeks to provide an overview of the contemporary landmarks of information warfare by exploring a larger range of armed conflicts together, as detailed in the next section. Finally, the unfolding Russo-Ukrainian war reawakens the debate on regulation of information warfare. Hence, this dissertation is an opportunity to analyse if regulation is needed and where the international community stands today with the diverse options for regulation.

Chapter 2 - Research Design

Case studies

The research is conducted based on the practice of states in several case studies related to the use of information as part of the military strategy in international armed conflicts. They were selected based on the amount of available information and the recurrence of references to these conflicts in the literature on information warfare. The case studies are the following.

- The NATO attack on the Radio Television of Serbia headquarters, which occurred on the 23rd of April 1999 as part of the Kosovo war (1998-1999), is analysed. It is considered as the beginning of a new era for the military campaign, based on the understanding that communication strategies are an inevitable part of military ones.[42]
- The 2006 Lebanon war, or the Second Lebanon war, is often cited as a case study for information warfare and psychological

[42] Morand Fachot. The Media dimension in Foreign Interventions. *Options Politiques.* (2001).

warfare because of the widespread propaganda, the numerous attacks on media infrastructure and the manipulation of images.

- Several conducts in the Russo-Georgian war (2008) and from the Russo-Ukrainian war (2014-ongoing) are examined. The case study of the Russo-Ukrainian war is particularly important since it has led to the development of the concept of hybrid warfare, and thus, resulting to a growing interest for information warfare.

These case studies are international armed conflicts. The involvement of the Russian Federation caused yet many debates over the qualification of the latter conflict between 2014 and February 2022.[43] Regarding the 2006 Lebanon War, it opposed Israel and Hezbollah. But the question is to determine whether Hezbollah was controlled by the Lebanese government. The Appeals Chamber of the International Criminal Tribunal for the Former Yugoslavia established a criterion for the "overall control" in the case against Dusko Tadic.[44] This test aims at determining whether an armed force could be linked to the state in which they are located. If the state exercises a high level of control over the group, it would be an international conflict. The criterion is a 'degree of authority or control' over those armed units by organized and hierarchically structured groups. (§97) The control does not solely lie in equipping, financing, training and providing operational support to the group, but also in coordinating or helping in the general planning of its military or paramilitary activity. (§131, §137). As international humanitarian law seeks to determine whether it is a foreign involvement in an internal conflict, the rules of attribution of international law on state responsibility should be also considered. The case Military and Paramilitary Activities in and against Nicaragua of the International Court of Justice established an "effective control" test.[45] However, the Appeals Chamber found that this test is not adequate for acts of 'organized groups'. In its 2006 report, the Commission on Inquiry on Lebanon clarifies the nature of relationship between Hezbollah and the Lebanese government before

[43] RULAC. "International armed conflict in Ukraine". Available at: https://www.rulac.org/browse/conflicts/international-armed-conflict-in-ukraine
[44] *Prosecutor v. Duško Tadić a/k/a « Dule »*, ICTY-94-1. July 14, 1997.
[45] *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*, Jurisdiction and Admissibility, 1984 ICJ REP. 392 June 27, 1986. paras. 105–115.

concluding that Lebanon was party to the conflict for several reasons.[46] First, Hezbollah is a legally recognized political party. Second, 'the effective behaviour of Hezbollah in South Lebanon suggests an inferred link between the Government of Lebanon and Hezbollah in the latter's assumed role over the years as a resistance movement against Israel's occupation of Lebanese territory'. Hezbollah was a militia compensating the absence of the regular Lebanese Armed Forces in South Lebanon for the defence of the territory partly occupied. The report also noted that 'Hezbollah had also assumed *de facto* State authority and control in South Lebanon in non-full implementation of Security Council resolutions 1559 (2004) and 1680 (2006), which had urged the strict respect of the sovereignty, territorial integrity and unity of Lebanon under the sole and exclusive authority of the Government of Lebanon throughout the country.' Thirdly, the Lebanese state was the victim of direct hostilities conducted by Israel. Hence, according to this contextualisation, it seems that the results of overall control test would concur the report of Commission on Inquiry on Lebanon and thus, the 2006 Lebanon war involved Hezbollah, Lebanon and Israel as parties to the conflict.

This thesis explores the primary sources of international humanitarian law, as written in Article 38(1) of the International Justice Court statute, i.e. international treaties, customary international law and general principles recognized by civilized nations.[47] Treaties should be interpreted 'in accordance with the ordinary meaning to be given to the terms of the treaty in their context and in the light of its object and purpose.'[48] Customary international law derives from a long-standing and general practice accepted as law, evidence of which can be found in military manuals, case law, etc. Article 38(1)(d) specifically lists 'subsidiary means' for interpretation, including international jurisprudence, domestic jurisprudence, scholarly writings, which are frequently used to

[46] Human Rights Council, Report of Commission of Inquiry on Lebanon pursuant to Human Rights Council resolution S-2/1, A/HRC/3/2, 23 November 2006, available at http://www.ohchr.org/Documents/Publications/HR_in_armed_conflict.pdf

[47] Khan, I. 2019. "Article 38 of the Statute of the International Court of Justice: A Complete Reference Point for the Sources of International Law?" *The New Jurist.* 5 April 2019. https://newjurist.com/article-38-of-the-statute-of-the-international-court-of-justice.html

[48] Vienna convention on the law of treaties. Article 31. (1969)

understand international humanitarian law.[49] The Pictet Commentaries and the Commentaries to the Additional Protocols are considered authoritative by the International Criminal Tribunal for the former Yugoslavia.[50]

Methodology

This dissertation will analyse the practice of States with respect to the information warfare phenomenon and its interaction with international humanitarian law. This thesis aims at understanding how international humanitarian law applies to information warfare practice of states in armed conflicts and why, leading to a reflection on the effectiveness of this legal framework facing this particular form of warfare.

This dissertation provides an assessment of the elements of novelty in contemporary practice related to information warfare. Then, applicable rules and the problems related to their application are analysed in the light of established methods for treaty interpretation and for the assessment of customary law. First, the main theoretical features of information warfare are selected from the scholarship debate on the matter. Then, the analysis of secondary data, such as official governmental and NGOs reports and newspaper articles, on the history of the conflict and the current situation will enable to identify with more clarity the information warfare practices in the selected armed conflicts. Subsequently, diverse options to move the debate forward are examined, giving space to question the need and the type of regulation for information warfare.

Limits

Considering the development of the Russo-Ukrainian war since 2014, the debates around information have been reinforced as an underlying topic of hybrid warfare. Therefore, specific literature on information warfare and the Russo-Ukrainian war has increased, almost outshining the literature on other conflicts where information warfare was an important component.[51]

---

[49] Marco Sassoli. *International Humanitarian Law: Rules, Controversies, and Solutions to Problems arising in warfare*. Edward Elgar Publising Limited. (2019). p62-65.
[50] ICTY, The Prosecutor v. Tadić: A. Appeals Chamber, Jurisdiction, para 93
[51] Miranda Lupion. The Gray War of Our Time: Information Warfare and the Kremlin's Weaponization of Russian-Language Digital News, *The Journal of Slavic Military Studies*, Vol

The Russo-Ukrainian war serves as a case study for this master's thesis although it is an ongoing conflict. Its environment and related events change and unfold rapidly and are out of the control of the author. Current events make it difficult to study the conflict due to the lack of hindsight in the academic studies on the most recent developments and the distortion of information used by both parties. It is also difficult to find sources covering the period from 2014 to February 2022 as current events take up all a lot of room in the research findings.

The sources reviewed are from French and English language documents, i.e. not the official languages of any of the examined parties to the conflicts. Concerning the Russo-Ukrainian war, it should be noted that disinformation comes from both sides of the conflict. Therefore, the availability of information in English emanating from Russian or Ukrainian sources may have been translated for the purpose of disinformation or propaganda targeting a foreign audience. The challenge is to assess what legitimacy can be given to sources emanating from a conflict party seeing the sensitive role of information for this topic. Furthermore, the Russian Federation has conducted a silencing repression on all independent media within its territory.[52] It is therefore very likely that information emanating from a Russian media, located within the Russian Federation or self-proclaimed republics, lacks impartiality so sources should be always looked with particular scrutiny. Concerning the 2006 Lebanon war, it is difficult to access sources and documentation with a neutral perspective on the conflict or not one-sided for Israel. This could be explained by the fact that Hezbollah is an organisation listed as a terrorist organisation in many countries, which therefore restrict access to information emanating from this organisation.

Part I. Delineating the boundless possibilities of Information Warfare

31. No. 3. (2018) pp. 329-353.; Marie Baezner, Patrice Robin. « Cyber and information warfare in the Ukrainian conflict ». *Center for Security Studies.* (2018)*;* M, Jaintner. "Russian Information Warfare: Lessons from Ukraine" in Geers, K. (2015) *Cyber War in Perspective: Russian Agression against Ukraine*, NATO CCD COE Publications. (2015)

[52] Center for Strategic & International Studies (2022) "Russia's Crackdown on Independent Media and Access to Information Online". *Center for Strategic & International Studies.* March 30, 2022.

The traditional understanding of war, on which is based international humanitarian law is challenged by the nature of information warfare (A) pushing the boundaries of the protection granted by this legal corpus (B).

A. Confronting traditionally framed rules and Information Warfare

The confrontation of contemporary practices of information warfare and international humanitarian law raises many questions as this legal corpus was framed by an understanding of war based on traditional means and methods of warfare. It challenges the notions of the use of force and attack (i) and the assessment of damages (ii).

i. Challenging the Use of Force

The characterization of an attack is essential since it enables to define when an armed conflict arises and which legal corpus should be applied. Indeed, the use of force is regulated in different ways by international law. On the first hand, Article 51 of the United Nations Charter prohibits the use of force. Yet, a state is allowed to use force within its right to self-defence notifying the United Nations Security Council. Considering the nature of information operations, the definition of 'armed attack' is challenged. Could information be considered a weapon or an attack? When there is no lethal or physical destructive consequences, it has not been established that information attacks constitute an armed attack or the use of force under the United Nations Charter.[53] There is an increasing debate within the NATO member states when it comes to Article 5 of the founding treaty establishing the principle of collective defence.[54] Modifying 'armed attack' into 'attack' would enable to encompass cover or blurry actions attached to hybrid warfare. It would also enable rapid joint reaction of the states to counter these information operations and other hybrid warfare methods. Yet, it would also significantly lower the threshold of collective defence, which is something that NATO is struggling to engage in.[55]

---

[53] Lawrence Greenberg, Seymour Goodman, Kevin Soo Hoo. 'Information Warfare and International Law', *National Defense University Press.* (1998).

[54] House of Commons Defence Committee, 'Towards the Next Defence and Security Review: Part Two – NATO', (2014). p. 41.

[55] Jackson, S. NATO Article 5 and Cyber Warfare: NATO's Ambiguous and Outdated Procedure for Determining When Cyber Aggression Qualifies as an Armed Attack. *Center for*

Although these questions need to be considered as part of the global debate surrounding information warfare, they fall into the scope of *jus ad bellum* (the right to wage war), which should be distinguished from *jus in bello* (the law applicable in war), i.e. international humanitarian law. Under international humanitarian law, an attack is defined by Article 49 of the First Additional Protocol to the Geneva Conventions as 'acts of violence against the adversary, whether in offence or in defence'. Professor Sassoli specifies that an international armed conflict is triggered when an act of violence, which is attributable to a state and approved by the highest authorities against another state's territory or armed forces, is committed.[56]

Information warfare is particular as it can take the forms of physical attacks to disrupt command and control systems or telecommunications infrastructure, but it can also be the use of information *per se* to gain a military advantage. The first type can be illustrated by the 1999 NATO bombing of the Radio Television of Serbia headquarters, which resulted in 16 deaths, during the Kosovo War.[57] This physical degradation of information and broadcasting infrastructure is one of the most emblematic examples of the use of information warfare aiming at disruption with physical consequences. This attack fall easily into the scope of 'armed attack' under the United Nations Charter and 'attack' of Article 49 of the First Additional Protocol to the Geneva Convention.

Yet, the second type of information warfare relies on the development of social media and the mainstreaming of technology. The technological progress has led to a transformation of the nature of the operations, with disinformation campaigns and deceptive operations, aiming at deception and influence of the adversaries. There are disagreements in the international community of experts on the precise definition of 'attack' when it comes to the cyber context and it seems that it depends on the nature of the information operations. The Tallinn

---

Insfrastructure Protection & Home Security. August 16, 2016. https://cip.gmu.edu/2016/08/16/nato-article-5-cyber-warfare-natos-ambiguous-outdated-procedure-determining-cyber-aggression-qualifies-armed-attack/

[56] Marco Sassoli. *International Humanitarian Law: Rules, Controversies, and Solutions to Problems arising in warfare*. Edward Elgar Publising Limited. (2019). p.173.

[57] Stojanovic, M. 2021. Suspicions Persist About NATO's Deadly Bombing of Serbian TV. *Balkan Transitional Justice.* April 23, 2021. https://balkaninsight.com/2021/04/23/suspicions-persist-about-natos-deadly-bombing-of-serbian-tv/

Manual 2.0 notes that operations causing 'inconvenience or irritation' to civilians do not meet the threshold of an attack in the sense of international humanitarian law. Yet, there is no agreement either on the precise scope of 'inconvenience or irritation'. The Tallinn Manual 2.0 specifies that telecommunications jamming, such as Distributed Denial-of-Service attack, are not 'attacks' in the sense of international humanitarian law.[58] However, if the operation is a part of a more global action, which qualifies as an attack, and contributes making this attack possible, international humanitarian law is applicable. Therefore, it seems that deceptive information operations do not seem to qualify as an 'attack' on their own.

One should go through the specifications of the Rules 92 and 93 of the Tallinn Manual 2.0 in the context of cyber operations to determine whether information warfare could fit this definition. Firstly, the Tallinn Manual 2.0 states that violence encompasses violent consequences. Rule 92 specifies that violence 'must be considered in the sense of violent consequences' i.e. causing injury or death to persons or damages or destruction to objects. Therefore, the attack is defined by its aftermath whether it has caused great harm or not. This approach closes the door to most of contemporary information operations, as they would rather aim at influencing rather than destroying the adversary. The international group of experts of the Tallinn Manual 2.0 proposes to extend the notion of violent consequences to non-tangible ones, such as serious illness and severe mental suffering, to provide a better protection to civilians. Yet, those would still be subsequent to kinetic injury, which still leaves aside a large amount of contemporary information operations.[59] The scale of the consequences is also taken into account. Thus, large-scale operations, such as the disruption of all email communications, are prohibited.[60] Yet, the majority of the Tallinn experts are reluctant to draw conclusions on the disruption of communication as an armed attack, because international humanitarian law

[58] International Committee of the Red Cross. 2019. "International Humanitarian Law and the Challenges of Contemporary Armed Conflicts". 22 November 2019. p.26-34. Available at: https://www.icrc.org/sites/default/files/document/file_list/challenges-report_new-technologies-of-warfare.pdf.
[59] Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Rule 92. §8 (2017).
[60] *ibid.*

currently does not provide such an extensive coverage yet. The International Committee of the Red Cross considers that an 'attack' should not only cover the operations causing death, injuries or physical damages but also rendering something dysfunctional. Indeed, seeing the diversity of forms of warfare, the sole interpretation of the traditional armed attack would be too restrictive to fulfil the purpose of civilian protection of international humanitarian law.[61]

Secondly, the Tallinn Manual 2.0 states that an attack 'is not limited to violent acts'. However, 'nonviolent operations, such as psychological cyber operations and cyber espionage, do not qualify as attacks'.[62] Acts of violence should be understood as activities releasing kinetic forces, although other kinds of attacks. This approach underlines the traditional framework given to the legal corpus of armed conflicts. Until now, war has been understood as the use of physical force with physical armies but the growing use of technology questions this approach. The Tallinn Manual 2.0 provides the example of a fake tweet published to cause panic among the civilian population. However, the publication does not constitute either an attack, or a threat. Although this information could trigger terror among civilians, it would not be considered an attack as it does not result in foreseeable injury or damages and remains a lawful action under international humanitarian law. Yet, there are a number of means of warfare, such as radiological or chemical weapons, which do not release kinetic forces, but are widely considered attacks.[63] Therefore, although information warfare seems not to fit the definition of an 'attack' because of its intangibility, there is thus a possibility for evolution here.

The international group of experts of the Tallinn Manual 2.0 seems reluctant to take the lead on qualifying information operations as an attack, and it would be interesting to see if there is any evolution on this in the future Tallinn Manual

[61] International Committee of the Red Cross (2019) "International Humanitarian Law and Cyber Operations during Armed Conflicts". Position paper submitted to the 'Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security' and the 'Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security'.
[62] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts. Art. 49(1). (1977)
[63] International Criminal Court. *Prosecutor v. Dusko Tadic a/k/a "Dule"*. Decision on the defence motion for Interlocutory appeal on jurisdiction §120.

3.0 to be published in 2026.[64] Just like it did for chemical weapons, international jurisprudence might endorse this leadership role and open the way for the systematic qualification of information operations as an attack.[65] Indeed, as above-mentioned, there are little opportunities for reinterpretation of the 'armed attack' and such qualification.

ii. Intangibility of the Damages

International humanitarian law aims at protecting civilians and humanizing armed conflicts by imposing limits on the conduct of hostilities and the means of warfare. In this view, the assessment of potential or actual damages is essential in the conduct of hostilities to determine if a mean or method of warfare cause unnecessary sufferings. The scope of 'damages' varies depending on the type of information operations. Information operations can lead to tangible damages, in which cases international humanitarian law is easy to apply. It is the case of physical attacks on telecommunications infrastructure and information controls systems, and non-physical attacks related to cyberwarfare on those, resulting in financial costs, human casualties or property damages. The 1999 NATO bombing of the Radio Television of Serbia was criticised a lot as it resulted in the death of 16 journalists.[66] It raised questions about media participation in hostilities and the legitimacy of targeting broadcasting infrastructure – which this dissertation will attempt to answer in the next sections. This event led to numerous NATO press releases to justify the bombing until the publication of the report of the investigating committee.[67]

---

[64] The NATO Cooperative Cyber Defence Centre of Excellence. 'The Tallinn Manual' https://ccdcoe.org/research/tallinn-manual/

[65] International Committee of the Red Cross Study on Customary International Humanitarian Law, Practice Relating to Rule 74. Chemical Weapons. https://ihl-databases.icrc.org/customary-ihl/fre/docs/v2_rul_rule74

[66] Zivanovic, M. Haxhiaj, S. (2019). '78 days of fear: Remembering NATO's Bombing of Yugoslavia'. *Balkaninisghts.com.* March 22, 2019; The Irish Times. (1999) 'Government stance on NATO bombing of Serbia criticised by opposition' *The Irish Times.* March 26, 1999; Erlanger, S. (2000) 'Rights Group says NATO bombing in Yugoslavia violated law'. *New York Times.* June 8, 2000.

[67] International Criminal Tribunal for the forNATO's Bombing of mer Yugoslavia. Final report to the Prosecutor by the Committee Established to Review the NATO Bombing Campaign Against the Federal Republic of Yugoslavia. 13 June 2000. Available at: http://www.icty.org/sid/10052#IVB4

Despite the controversies surrounding this event, numerous bombings of telecommunications and broadcasting stations occurred during the 2006 Lebanon war and after.[68] Some stations and satellites of the Al-Manar Television channel and Nour radio were bombed. Indeed, they were considered the Hezbollah relay of terrorist messages, inciting to violence. The head of Al-Manar already recognised in 2000 that the station intended to wage 'psychological warfare against the Zionist enemy'.[69] However, the bombings did not reduce to silence the television channel very long as the public relations director declared that the organisation had developed an emergency plan to transmit from other places after the United States of America decided to list Hezbollah as an alleged terrorist movement.[70] This emergency plan can certainly be explained by the lessons learnt from the bombings of the Serbian radio and television headquarters by NATO during the Kosovo War.

However, contemporary information operations tend to use new means and methods of warfare, resulting in intangible damages, such as defamation, degradation of reputation relying on propaganda, or deprivation of truth and facts with misinformation and disinformation. In those cases, the application of the rules of international humanitarian law rules relating to damages is difficult because of the intangible nature of contemporary practices of information warfare. It is extremely difficult to assess the gravity and extent of the consequences of all of these forms of information operations. So far, the legal corpus remains silent facing these intangible damages as they do not match the types of damages that international humanitarian law was intended to alleviate initially. This silence results in the lack of restrictions on those activities unless it physically harms non-combatants, with the exception of terror and perfidy.

---

[68] Government of Israel. 2007. "Behind the headlines: The Second Lebanon War - One year later." Govt. Israel 12 Jul 2007. Available at: https://reliefweb.int/report/israel/behind-headlines-second-lebanon-war-one-year-later

[69] European Parliament. 2005. "Parliamentary questions: Al-Manar Hizbullah Television" Charles Tannock (PPE-DE), Jana Hybášková (PPE-DE) and Jas Gawronski (PPE-DE) to the Commission 10 March 2005. E-0909/05. Available at: https://www.europarl.europa.eu/doceo/document/E-6-2005-0909_EN.html

[70] Congressional Research Service. *Lebanon: the Israeli-Hamas-Hezbollah Conflict*, Congressional Research Service, The Library of Congress. (2006).

Some argue that the outcomes of the information operations and operations with a traditional use of force should be compared. If both outcomes are the same, then, information warfare should be considered a use of force triggering damages. Professor Robbat provides the example of a group of information warriors grounding a military plane, which enables to win the battle. Information warfare enables it when it could have been done by physically capturing the plane and the staff.[71] When it comes to the consequences of new technologies, information circulates faster on a wide scale and it is to be feared that the damages could be exacerbated since it is more difficult to keep control of information. On the other hand, there are more alternatives to fact check, change of television channel or twitter accounts to access different information. Some would argue that information deceives only those who want to be deceived.[72]

These information operations are launched remotely and anonymously. These contactless operations make the causality link difficult to prove and render accountability also complex to establish. Similarly, it is difficult to delimit who should be held accountable among all the people who took part in the creation and the broadcasting of the information operation. Some suggest that responsibility should always be kept at the personal, command and national levels, even though there could be complications when the attacker use the information and communication platforms of another state.[73] The distance between the attacker and the target does not alter the identification of the responsible people *per se,* but rather increase the phenomenon of depersonalisation.[74] Some scholars consider that there should be a minimum level of interpersonal relationship between adversaries to avoid the deconsecration of the gravity of the attack and the significance of death.[75] Although the development of new technologies helps reduce significantly the

[71] Michael J. Robbat. "Resolving the legal issues concerning the use of information warfare in the international forum: the reach of the existing legal framework and the creation of a new paradigm. *Science and Technology.* (2000).
[72] Lev Rubinshtein « obnazheniye priyema » *grani.ru.* 11 September 2008.
[73] Draft Articles on the Responsibility of States for Internationally Wrongful Acts. Commentaries. Art. 6, §3 (2001).
[74] William Boothby. "Some legal challenges posed by remote attack". *International Review of the Red Cross.* Vol. 94. No. 886. (2012).
[75] Sparrow, R. "Killer Robots". *Journal of Applied Philosop*hy, 24(1) pp. 62–77. (2007).

number of casualties, it also leads to invest in more discreet technologies, which shed less blood, such as information operations.

B. Distinguishing the Unlawful from the Legitimate Targets

In armed conflicts, combatants should be distinguished from combatants as well as civilian objects from used-military objectives. Information warfare makes this distinction difficult (i). When an object serves both military and civilian function, it should be assessed if this object constitutes a military objective by examining the military necessity of this attack and ensuring the respect of the principle of proportionality. This assessment becomes blurry with the evolution of information and communication technologies (ii).

i. Interconnectedness and the Principle of Distinction

One of the most important principles of international humanitarian law is the principle of distinction. The parties must distinguish combatants from civilians and military objects from civilian objects when conducting hostilities. The first category is lawful target while the civilian category enjoys protection from attacks.

The 2006 Lebanon War is often cited as a case study for information warfare for several reasons. Israeli armed forces made a massive use of information for their military strategy. The release of warning messages through diverse media, such as dropping leaflets, radio broadcasts, etc. to warn the population of the areas where Hezbollah was operating.[76] This advance warnings must be made in accordance with the Rule 20 of the International Committee of the Red Cross Study of Customary international humanitarian law.[77] The study of state practice 'indicates that all obligations with respect to the principle of distinction and the conduct of hostilities remain applicable even if civilians remain in the zone of operations after a warning has been issued. Threats that all remaining civilians would be considered liable to attack have

[76] Behind the headlines: The Second Lebanon War - One year later Govt. Israel12 Jul 2007
[77] International humanitarian law database. Rule 20 Advance Warning.

been condemned and withdrawn.' It was thus reported that the Russian Federation dropped leaflets stating that those who remain will be viewed as terrorists and bandits and will be destroyed.[78] *De facto,* these information operations were conducted in the view of respecting the principle of distinction and constant care, to spare civilians. Despite this rule, many Israeli officials made statements suggesting that anyone staying in those areas after the warnings would be linked to Hezbollah.[79] The authorities assumed that civilians could not have ignored or not received the messages. Thus, they considered civilians as lawful and legitimate targets.[80] Information became therefore an instrument to legitimise attacks in civilian areas, when these zones appear suspicious.

Contemporary practices of information warfare make this distinction complicated because of the targeted audience and because of the format. First, there is an increasing practice of disinformation campaigns targeting civilians as part of a more global strategy. International humanitarian law only prohibits operations directed at civilians if they amount to an attack. Yet, as seen before, the characterization of 'attack' of certain information operations is still ambiguous. Information operations can therefore legitimately target civilians. Although such operations targeting civilians would be legal, the battlefield seems to move to the civil ground from the ethical stance. It might lower the threshold of what it is acceptable for civilians to suffer as 'inconvenience' during an armed conflict. However, if there is a risk of foreseeable damages, the operations should be avoided according to the customary principle of precaution for civilians.[81] Once again, this comes up against the difficulties of qualifying the consequences of information operations as damages.

The difficulties raised by this blurry distinction have implications not only on the target but also on the method. Indeed, weapons, means and methods of warfare must comply with the principle of distinction and other existing

[78] *Ibid.*
[79] Human Rights Watch. "Why They Died, Civilian Casualties in Lebanon during the 2006 War". Human Rights Watch. (2007).
[80] *Ibid.*
[81] Protocol I to the Geneva Conventions. Art. 57(1). (1977).

international humanitarian rules and therefore any means of war with indiscriminate effect is prohibited. In this context, the use of new information and communication technologies needs to be monitored. Concerning cyber operations, the Tallinn Manual 2.0 specifies that creating a chain of events, which would be out of the control of the attacker, is considered violating the principle of distinction.[82] When it comes to information, it is disseminated widely and rapidly on social media once published or shared. Information operations can be operated even by civilians. It spreads uncontrollably at the whim of retweets, messages and shares. The Tallinn Manual 2.0 rules could thus be applicable here. Yet, as long as the circulation of such information does not cause foreseeable injury or damage, it does not constitute an indiscriminate operation.[83] Once again, it is subjected to tangible and violent consequences. Thus, the distinction becomes blurry and so do the lawful military targets.

ii. Information and Military Objectives

Information, Propaganda and broadcasting infrastructure

One of the aspects of the principle of distinction is the prohibition to target civilian objects. Articles 48 and 52(2) of the Additional Protocol I regulate this prohibition stating that attacks should be limited to military objectives. It defines military objectives as 'objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage'.[84] It is more complicated when it comes to 'dual-use objects', referring to objects, which serve civilian function but could qualify as a military objective. This is the case of telecommunications networks and social media, which hold a delicate position amplified by the development and mainstreaming of information and communications technologies. This duality makes the applicability of this rule more difficult. Indeed, these telecommunications equipment and networks are

[82] Tallinn Manual 2.0, Rule 105. (2017).
[83] Cohen, L. (2022) "The new era of disinformation wars". *Voelkerrechts blog.* 30 November 2020. https://voelkerrechtsblog.org/de/the-new-era-of-disinformation-wars/
[84] Additional Protocol I, Articles 48 and 52(2)

dual-used, interdependent and interconnected. Targeting a part of the network, like a military telecommunications network or system, would necessarily have an impact on the civilian network or system. In this sense, it is quite likely that most of information operations will thus fall into civilians' hands and the foreseeability of this undermines the principle of constant care.

The question was raised and discussed in the aftermath of the much-criticised NATO bombing of the Radio Television of Serbia headquarters, which occurred on the evening of 23 April 1999, resulting in 16 deaths.[85] This operation intervenes in the context of the Kosovo war opposing the Kosovo Liberation Army and NATO against the State Union of Serbia and Montenegro. The national broadcasting building was a dual-use object, 'making an important contribution to the propaganda war which orchestrated the campaign against the population of Kosovo'.[86] In 2000, the final report of the Prosecutor by the Committee established to review the NATO bombing campaign against the Federal Republic of Yugoslavia seeks to bring answers to the question of legitimacy of the national infrastructure broadcasting propaganda as a definite military objective and to the question of the proportionality of civilian casualties next to the military advantage.[87]

Article 52(2) of the Additional Protocol I provides that 'in case of doubt whether an object which is normally dedicated to civilian purposes […] is being used to make an effective contribution to military action, it shall be presumed not to be so used'. Following this logic, the question of the legitimacy of

[85] Stojanovic, M. 2021. Suspicions Persist About NATO's Deadly Bombing of Serbian TV. *Balkan Transitional Justice.* April 23, 2021.
[86] Avril McDonald. *Yearbook of International Humanitarian Law - 2003.* Volume 6. Cambridge University Press. 31 December 2006.
[87] Following the NATO bombing campaign against the Federal Republic of Yugoslavia, the Prosecutor of ICTY has received numerous requests to investigate allegations that senior political and military figures from NATO countries committed serious violations of international humanitarian law during the campaign, and to prepare indictments pursuant to Article 18(1) & (4) of the Statute. According to Article 18 of the Tribunal's Statute provides that the Prosecutor shall initiate investigations *ex officio* or on the basis of information obtained from any source, particularly from Governments, United Nations organs, intergovernmental and non-governmental organizations. The Prosecutor shall assess the information received or obtained and decide whether there is sufficient basis to proceed". The committee was established on 14 May 1999. International Criminal Tribunal for the former Yugoslavia. Final report to the Prosecutor by the Committee Established to Review the NATO Bombing Campaign Against the Federal Republic of Yugoslavia. 13 June 2000. Available at: http://www.icty.org/sid/10052#IVB4

attacking broadcasting infrastructure should not be even raised as it should be considered that this attack should have been avoided. In addition, the International Committee of the Red Cross defines the term 'military advantage' in its Commentary on the APs as excluding 'an attack which only offers potential or indeterminate advantages'.[88] This is also confirmed by the International Committee of the Red Cross and Major General Rogers, both including broadcasting and television stations in legitimate military objectives under the condition that they meet the fundamental military importance criterion.[89] *De facto,* the attack against the radio and television headquarters only interrupted broadcasting for several hours. This raises doubts about the alleged military advantage gained by this attack next to the 16 deaths it caused. NATO was aware that the network of communications is more complex than just one strike on one station could interrupt propaganda.

In the report of the Prosecutor, it is argued that this bombing attack was necessary to 'disrupt and degrade the command, control and communications network' of the Yugoslav Armed Forces.[90]The report justified the attack because it was part of a bigger strategy aiming at the disruption of the Serbian military command and control system maintaining Milosević in power. NATO emphasized this point in several press conferences. The organization firstly declared that television transmitters were not targeted directly but were only a secondary effect.[91] The month after, NATO gave another press release to explain that the operation aimed at targeting the Yugoslav command and control network as a whole. Indeed, these telecommunications networks were 'essential to Milosevic's ability to direct and control the repressive activities of his army and special police forces in Kosovo' and that it was 'a key element in the Yugoslav air-defence network'.[92] The report thus found that the Radio Television of Serbia headquarters was a lawful military objective, because part

[88] International Committee of the Red Cross Commentary on the Additional Protocols of 8 June 1977. §2024

[89] General Rogers, *Law on the Battlefield.* Manchester University Press. (1996)

[90] Final report to the Prosecutor by the Committee Established to Review the NATO Bombing Campaign Against the Federal Republic of Yugoslavia. 13 June 2000. §72 Available at: http://www.icty.org/sid/10052#IVB4

[91] NATO, Press conference, Spokesman Jamie Shea and Air Commodore David Wilby, 9 April 1999

[92] NATO, Press Conference, Mr. Peter Daniel and Colonel Konrad Freytag. 1 May 1999

of a bigger military strategy aiming at telecommunications networks representing a real advantage.

However, the report also found that generating support for the war through propaganda broadcasting is not sufficient to make the radio television of Serbia headquarters building a legitimate target. Indeed, although prohibited under international human rights law, propaganda for war, meaning the production of one side of the political rhetoric, has been widely accepted as a means of warfare.[93] The Tallinn Manual 2.0 argues that generally, 'psychological operations such as dropping leaflets or making propaganda broadcasts are not prohibited even if civilians are the intended audience'.[94] Furthermore, undermining political support by stopping propaganda broadcasting is not an attack falling into the scope of the concrete and direct military advantage in the meaning of the Commentaries of the International Committee of the Red Cross.[95] This example shows the difficulties related to the principle of distinction and the delicate status of propaganda broadcasting infrastructure in armed conflicts.

Consequences of the Militarisation of Information Infrastructure

This attack had a significant impact on the 2006 Lebanon War as the targeting of broadcasting infrastructure became easier to politically and legally justify. Indeed, the Israeli armed forces attacked the television station al-Manar and the radio station Nour. The armed forces relied on the example of Kosovo to justify their attack.[96] Human Rights Watch noted that both infrastructure served as propaganda outlets for Hezbollah but argued that spreading propaganda does not make these infrastructure military targets as if it does not consist of a concrete and direct military advantage.[97] However, the organisation

[93] International Covenant on Civil and Political Rights. Art 20. (1966). Henning Lahmann, "Protecting the Global Information Space in Times of Armed Conflict". *International Committee of the Red Cross Review* No. 915. (2022).
[94] Tallinn Manual 2.0. Rule 93. §5 (2017).
[95]International Committee of the Red Cross Study on Customary International Humanitarian Law. Practice Relating to Rule 14. Proportionality in Attack
[96] Government of Israel. 2007. "Behind the headlines: The Second Lebanon War - One year later." Govt. Israel 12 Jul 2007. Available at: https://reliefweb.int/report/israel/behind-headlines-second-lebanon-war-one-year-later
[97] Human Rights Watch. "Why They Died, Civilian Casualties in Lebanon during the 2006 War". Human Rights Watch. (2007).

also noted that the Al-Manar station helped Hezbollah to recruit people thanks to this propaganda.[98] It could be argued that this military advantage is sufficiently concrete to justify the attack. However, the station did not provide any military directive during the conflict as propaganda was only disrupted for a few minutes. One thing is certain: the attack on the radio and television of Serbian headquarters has made it easier to justify attacks on broadcasting stations.

Secondly, this attack and the interpretation made by the committee established to review the NATO bombing campaign against the Federal Republic of Yugoslavia had significant implications for the further development of information warfare and technologies. One could ask what the limits of 'broadcasting and telecommunications infrastructure' are. Indeed, phones and computers become the broadcasting platforms, as it is only one click to spread information or create a radio app. A person knowingly forwarding or circulating malicious software or information, causing harm, would be considered as conducting an attack. Similarly, if 'broadcast' would mean massively posting or re-sharing social media content, anyone's social media, and thus, their physical support, could become a military objective. This would severely undermine the protection of civilians if mainstream technologies of daily life were considered legitimate targets. In the end, the use of information warfare did not prove success as it did not silence Serb propaganda. An efficient military strategy would probably have required a better coordination of information warfare operations and traditional methods to achieve such objective.[99] Furthermore, it is also to be noticed that starting from this attack, information warfare will be a tool of influence, rather than a tool of disruption. Indeed, with the development of technologies, information warfare shifts to numerical manipulation of information and wide campaign of information, rather than targeting with physical attacks propaganda infrastructure.

Another issue is the involvement of journalists or media workers in armed conflicts. In terms of responsibility, the established committee for the

[98] *Ibid.*
[99] Singer, P. "Winning the War of Words: Information Warfare in Afghanistan". *Brookings.* (2001).

NATO bombing on the radio and television of Serbia headquarters established the participation of journalists in propaganda may not be considered as a direct participation in hostilities. However, this question often comes back to the table. Indeed, the International Council on Human Rights Policy raised the following questions about the International Criminal Tribunal for Rwanda: 'can journalism kill? At what point does political propaganda become criminal?'[100] Media workers were tried by this tribunal on the charge of incitement to genocide and some of them were found guilty as they played a crucial role in the incitement of ethnic hatred and violence, which Radio Television Libre des Milles Collines vigorously pursued'.[101] Therefore, it seems journalists stand in a delicate position. In terms of protection, journalists are under the protection of civilians' status. However, the established committee concluded its report by legitimising the bombing because it aimed at the disruption of a bigger command and control systems. This could suggest that journalists are taking part in the hostilities by performing their job as media workers. While they were enjoying a specific status under international humanitarian law, one could wonder if creating a special status for independent journalists would be appropriate. Indeed, the increasing number of special status could weaken the protective value of already accepted status.[102]

As the number of civilian journalists killed during armed conflicts is still significant, there is a lack of effective investigations on those intentional attacks, kidnapping and acts of torture perpetrated against them.[103] States have the positive obligation to protect the right to life and to conduct effective

[100] The International Council on Human Rights Policy was established in 1998 to conduct applied research into problems and dilemmas that face organisations working in the field of human rights, and closed down in 2012. The Council was independent of governments and inter-governmental organisations as well as voluntary and private sector organisations. The 30 Council Members met annually to identify and discuss emerging international human rights issues.
International Council on Human Rights Policy (2002) *Journalism, Media and the Challenge of Human Rights Reporting*, Switzerland, p.16 quoting Marlise Simons, *Internatinal Herald Tribune* 'Trial examines war crimes free speech and journalism' 5 March 2002

[101] International Criminal Tribunal for Rwanda. *The Prosecutor v. Georges Ruggiu*. 2000. §50. Available online at http://www.ictr.org/default.htm

[102] Alexandre Balguygallois, « Protection des journalistes et des médias en période de conflit armé ». *International Review of the Red Cross*. Vol. 86, No. 853. (2004). pp. 37-68; https://casebook.icrc.org/case-study/protection-journalists.

[103] Mijatović, D. (2022) "Not a target – the need to reinforce the safety of journalists covering conflicts: Statement by the Council of Europe Commissioner for Human Rights". 2 May 2022.

investigations when somebody died in violent or suspicious circumstances.[104] To close this gap, the Council of Europe proposed a series of measures last May, including the provision of an effective early warning before carrying out attacks which may affect the civilian population, such as the attacks of broadcasting infrastructure, the easing of licensing to obtain protective equipment or diplomatic and logistical assistance in case of evacuation or relocation.[105] Beyond the concerns of legitimate targets, one should examine the contemporary methods used in conflicts.

Part II. Scrutinising the Means of Information Warfare in the Conduct of Hostilities

There are numerous rules for the conduct of hostilities in international humanitarian law drawing limits on military operations. This section will come back on the prohibition of perfidy (A) and the prohibition to terrorize civilians (B) and the incitement to violence (C) applied to information warfare practices in the Second Lebanon War, the Russo-Georgian war and the Russo-Ukrainian war.

A. The Prohibition of Perfidy: Safeguarding Civilians and Combatants from Deviousness

As information warfare relies on deception, perfidy and ruses of war should be distinguished (1). The application of international humanitarian law to the current practice of deceptive information operations in the Russo-Ukrainian war should be examined (2) as well as the challenges raised by this practice and the potential development of information technologies could trigger (3).

1) Information Warfare as a Mixture of Perfidy and Ruses of War

[104] European Court on Human Rights. "Guide on Article 2 of the European Convention on Human Rights: Right to Life" Updated on the 31rst December 2021. Available at: case-law

[105] Council of Europe, 'Not a target – the need to reinforce the safety of journalists covering conflicts'. Statement by the Council of Europe Commissioner for Human Rights. 2 May 2022. Available at: https://www.coe.int/en/web/kyiv/-/not-a-target-the-need-to-reinforce-the-safety-of-journalists-covering-conflicts

As information warfare intrinsically relies on the use and manipulation of information for strategic advantage, ruses of war and perfidy are omnipresent. These two concepts must be first distinguished. Indeed, ruses of war are permissible while perfidy is prohibited under international humanitarian law but the line is thin.

Article 37(1) of the Additional Protocol I to the 1949 Geneva Conventions defines perfidy as killing, injuring or capturing of an adversary by resort to an act that invites, 'the confidence of an adversary to lead him to believe that he is entitled to, or is obliged to accord, protection under the rules of international humanitarian law with the intent to betray that confidence'. This rule is also considered customary international law when perfidy leads to death and injury.[106] Indeed, Hague Regulations and the Rome Statute do not mention perfidy when it leads to capture.[107] Concerning cyber operations, the Tallinn Manual 2.0 specifies that the act does not need to be successful to be qualified perfidy and that the perfidious act must be the proximate cause of the damage.[108] Therefore, the act must simultaneously (i) relate to an international humanitarian law protection for a particular person, object or activity; (ii) invite the adversary confidence that they are entitled to this protection; (iii) intentionally betray the confidence of the adversary; and (iv) result in the prohibited effect of the adversary's death or injury. As mentioned above, the Tallinn group of experts disagrees whether the perfidious act must actually result in the injury or death of the adversary and so does the International Committee of the Red Cross Commentary to Article 37.[109] Some argue that 'the attempted or unsuccessful act' is sufficient to be prohibited. Indeed, even though the perfidious act fails, it still remains the use of perfidy and thus, such conducts should be condemned.

Perfidy needs to be distinguished from the ruses of war, which are 'acts intended to mislead the enemy or to induce enemy forces to act recklessly' and are legal acts. These include the use of diverse methods, such as mock

[106] International Committee of the Red Cross Study on Customary International Humanitarian Law. Rule 57 Ruses of war.
[107]Tallinn Manual 2.0. Rule 122. §2. (2017).
[108] *Ibid* §5.§7
[109] International Committee of the Red Cross Commentary to Article 37.

operations or misinformation. An example of permissible ruses of war is provided in the 1987 International Committee of the Red Cross Commentaries on the APs to the GCs as the circulation of misleading information, but there is no mention of manipulated or falsified information or sources of information.[110] The Rule 57 of the International Committee of the Red Cross on Customary Law establishes that an element of legality is crucial to distinguish both concepts as 'ruses of war are not prohibited as long as they do not infringe a rule of international humanitarian law'.[111] Lahmann re-examined the 1987 International Committee of the Red Cross Commentaries listing permissible ruses of war, such as the simulation of noise of an advancing column, the creation of fictitious positions or simulated attacks, because they confuse the senses of civilians. Lahmann specifies that 'actively corroding a civilian information space with the aim to spread confusion and uncertainty among the civilian population and without any direct link to combat activity' does not qualify a permissible ruse of war.[112] Indeed, the direct link is an essential element, otherwise the operation would be affecting civilians without gaining any military advantage and thus, it would undermine the principle of distinction. Overall, these two concepts put next to each other, the scope of permissible deception, i.e. ruses of war, has a broader scope than perfidy since the latter requires specific conditions, including international humanitarian law breaches of protection and damages. As information warfare relies on the dissimulation or the intentional availability of information for the adversary, perfidy and ruses of war are combined. Looking at the contemporary practices of information warfare, it can be difficult to distinguish the legal practices from the illegal ones.

2) The Use of Perfidious Information Operations and deep fakes

Taking the example of the ongoing Russo-Ukrainian war, Moscow announced the rendition of the Ukrainian soldiers of the Azovstal siege several

[110] Yves Sandoz, Christophe Swinarski & Bruno Zimmermann (eds), Commentary to the Additional Protocols, International Committee of the Red Cross. §1516.
[111] International Committee of the Red Cross Study on Customary International Humanitarian Law. Rule 57 Ruses of war.
[112] Robin Geiss, R & Henning Lahmann. "Protecting the global information space in times of armed conflict". *The Geneva Academy.* (2021).

times.[113] A particularly marking event was the release of a deep fake video displaying President Zelensky calling on his soldiers to lay down their weapons. The video was uploaded on a Ukrainian news website, which had been hacked, on the 16th of March 2022 (See figure 4). The same day, a deep fake video of President Putin also circulated claiming that the Russian Federation has won the war and that Ukraine has recognized Crimea as a Russian territory.[114] Although the videos were well assembled, many people noted the problem of lip-syncing or other hints revealing the fraud. By releasing these two videos, the Russian military hoped to galvanize Russian troops and to lead Ukrainian soldiers to surrender. The target was the Azovstal siege at Mariupol, which was a strategic point of interest for the Russian military and a highly symbolic place against the Ukrainian army so far. The videos invited the confidence of the Ukrainian soldiers, so they would surrender believing they benefited from the prisoners of war status. This was a strategic move to weaken the siege of Mariupol and gain an advantage on Kiev. It was likely that the surrendered soldiers would have been captured or injured. This information operation to weaken the Azovstal siege and the example provided by the Tallinn Manual to illustrate cyber perfidy look particularly alike. Indeed, the Tallinn Manual illustrates cyber perfidy with the example of 'an email sent by a military unit to the adversary indicating an intention to surrender some days later at a specific location'. This act would lead to an ambush resulting in a soldier's death and could be considered perfidy. As for the deep fake videos, it is obvious that such perfidious dissemination of information aims at demoralising Ukrainian soldiers. As it intervened in the heated last days of the Azolstal siege, it is likely that it also aimed at capturing the Ukrainian combatants. The second assumption is that there would have been casualties considering the environment of impunity since the invasion of Ukraine, which is currently the object of an investigation by the International Criminal Court.[115] Both these information operations invite the adversary confidence that they are entitled to this protection under international

[113] L'Obs, « Bombardements, reddition de soldats ukrainiens démentie… Le point sur la situation a Mariupol » *L'Obs*. (2022).
[114] Byrne, J. 2022. "Deepfakes now a political weapon in the Ukrainian war". *Thred.* 18 March 2022. https://thred.com/tech/deepfakes-now-a-political-weapon-in-the-ukrainian-war/
[115] Khan, K.. "Statement of ICC Prosecutor, Karim A.A. Khan QC, on the Situation in Ukraine: Receipt of Referrals from 39 States Parties and the Opening of an Investigation". *International Criminal Court. (*2022).

humanitarian law with an intent to betray the confidence of the adversary, which qualify as perfidy, even though it did not lead to the adversary's death or injury.

3) Perfidy and the Modern Practices of Information Warfare

The Tallinn Manual explicated how perfidy and ruses of war should be applied to the cyber context. There are similarities between the applicability of these rules to cyberattacks and information operations. The conditions remain the same and both types of warfare meet the same difficulties when it comes to the requirements of damage and proximate cause. Indeed, damages are more difficult to assess because of their intangible character in most of the cases and their temporal distance with the information operation. Similarly, the causal link might not be clear between an information being disseminated and circulated and the result of death or injuries. Modern practices of disinformation seek to influence the adversaries to gain a military advantage rather than physically harm them. Therefore, the scope of perfidy applies in a very narrow manner when it comes to information warfare as the Tallinn experts and states are still mitigated whether it must result in physical damage to be qualify as perfidy. Indeed, it would solely prohibit information operations, which aim at physical consequences with a specific mode of deception, as mentioned above.

Incidentally, Professor Sassoli expresses doubts over online perfidy and the example provided by the Tallinn Manual.[116] In his view, the perfidious dissimulation of emblems cannot be compared to military websites, which take the appearance of civilian status in order to deceive the adversary into being killed, captured or injured. Indeed, 'why could a user of a civilian website believe that he is entitled to, or obliged to accord, protection by international humanitarian law, which is part of the definition of perfidy?' Therefore, the application of the rule of perfidy to information warfare is delicate because it brings back unsettled questions on the front scene concerning the delimitation of the rule concerning physical effects.

[116] Marco Sassoli. International Humanitarian Law: Rules, Controversies, and Solutions to Problems arising in warfare. Edward Elgar Publising Limited. (2019). p.541.

The example of deep fake videos used in the Russo-Ukrainian war is of particular concern, as part of the emerging and disruptive technology, which was also called 'weapon of mass distortion' by a researcher from King's College London.[117] These synthetic media technology is prompt to perfidy and could have worrying implications on nuclear weapons decision-making. Indeed, as states slowly incorporate deep fakes for warfighting, these videos are a threat to command, control and communications systems. They intervene in a context of political divide and trust erosion lowering the nuclear threshold. This kind of information operation could lead to pre-emptive strikes or quick escalation to conflict because of a deep fake video involving a nuclear ultimatum. Technology has enabled new possibilities for information warfare making even more difficult to distinguish the reality from fiction. This specific technology is a relevant illustration of the need of norms to regulate the use of information in crisis and conflict time.[118]

B. The Prohibition of Terror: The Recognition of Non-Tangible Sufferings

The prohibition of terror is a long-standing prohibition (A), which keep open the way for a better protection of civilians against information warfare (B).

B) The prohibition of terror

International humanitarian law sometimes considered non-tangible harm suffered by civilians. Indeed, the rule prohibiting terror aimed at preventing mental suffering from the civilian population. Article 33 of the 1949 GC IV provides that 'all measures of intimidation or of terrorism are prohibited'. Article 51(2) of the API prohibits 'acts or threats of violence the primary purpose of which is to spread terror among the civilian population'. Other instruments, judicial or quasi-judicial bodies, and a large range of military

[117] Marina Favaro. "Weapons of Mass Distortion: A new approach to emerging technologies, risk reduction and the global nuclear order". Centre for Science & Security Studies of King's College London. (2021).
[118] Mishra, S. 2021. "Deep fakes: the next digital weapon with worrying implications for nuclear policy". *European Leadership Network.* 3 November 2021. https://www.europeanleadershipnetwork.org/commentary/deep-fakes-the-next-digital-weapon-with-worrying-implications-for-nuclear-policy/

manual also prohibit the use of terror.[119] Therefore, the prohibition of terror is widely recognized and part of customary international law.

The prohibition targets a specific type of action since terrorizing the population must be the primary purpose of the act, whatever the military advantage gained afterwards. In this sense, the International Criminal Tribunal for the former Yugoslavia defines the concept of terror in the *Galić* judgement in 1993. Terror would equate with a long-term and direct 'extreme fear', capable of causing long-term consequences targeting civilians and causing deaths or serious injuries to body and health.[120] The prosecution specified, 'It affected every waking moment of their lives. People for 15 months over the period of this indictment knew absolutely no sense of safety anywhere in the city. Terror is […] the intentional deprivation of a sense of security. […] This is a fear calculated to demoralize, to disrupt, to take away any sense of security from a body of people who have nothing […] to do with the combat.'[121] *De facto,* the court was dealing with a case of massive snipping and shelling campaign. Thus, one should wonder whether such prohibition can apply to information operations. The subsequent question would be to determine how the assessment of the limits of terror and demoralization in information should be conducted.

2) <u>The Recognition of non-tangible damages</u>

Coming back to information warfare, the prohibition of terror is strictly conditioned to an attack, meaning that the sole terrorizing information does not amount to an attack if it is not accompanied by one. Trying to illustrate this in the context of cyber operations, the Tallinn Manual 2.0 actually provides an example amounting to information operations. Indeed, a Twitter message, announcing the spreading of a highly contagious and deadly disease throughout the population, would be neither an attack, nor a threat. Although the population is terrified, it does not fall into the scope of terror because there was no attack. Therefore, the mere exploitation of terror or the threat of an attack is not

[119] International Humanitarian Law Database, Practice Relating to Rule 2. Violence Aimed at Spreading Terror among the Civilian Population
[120]International Criminal Tribunal on the former Yugoslavia. *The Prosecutor v. Galić*: A. Trial Chamber, Judgement and Opinion, §91–137, 208–597.
[121] International Humanitarian Law database. Practice Relating to Rule 2. Violence Aimed at Spreading Terror among the Civilian Population

sufficient, as it does not reach the threshold of an attack under international humanitarian law. It does therefore lead back to the debate on the characterization of information operations as an attack.[122] The legal reasoning of the experts of the Tallinn Manual is conducted through a cyberwarfare lens, ignoring the growing modern practice of information warfare. The requirements of (i) an attack and (ii) a primary intent to terrorize largely narrow the scope of terror when it comes to information warfare. It under-evaluates psychological implications of massive disinformation campaigns and deep fakes, which are now made possible by social media.

The limits between psychological warfare and actual terror can be blurry. During the 2006 Lebanon war, Israel issued repeated messages to warn the population of their operations and the fights, using leaflets, television announcement and phone calls. Some argue that specific instructions were given to respect the constant care principle, such as the route and types of vehicles used by the Israeli armed forces to be distinguished from Hezbollah ones.[123] They broadcast in Arabic messages to the intention of the Lebanese population to ask residents to evacuate the areas and call officials to make sure they proceed to evacuations.[124] On 2 August 2006, Israel launched an information operation hacking the Al-Manar television channel attached to Hezbollah as part of the second Lebanon war. The video displayed Hassan Nasrallah asserting the superiority of Israel and dead bodies and bombings on the organisation control centres and rocket launchers.[125] The constancy of warning messages and frightening video messages inflicted steady fear upon civilians to be bombed or to leave their houses and leave everything behind them.

Another example of immaterial damages caused to civilians can be observed in the aftermath of the invasion of Ukraine as both governments tried to keep their body counts quiet. The Russian Federation is particularly reluctant

---

[122] See part I. A. (i) on 'challenging the use of force'.

[123] Government of Israel. 2007. "Behind the headlines: The Second Lebanon War - One year later." Govt. Israel 12 Jul 2007. Available at: https://reliefweb.int/report/israel/behind-headlines-second-lebanon-war-one-year-later.

[124] *Ibid.*

[125] AFP. 'Israeli 'hackers' target Hezbollah TV'. *Aljazeera.* 2 August 2006. https://www.aljazeera.com/news/2006/8/2/israeli-hackers-target-hezbollah-tv; 'Israel Hacks into Al Manar during lebanon war 2006'. Internet Archive. Uploaded : 15 November 2017 by LiveLeakDotCom2507792. Available at : https://archive.org/details/LiveLeakDotCom2507792

to share numbers about the 'special operation'.[126] However, states do have a legal duty to identify the dead and missing persons, respectfully manage the remains and inform the families under international humanitarian law.[127] In February 2022, the Ukrainian Interior Ministry called on the Russian soldiers' relatives to look for their own through photos and videos posted on social media of Russian soldiers captured or killed by Ukrainian forces.[128] The government used a facial recognition artificial intelligence, which searched faces through Russian social media to make the investigation easier and faster. This operation relies on the control of information and undermines the credibility of the Russian Federation, which claims a very low number of casualties. Indeed, the Kremlin supports its narrative by progressively creating a blackout of information on the conflict, with laws shrinking civil society, criminalizing anti-war statements, the absence of official death tolls or details on military assaults against Ukrainian cities.[129] On the other hand, this Ukrainian initiative would ultimately undermine the moral and the support of the Russian people resulting in trauma and emotional distress, if not creating a constant fear for the families.

Information control and operations can therefore lead to great mental sufferings, especially when it touches upon such a sensitive topic as death and the fate of the soldiers. It questions the necessity to fulfil the requirement of an attack since the civilian population are inflicted metal sufferings. As the primary goal of the prohibition of terror aims at preventing and limiting mental sufferings of civilians, it could be argued that an information operation, which has a primary purpose to spread terror, should be prohibited, regardless of the qualification of attack or threat of violence to fulfil this objective.[130]

---

[126] Keating, J. 2022. "A gruesome way of accounting': The politics of body counts in Ukraine". *Grid News.* 1 April 2022. https://www.grid.news/story/global/2022/04/01/a-gruesome-way-of-accounting-the-politics-of-body-counts-in-ukraine/

[127] International Committee of the Red Cross. 2020. « Humanity after life: Respecting and Protecting the Dead" ICRC. Legal Factsheet.

[128] Paresh, D (2022) "Ukraine uses facial recognition to identify dead Russian soldiers, minister says" *Reuters.* 24 March 2022. https://www.swissinfo.ch/eng/ukraine-uses-facial-recognition-to-identify-dead-russian-soldiers--minister-says/47458538

[129] Current Time. (2022) 'Court bans publication of information on Russian Military death toll in Ukraine'. *Radio Free Europe.* June 7, 2022; OHCHR (2022) 'Russia: UN experts alarmed by 'chocking' information clampdown' *OHCHR Media Center.* 12 March 2022.

[130] Lahmann, H. (2022) "Protecting the Global Information Space in Times of Armed Conflict". *International Review of the Committee of the Red Cross.* n°915.

C. Incitement to Violence and New Technologies

Incitement to violence in breach of international humanitarian law is prohibited by common Article 1 to the Geneva Conventions as all parties are under the obligation to respect and ensure respect for international humanitarian law.[131] It means that the dissemination of information inducing combatants or civilians to attack or harm civilians would violate this rule.[132]

The 2006 Lebanon war has been much talked about because of the use of information and communication equipment to incite violence. Indeed, the television channel Al-Manar, openly supporting Hezbollah, incited the Palestinian population and resistance organizations to escalate their campaign against Israel with anti-Semitic propaganda.[133] The ultimate goal was to enlist support of the Palestinian population and suggest that the victory in Lebanon would lead to the victory of the occupied Palestinian territories as well.[134] There have been several cases of media manipulation, one of those being the Adnan Hajj case, which is one of the early examples of manipulation of digital photography. On the 5th of August 2006, a picture from this independent Lebanese journalist was published by Reuters, displaying Beirut after an Israeli raid (See figure 2). This publication intervened in a context of extreme tensions because of the Kana massacre, which had occurred several days before. This airstrike carried out by the Israeli armed forces resulted in 28 civilians.[135] This event was widely mediatised as the large majority of the victims were children. Israeli newspapers asserted that the death toll was swollen to foster anti-Israeli sentiment and argued that the pictures of dead children were staged to shock the audience.[136] (See figure 3) Therefore, the Reuters publication occurred in a tense

[131] Geneva Conventions. Common Art 1. (1949).
[132] The NATO Cooperative Cyber Defence Center of Excellence. 2020. "International Cyber Law: Interactive Toolkit, "Scenario 19: Hate Speech", 1 October 2020, §16. available at: https://cyberlaw.ccdcoe.org/wiki/Scenario_19:_Hate_speech
[133] Reuven Erlicj, Yoram Kahati (2007) "Hezbollah as a case study of the battle for hearts and minds". Intelligence and Terrorism Information Center at the Israel Intelligence Heritage & Commemoration Center.
[134] CNN.com. 2000. "Militant group claims responsibility for Gaza suicide bombing". October 2006, 20. Available at: https://edition.cnn.com/2000/WORLD/meast/10/26/mideast.03/index.html
[135] Reuters. 2007. "Factbox – War in Lebanon, one year ago". 8 July 2007.
[136] Izenberg, D.; Siegel-Itzkovich, J.; Rosen, N. 2006. "Bloggers raise questions about Kana". *The Jerusalem Post.* 2 August 2006; Fendel, Hillel. 2006. "Evidence Mounts that Kana

context of particularly strict scrutiny over newly published content, especially from the Israeli side. Shortly after the publication, numerical retouching was found on the picture as it seems that the smoke from the bombed building had been thickened. This event was interpreted as the intent to amplify the consequences of the raid and thus, sway public opinion.[137] The manipulation of pictures by journalists on both sides of the camp lead to the fostering of hatred and violence against the adversary. Media are thus a central scene for information warfare and media workers stands closely from the prohibited line of incitement to violence in breach of international humanitarian law.

Contemporary information warfare practices are covered by these three prohibitions of international humanitarian law. These prohibitions could be the open door that information warfare needs for the recognition of non-tangible harm. It would be a step forward in recognizing the immaterial damages or sufferings caused by armed conflicts.

Part III. Advancing the Debate on Information Warfare Rules

Some scholars argue that information warfare is already regulated by international law when having an extensive interpretation of international legal framework (A). Although these points of debate are important, there is a legal gap to fill in considering the challenges in the application of international humanitarian law to information operations discussed above (B).

A. The Regulation of Information Operations in International Law

Some argue that information warfare already falls into the scope of international law, such as the law of space and telecommunications (i) or the

"Massacre" Was a Fake". *Arutz Sheva*. 3 August 2006; zombie. 2006. "The Reuters Photo Scandal". *zombietime.com*. 8 August 2006.

[137] Gunthert, A. 2006. « L'affaire Adnan Hajj: première manipulation emblématique de l'ère numérique » 8 August 2006. *Le blog d'André Gunthert.* Available at : https://archive.wikiwix.com/cache/index2.php?url=http%3A%2F%2Fwww.arhv.lhivic.org%2Findex.php%2F2006%2F08%2F08%2F204#federation=archive.wikiwix.com

rules on hate speech (ii). Therefore, an extensive development and interpretation would not be required to fill in the legal gaps or ambiguities left by information operations.

i. Outer Space and Telecommunication Treaties

Dr. Qureshi argues that international law facilitates information operations rather than regulating them as he considers the applicability of the outer space legal framework to information warfare.[138] The 1967 Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space Including the Moon and Other Celestial Bodies (the Outer Space Treaty) includes 112 parties and numerous rules are based on customary principles. Under this treaty, space and celestial objects are the common heritage of humankind. Therefore, space cannot be self-appropriated and every state may conduct its own activities there. As information operations use radio waves transmitted by satellites, space becomes therefore the facilitator of those operations. According to him, international law would thus provide a legal protection to these operations rather than regulating them. In this sense, it is also important to mention the 1958 Geneva Convention on the Law of the Sea, the 1973 United Nations Convention on the Law of the Sea and the International Telecommunications Convention of 1982 protecting submarine communications cables and telecommunications. The latter restricts the use of radio broadcasting for information operations as follows:

> 'Stations, whatever their purpose, must be established and operated in such a manner as not to cause harmful interference to the radio services or communications of other Members or of recognized private operating agencies, which carry on radio service, and which operate in accordance with the provisions of the Radio Regulations.'[139]

These arguments are yet questionable for several reasons. Although the outer space treaty does not say a word concerning wartime, it is necessary to examine the ground justification of this argument, i.e. the principle of common

[138] Waseem Qureshi. Information Warfare, International and the Changing Battlefield", *Fordham International Law Journal.* Vol 43. Issue 4. (2020)
[139] International Telecommunication Union, International Telecommunication Convention. Art 35. (1982).

heritage of humankind. This heritage should be held in trust for future generations. Hence, states are responsible for their space activities in accordance with international law, specifically the Draft Articles of the International Law Commission regulating state's international obligations.[140] Therefore, the coherency of belligerent activities with this principle is questionable. Space, including satellites, should not be exploited to damage, disrupt or interfere with the information systems. Furthermore, the analogy between space security and information security has its limits. Indeed, information warfare capabilities are widely available because of the cheapness and the accessibility of information and communication technologies. Not all states do have the resources to conduct space activities. However, not having the capabilities should not be seen by states as an excuse to avoid any regulation on information operations.

ii. Freedom of Expression and the Prohibition of Hate

One of the significant challenges for the regulation of information operations is that it touches upon the right to freedom of opinion and expression protected by Article 19 of the Universal Declaration on Human Rights and Article 19 of the International Covenant on Civil and Political among other binding instruments. The line of what is permissible under this right is thin as anyone can use the informational space to spread a narrative. The limit is incitement to hatred, which is prohibited by Article 20 of the International Covenant on Civil and Political Rights, as well as defamation or hate speech, as following:

> '1. Any propaganda for war shall be prohibited by law.
>
> 2. Any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence shall be prohibited by law.'

The European Union also has an extensive legal framework and jurisprudence when it comes to protection of freedom of opinion and

[140] Draft Articles on the Responsibility of States for Internationally Wrongful Acts, Report of the International Law Commission on the Work of its Fifty-third Session, UN GAOR, 56th Sess, Supp No 10, p 43, UN Doc A/56/10 (2001).

expression.[141] Defamation and hatred propaganda are thus already restricted by the international human rights legal framework. If within these margins, the right to freedom of opinion and expression is militarized, some argue that laws prohibiting hate speech could also be the foundations to regulate information warfare.[142]

The emergence and mainstreaming of social media have been conducive of deep changes of the militarization of social media and the Internet. Indeed, they became a crucial battlefield for the dissemination of information as anyone can use them, publish and share content. The Russo-Ukrainian war is particularly illustrative on this point. There is a significant evolution in the strategic use of media by the Russian Federation between 2008 and 2014.[143] Indeed, during the Russo-Georgian war, the Russian Federation used information control mainly through television channels. With daily interviews, the Russian Federation controlled the flow of information, framed narratives of the Russian army's efforts to free the oppressed Russians of Georgia and propagandized the atrocities perpetrated by the Georgian army.[144] It is interesting to note that new technologies were not the primary broadcast source of diffusion in this armed conflict whereas two years before, the Internet was a key element for Hezbollah to spread anti-Israeli information during the second Lebanon war.[145] Indeed, Hezbollah used a diverse source of broadcasting from the radio and television to the multitude of websites in Arab, Hebrew, French and English. It made an extensive use of multilingual websites to circulate pictures and video footage of dead bodies, bombed houses, etc. to show the Israeli armed forces in a bad light. If a non-state armed group like Hezbollah had such a communication strategy online in 2006, it is surprising that the

[141] Sejal Parmer, The Legal Framework for Addressing "Hate Speech" in Europe, *presented in* Addressing Hate Speech in the Media: The Role of Regulatory Authorities and the Judiciary, in the International Conference Organized by Council of Europe in Partnership with the Croatian Agency for Electronic Media (Nov. 6–7, 2018). Available at: https://bit.ly/3JA3YuM
[142] David Streckfuss. Truth on Trial in Thailand: Defamation, treason and lèse-majesté. (1st ed.). Routledge. (2010).
[143] Emilio Iasiello. "Russia's Improved Information Operations: From Georgia to Crimea" *Parameters 47*. No. 2. (2017).
[144] *Ibid.*
[145] Clarke, C. (2017)"How Hezbollah Came to Dominate Information Warfare". *The Rand Blog.* September 19, 2017. Available at: https://www.rand.org/blog/2017/09/how-hezbollah-came-to-dominate-information-warfare.html

Russian Federation did not give priority to this media in 2008. As early as 1999, President Putin acknowledged the Russian Federation's relative failure to modernise its information dissemination strategy, as compared to states which had already deployed the Internet for such purposes.[146] Accordingly, the Russian Federation was disadvantaged during the Russo-Georgian war, when Hezbollah expanded its strategies to the world of social media.

Although Georgia is a small country with low military capabilities compared to the Russian Federation, the results of the Russo-Georgian war were mitigated. Both sides of the armed conflict consider they lost the information war, 'either because they had failed to understand the emerging media environment, had sent the wrong messages at the wrong time, or, in the Georgian's case, they could not sustain the information war long enough to win the conditions on the ground were so much against Tbilisi'.[147] The lesson was learnt for the Russian Federation, which adapted its strategy when occupying Crimea in 2014. The Kremlin moved its informational 'troops' to social media like other states, to make information more accessible, widely diffuse and open.[148] The United States Intelligence Community published a report revealing the activities of the Internet Research Agency, a Russian company engaged in online influence operations on behalf of Russian business and political interests.[149] The 'troll farm' comments on Russian actions in Ukraine using fake accounts, discussion forums, comments section of online newspaper, etc.[150] This army of troll accounts are used to propagate anti-Ukrainian narratives and support pro-Russian content promoting their interests on the territory of Ukraine since 2014.

---

[146] Goble, P. "Russia: Analysis from Washington—A Real Battle on the Virtual Front," *Radio Free Europe/Radio Liberty*. (1999).
[147] Paul Goble. "Defining Victory and Defeat: The Information War between Russia and Georgia". in Svante Cornell & Frederick Starr. *The guns of August 2008: Russia's War in Georgia.* (Armonk, New York. 2009).
[148] *Ibid.*
[149] Priestap, Bill. 2017. ″Assessing Russian Activities and Intentions in Recent Elections″ *fbi.gov.* 21 June 2017.
[150] Jared Prier. "Commanding the Trend: Social Media as Information Warfare″. *Strategic Studies Quarterly.* Vol 11. No. 4 (2017) pp 50–85.

These examples reveal a significant militarization of social media and internet platforms, which should be regulated both for the protection of freedom of expression and opinion and for the prevention of bellicose practices.[151] Recent political developments have led the international community to take more and more steps towards information regulation. In March 2022, the United Nations Human Rights Council adopted a non-binding but symbolic resolution recognizing the negative impact of disinformation on the enjoyment and realization of human rights during its forty-ninth session.[152] It emphasizes that disinformation can be 'designed and spread so as to mislead, and to violate and abuse human rights, […] including in times of emergency, crisis and armed conflict, when such information is vital'. Amidst the negotiations of sanctions against the Russian Federation, the High representative of the European Union for Foreign Affairs and Security Policy told the European Parliament that he would propose a new sanction mechanism against malign disinformation.[153] However, no further steps were to be observed since March 2022. This could go along with a code of conduct for media agencies to prevent and criminalize the dissemination of hate speech, misinformation or disinformation online, just like the document that the European Union negotiated with information technology companies in 2016, or with an international agreement.[154]

B. The Long and Persisting Road to Regulation in Armed Conflicts

Despite the overlap with other branches of international law, the grey zones of information warfare still need to be clarified to better protect civilians. There are a growing number of calls for regulation of information operations (i). A question is still pending: how to move forward? (ii)

[151] Ibid, p. 933
[152] Human Rights Council resolution 49/21. *Role of States in countering the negative impact of disinformation on the enjoyment and realization of human rights*. A/HRC/RES/49/21. (2022).
[153] Emmott, R. 2022. "EU to propose sanctions regime against disinformation". *Reuters.* 8 March 2022. Available at: https://www.reuters.com/world/eu-propose-sanctions-regime-against-disinformation-2022-03-08/
[154] European Commission, The EU Code of conduct on countering illegal hate speech online.

i. The Intensification of the Calls for Regulation

The regulation debate has gained a growing interest at the United Nations in the late 1990s. This timing could be explained by the mainstreaming of the Internet occurring at the same period with the rise of instant communication, browsers and websites. At the time, the Russian Federation tabled a resolution at the United Nations General Assembly to recognize that information and telecommunications could be used for purposes, which are inconsistent with the objectives of maintaining international stability and security, and therefore to propose an international legal regime.[155] The resolution did not receive enough support to be adopted. Yet, the General Assembly adopted a resolution to promote multilateralism to counter threats to information security shortly after.[156] This is interesting to note that one of the first states to push for an international code of conduct on information operations is now one of the most fervent users of this type of warfare.

In 2004, the United Nations established six groups of governmental experts in charge of studying the threats posed by the use of information and communications technologies in the context of international security. In 2015, the Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security namely recalled that 'established international legal principles, including, where applicable, the principles of humanity, necessity, proportionality and distinction' as a shy step to prepare the ground for regulation.[157] The next report will be published in 2025 and could contain more pressing paragraphs considering the increasing presence of hate speech, disinformation and misinformation both in peacetime or wartime. The United Nations Secretary-General also regularly publishes reports reinforcing awareness and the political will of states. In 2018, he launched the

[155] United Nations General Assembly draft resolution 53/L.17. *Developments in the field of information and telecommunications in the context of international security.* A/C.l/53/L.17. (1998).
[156] United Nations General Assembly 53/70. *Developments in the field of information and telecommunications in the context of international security.* Res. A/53/70. (1999)
[157] United Nations General Assembly, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/70/174.

Agenda for Disarmament to address the challenge of malicious acts in cyberspace, which contribute to diminishing trust among States.[158] The most recent resolution on the matter was adopted in 2020 by the United Nations General Assembly and underlines the evolution of the position of this international organization organ as follows:

> 'Expressing concern that a number of States are developing information and communications technology capabilities for military purposes and that the use of information and communications technologies in future conflicts between States is becoming more likely,
> Stressing that it is in the interest of all States to promote the use of information and communications technologies for peaceful purposes and to prevent conflicts arising from the use of information and communications technologies.'[159]

This new resolution emphasizes even more the need to address the belligerent use of information and communication technology. This text is a step forward to complete the triptych prevent-promote-protect, which misses the first part.

ii. The Attempts of Weapons Reviews

The rapid technological progress necessarily leads to new means and methods of warfare, that international humanitarian is slow to regulate. When studied, developed, acquired or adopted, new weapons, means or method of warfare must be under scrutiny as provided by Article 36 of Additional Protocol I of 1977. This article aims at preventing the use of weapons which would violate international humanitarian law before this type being operated. The 'weapons' of Article 36 is technology neutral as it is about 'means and methods'. States are 'under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by this Protocol or by any other rule of international law applicable'.[160] Article 36 therefore

[158] United Nations (2018). *"Securing our common future: An agenda for Disarmament"*. Office for Disarmament Affairs, New York.
[159] United Nations General Assembly 75/240. *Developments in the field of information and telecommunications in the context of international security*. A/RES/75/240. (2020).

[160] Protocol I to the Geneva Conventions. Art 36. (1977).

places the responsibility on the states to evaluate whether their technological development of armaments would go against international humanitarian law to ensure that this legal framework remains relevant.

The terminology is complex because of the absence of definition of 'weapons', 'means' and 'methods' of warfare. Lieutenant Colonel McClelland argues that means of warfare are not necessarily weapons, but encompass instead items of equipment, which have a direct impact on the military capabilities citing the example of a mine clearance vehicle.[161] He states that it would "reasonably fall within the scope of the term "means or methods of warfare" as providing a direct contribution to the offensive capability of a military force". Therefore, even though international humanitarian law does not recognize information operations as an attack or the non-lethal damages caused by them, this definition enables to include non-weapon items. Similarly, Professor O'Connell denounces a simplistic approach of weapons reviews. According to her, technology should not be above the law when it significantly contributes to the conduct of hostilities. This is a view that the International Committee of the Red Cross also shares.[162] In 2019, the United Nations Secretary General Antonio Guterres also addressed the World Economic Forum stressing the need for 'a minimum of consensus in the world on how to integrate these new technologies in the laws of war that were defined decades ago in a completely different context'.[163] There is an increasing trend to shift the narrative and establish a review of 'technologies of warfare' instead of the 'means of warfare'. Professor O'Connell proposes four criteria to determine if an equipment item should be subjected to such a review: (i) the lack of compliance with international law; (ii) intended use within the critical military infrastructure; (iii) the action-ability of the information to military decision-making and operations; and (iv) the intended use in the conduct of hostilities.[164]

---

[161] Justin McClelland. "The Review of weapons in accordance with Article 36 of Additional Protocol I". *International Review of the Red Cross.* Vol. 85. No. 850. (2003). p.405.
[162] Vincent Bernard. "Editorial: Science cannot be placed above its consequences". *International Review of the Red Cross.* Vol 94. No. 886. (2012).
[163] World Economic Forum (2019) "António Guterres: Read the UN Secretary-General's Davos Speech in Full", World Economic Forum. 24 January 2019.
[164] Klaudia Klonowska. "Shifting the narrative: not weapons, but technologies of warfare ». *Humanitarian Law & Policy.* International Committee of the Red Cross. (2022).

Information operations are matching all the proposed criteria. The idea of a compliance mechanism was brought forward with Article 36 in 1999 and 2003 at the International Conference of the Red Cross, but did not gather enough support among state parties.[165] Although several states established their own mechanisms, it still lacks in effectiveness and the idea of a common mechanism still appears to be politically impossible. Therefore, civil society has an important role to play in creating a culture of review.[166]

Taking a technology-specific approach, new weapons, means and methods have not always passed this review successfully because they may be deemed to be excessively injurious or to have indiscriminate effects.[167] Just like environmental modifications techniques or blinding laser weapons, some scholars already discussed the option of a ban on information warfare or at least, some sort of control over the hostile use of information means in the 2000s.[168] Such ban would prohibit the development, possession, transfer or use of information warfare capabilities. This approach has the advantage to provide clear norms for the conduct of hostilities. This technology-specific regulation solely applies to the technology explicitly targeted in the convention. This approach will take into account strategic considerations in addition to the protection of civilians, such as at the cost of the technology acquisition. Yet, it seems to be still difficult to agree on what the specific means of information warfare are.[169] Hence, a technology-neutral law focuses on the effects of these weapons technology, which could be a way to solve the issue.[170] This difficulty is adding up to other ones, such as the rapid technology diffusion and its dual use making the enforcement of such ban complicated. It also seems premature

[165] Kathleen Lawand, 'Reviewing the legality of new weapons, mean and methods of warfare', *International Review of the Red Cross.* Vol. 88, No. 864. (2006). p. 926.
[166] International Committee of the Red Cross. "A Guide to the Legal Review of New Weapons, Means and Methods of Warfare". 2006. Available at: http://www.icrc.org/eng/assets/files/other/icrc_002_0902.pdf
[167] Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons, which may be deemed to be excessively Injurious or to have Indiscriminate Effects. (2003).
[168] David Elliott, Lawrence Greenberg, Kevin Soo Hoo. "Strategic Information Warfare: A New Arena for Arms Control?" *Center for International Security and Cooperation.* (1997).
[169] Lawrence Greenberg, Seymour Goodman, Kevin Soo Hoo. 'Information Warfare and International Law', *National Defense University Press.* (1998).
[170] Rain Liivoja. "Technological change and the evolution of the law of war" *International Review of the Red Cross.* Vol. 97. No 900. (2015).

to ban information warfare when international humanitarian law does not recognize its damages outside of lethality; neither qualify information operations as an attack or the use of the force. A compromise could be reached by agreeing that information warfare techniques should not interfere with command and control of strategic weapons or disrupt missile attack warning systems. Such an agreement would already enable to limit the scope of information warfare.[171]

C. Safeguarding International Humanitarian Law Principles

Customary international law could give momentum to answer the grey zones left by contemporary practices of information warfare (i) and rethink the information space (ii).

i. Giving a new momentum to Customary International Law

Declarations at the United Nations General Assembly are important as they give weight and legitimacy to certain issues, and take part in the development of customary international law. This purposeful influence technique has already been used to establish principles of customary international law by adopting widely supported declarations.[172] In 1998, the Russian Federation did not succeed in gathering enough interest and support for information security. However, the informational environment has known deep upheavals and such a declaration would have better chance to be supported now than in the late 1990s. On the other hand, many states understand the strategic importance of information warfare and would probably prefer to avoid an official recognition of the problem. As a matter of fact, the unfolding Russo-Ukrainian war reminds member states of the threats of information warfare more than ever. In addition, states are also threatened during peacetime as the coronavirus pandemic has been accompanied by a pandemic of misinformation, which has serious social

[171] Philipp Johnson. « Is it Time for a Treaty on Information Warfare? » *International Law Studies*. Vol 76. (2002) p.448.
[172] *Ibid*. p.452.

consequences around the world.[173] Opening the floor for discussions at the international level could lead to the emergence of norms on certain aspects of information warfare, such as the recognition of intangible harm or non-kinetic form of 'attack' related to information.

Another alternative would be a codification of the scholarly consensus on certain rules. This would not be the first time in history that academics and other experts gather to put on the paper international consensus of the interpretation of treaties. This was the case of the International Institute of Humanitarian Law gathering between 1988 and 1994 to create the San Remo Manual on International Law Applicable to Armed Conflicts at Sea.[174] This is what the NATO Cooperative Cyber Defence Centre of Excellence tries to achieve with the re-edition of the Tallinn Manual on the interpretation of international humanitarian law for cyberwarfare. The International Committee of the Red Cross also takes part in the development of law with commentaries and interpretations, with the Study on Customary Law and Interpretive Guidance on the Notion of Direct Participation in Hostilities.[175] Although this approach produces non-binding documents, they are symbolically powerful instruments.

ii. Rethinking the Information Space

The core development of international humanitarian law occurred in the aftermath of World War II, anchoring the 1949 four Geneva Conventions in kinetic and traditional means of war. The International Committee of the Red Cross made commentaries and the judicial bodies provided valuable interpretations of international humanitarian law. Yet, the legal corpus seems to be slow to evolve whereas it has new challenges to foresee like information warfare or autonomous lethal weapons. International humanitarian law rarely regulate or prohibit a new mean or method of warfare before it becomes

[173] Forum on Information & Democracy (2020) « Working Group on Infodemics: Policy Framework ».
[174] San Remo Manual on International Law Applicable to Armed Conflicts at Sea. (1994)
[175] ICRC, Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law. Available at: https://shop.icrc.org/interpretive-guidance-on-the-notion-of-direct-participation-in-hostilities-under-international-humanitarian-law-pdf-en.html

operational.[176] The phenomenon of 'one war behind reality' should be avoided by adjusting law to the development of new technologies through evolving interpretation of international humanitarian law.[177] The hybrid nature of conflict is one of these challenges as the objectives of war have changed to subvert and influence rather than defeat the adversary. Although the employed methods do not necessarily have physical consequences, they deeply affect civilians and the society structure as a whole.

So far, two trends should be noted. On the first hand, there are increasing calls from academia to engage with the matter and public statements of states on cyber operations and international law. On the other hand, there is also a growing approach of the states to counter any information operations with wide-scale information operations to disseminate their own narratives while remaining silent about any qualifications.[178] Several factors call for a rapid settlement on this issue. First, information operations promise to be all the more invasive and harmful in considering the growing digitalization of societies, which has been accelerated by the coronavirus pandemic. Second, the line between war and peace becomes more and more blurry with bellicose information operations deteriorating interstate relations in peacetime and societal stability. This might call for rules to regulate and delimit the spectrum of what is permissible for the protection of civilian information spaces.

It is important to note that the applicability of international humanitarian law does not bring a ground of legitimacy to the use of hostile information operations. Indeed, the first Additional Protocol to the Geneva Conventions remains the same and this legal corpus should not be 'be construed as legitimizing or authorizing any act of aggression or any other use of force inconsistent with the Charter of the United Nations', nor encouraging the

[176] ICRC, 'Fundamentals of IHL: Concept and Purpose of International Humanitarian Law'. Available at: https://casebook.icrc.org/law/fundamentals-ihl#_ftn_059.
[177] M. Conde Jiminián, "The Principle of Distinction in Virtual War: Restraints and Precautionary Measures under International Humanitarian Law". *Tilburg Law Review*. Vol. 15. n° 1 (2010)
[178] European External Action Service "EU vs. Disinfo" initiative, available at: https://euvsdisinfo.eu/.

militarization of the information space, but rather emphasizing the importance of preventing harm.[179]

The two experts Geiss and Lahmann proposes a 'safe digital haven' to overcome the problems related to the principle of distinction and to better protect civilians.[180] Indeed, as early as 2012, they advocated for a demilitarized zone in the scope of Article 60 of the first Additional Protocol to the Geneva Conventions to protect civilians from cyber operations. Applying this idea to information warfare, it would prohibit any attack on or use of the networks and information systems designated as the demilitarized zone for military purposes.[181] This would enable to segregate completely military and civilians cyber infrastructure because parties would have to reach an agreement on the infrastructure, which could not be used for military purposes. It would also prevent the use of civilian systems as a strategic back-up option. Such delimitation should rely on what services or systems are essential to the civilian population.

Conclusion

Information warfare has always existed as parties to a conflict have always looked to justify and foster war effort, demonise and delegitimise the adversaries. Indeed, during armed conflicts, the narrative is of outmost importance. A shift occurred with the development of information and communication technologies, with new opportunities and challenges for broadcasting information at a wider scale and in a personalised way with smartphones. International law lays down legal obligations upon states and restrict some practices, such as war propaganda, to regulate some aspects of the use of information for belligerent purposes.

International humanitarian law is challenges by the intangibility of information warfare. The legal corpus aims at regulating traditional kinetic

[179] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977. Preamble.
[180] Robin Geiss, Henning Lahmann. "Cyber warfare: applying the principle of distinction in an interconnected space". *Israel Law Review*. Vol 45. No 3. (2012). pp. 381-399.
[181] *Ibid.*

attacks and reducing physical damages to civilians. International humanitarian law recently started to recognise that an attack could take intangible form because of the necessity to regulate cyberwarfare. Information and communication technologies bring new opportunities for the dissemination of information with deep fakes or instant messages. The conducts stemming from this technological development is covered by international humanitarian law. After examination of relevant rules, belligerent manipulation of information falls into the scope of the prohibition of perfidy, terror or incitement to violence in breach with law. These three prohibitions cover immaterial harm inflicted upon civilians. It could be the opportunity for international humanitarian law to formally recognise the potential severity of information operations' damages and to rethink the concept of an 'attack' under this legal framework. The second major characteristics of information warfare challenging the application of this legal framework is the interconnectedness of information networks, rendering difficult to apply the principle of distinction and determine whether what military objectives are. This interconnectedness is problematic because it make civilians vulnerable. States should opt for the segregation of military and civilian infrastructure.

International humanitarian law applies to contemporary information warfare, but some practices require courts to take a stance to fill in the gaps and clarify the interpretation, which should be given. If states adopt a narrow interpretation of their obligations under international humanitarian law, then there will be significant gaps in the protection of civilians. New rules and interpretations would be useful to avoid over-militarisation of the information space and that belligerents do not take advantage of what would become a grey area. After this last part on questioning the ways to regulate information warfare, it is important to re-centre the debate on what really matters. International humanitarian law was born from the will to protect civilians from armed conflicts and limit the number of casualties. When interpreting treaties, there are a variety of approaches, including the original intent approach and the evolutionary approach. The first one would interpret the treaty following the intent of the founders of the treaty, i.e. protecting civilians, while the second one would identify the common will of the parties considering the evolving

circumstances since the negotiation of the treaty. The case law of the International Court of Justice argues that such an interpretation is allowed if it can be inferred from the terms of the treaty that such evolution is possible.[182] In both approaches, the objective would be to maximise the protection of civilians. It should not be lost sight of when commenting international humanitarian law, interpreting and reinterpreting its legal corpus to avoid over-militarisation of the civilian information space.

Seeing the contemporary practices of information warfare and the widespread damages these practices can cause, it appears that international humanitarian law should protect the information space as such. Humanitarian values should evolve to contemporary values, which would be sensitive to technological development and include the notions of 'integrity of national or global information spaces' or 'public trust'.[183] These steps will make a difference in the symbolic value of international humanitarian law as well. Indeed, this legal corpus would be providing either a full-scale protection against all threats in war, including the new and emerging ones linked to the use and manipulation of information for belligerent purposes, or a sole protection against the worst threats.

In the meanwhile, information warfare acts as a vector and a factor weakening even more fragile contexts and increasing harm inflicted to civilian. This makes humanitarian assistance all the more important, but mangled. International humanitarian law provides protection to humanitarian actors through several articles of the fourth Geneva Convention, both Additional Protocols to the Geneva Conventions and customary international law. Humanitarian action relies on three pillars, which are integrity, availability and confidentially, which can be affected by information warfare for diverse reasons. The International Committee of the Red Cross offers an extensive literature on the impact of information warfare on these three pillars. Firstly, certain practices, such as disinformation, can contribute to reputational damage

[182] Pierre-Marie Dupuy, "Part II Interpretation of Treaties, 7 Evolutionary Interpretation of Treaties: Between Memory and Prophecy", in *The Law of Treaties Beyond the Vienna Convention.* Oxford Scholarly Authorities on International Law. 17 February 2011.
[183] Lahmann, H. (2022) "Protecting the Global Information Space in Times of Armed Conflict". *International Review of the Committee of the Red Cross*. No. 915.

or security risks of the humanitarian organizations or personal.[184] Integrity and accuracy of humanitarian work can be easily undermined by information operations. Its availability and confidentiality are also at risk facing denial-of-service operations or other cyber operations.[185]

Another way to bring a better protection to civilians in conflict would be doing it through international human rights law, which applies in both wartime and peacetime. Looking at the Human Rights Council resolutions for the past ten years, it is to be noticed that the number of resolutions on new and emerging technologies in relation to human rights has significantly increased. The right to information is indirectly addressed through the resolution on the safety of journalists stating that Article 19 on the right to freedom of expression includes

> 'the right to seek, receive and impart information held by public authorities, subject only to any restrictions that fully comply with international law, and stressing the importance of freedom of access to information to the work of journalists and media workers, and that they themselves also play a critical role in the enjoyment of this right'.[186]

In 2022, the Human Rights Council adopted a resolution on disinformation for the first time since its creation in 2008. The resolution focuses on the role of states in countering the negative impact of disinformation on the enjoyment and realization of human rights. It recognised

> 'the importance of the accessibility and availability of information and means of communication, as well as information and communications technology, systems and formats, to ensuring that all persons, in all their diversity, including persons with disabilities, are able to enjoy their right to freedom of expression, including the freedom to seek, receive and impart information, on an equal basis with others, without which persons with disabilities may be at an increased risk of the negative impact of disinformation'.

[184] Massimo Marelli. "Hacking humanitarians: Defining the cyber perimeter and developing a cybersecurity strategy for international humanitarian organizations in digital transformation". *International Review of the Red Cross*. No. 913. (2021).
[185] Massimo Marelli, Adrian Perrig. "Hacking humanitarians: mapping the cyber environment and threat landscape" *Humanitarian Law & Policy.* International Committee of the Red Cross. (2020).
[186] Human Rights Council resolution 49/4. Situation of human rights in the Democratic People's Republic of Korea. A/HRC/49/L.4 (2022)

The right to information *per se* is not recognised although pushed forward by civil society organizations, such as Article 19 or Transparency.org. The implication of this formal recognition for international humanitarian law could be significant for the protection of civilians in armed conflicts as it would reinforce the efforts made so far by the international community to counter hate speech, disinformation and other forms of information manipulation for belligerent purposes. This could lead to the recognition of information and communication infrastructure as essential for the civilian population, which would be formally and firmly unlawful targets.

Technological development is neither good, nor bad as long as its use and purpose aligned with existing legal frameworks and values. In particular, information and communication technologies have given new possibilities for warfare, making the war narratives more dangerous and more intrusive into the civilian space. The flooding of information, with shocking images and videos designed to be viral, leads to a 'compassion fatigue'. As the audience becomes less and less receptive, it does not foster humanitarian action as it used to be while humanitarian organisations often rely on the power of images to convince donors and find funds. It also results in a public crisis of legitimacy from mainstream media.[187] On the other hand, more and more initiatives are taken to educate people into examining the sources of information and train critical thinking.

Waiting for the momentum on information warfare, there is a significant individual and collective trauma to address among the civilian population and future traumas to prevent due to information operations. It is the case of the Baltic countries, which were the target of hybrid operations in the recent years. Indeed, the countries have been victims of Russian disinformation through the growing of Russian-speaking websites for instance.[188] In the absence of express legislative protection, states have started to address the problem of psychological harm caused by information warfare through a comprehensive

[187] Andrew Hoskins, "Media and compassion after digital war: Why digital media haven't transformed responses to human suffering in contemporary conflict". *International Review of the Red Cross* (2020), Vol 102. No 913. pp 117–143.
[188] Król, A. 2017. « Russian Information Warfare in the Baltic States — Resources and Aims". The Varsaw Institute Review. 20 July 2017.

policy framework, including educational training instead of security and defence monitoring. However, fighting hostile information operations is a double edged sword as domestic laws on countering disinformation should not be too broad not to fall into the scope of censorship. Information is intangible and borderless, calling for an international answer. After nearly thirty years of discussions, it is time to make a decision on the future of the information space amidst the constant chaos of information fuel by hostile state relations.

List of figures

Content warnings: explicit violence and death, harm to a child, war.

Figure 1: Results of Google Trends when searching for “hybrid warfare” with the parameters “worldwide”, “news” and “from 2004 to today” showing the distribution of google searches of this term as well as the associated searches.

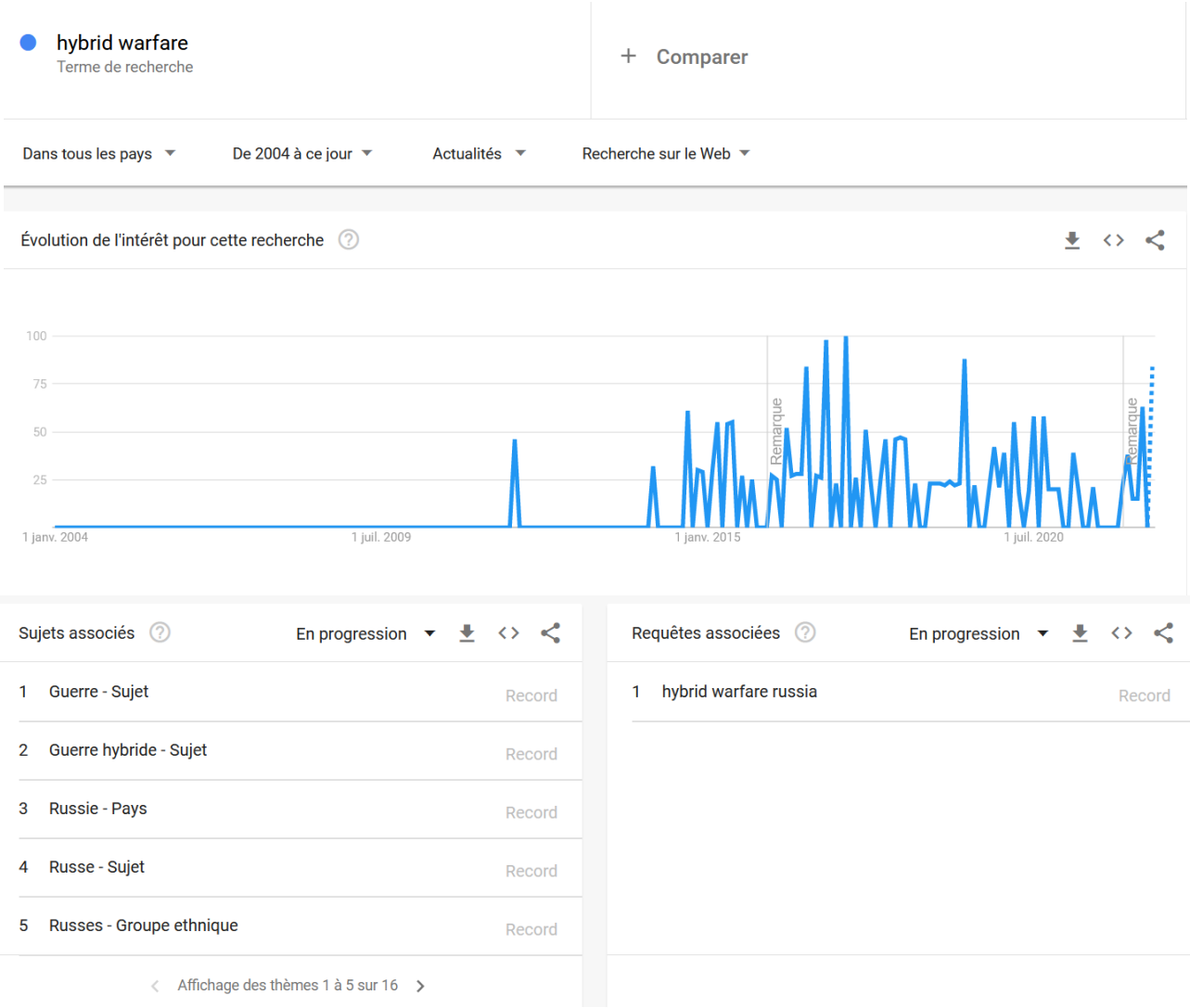


Figure 2: Photograph of burning buildings in Beirut during an Israeli air raid on the 5th August 2006 (left), manipulated version of the same photograph (right)

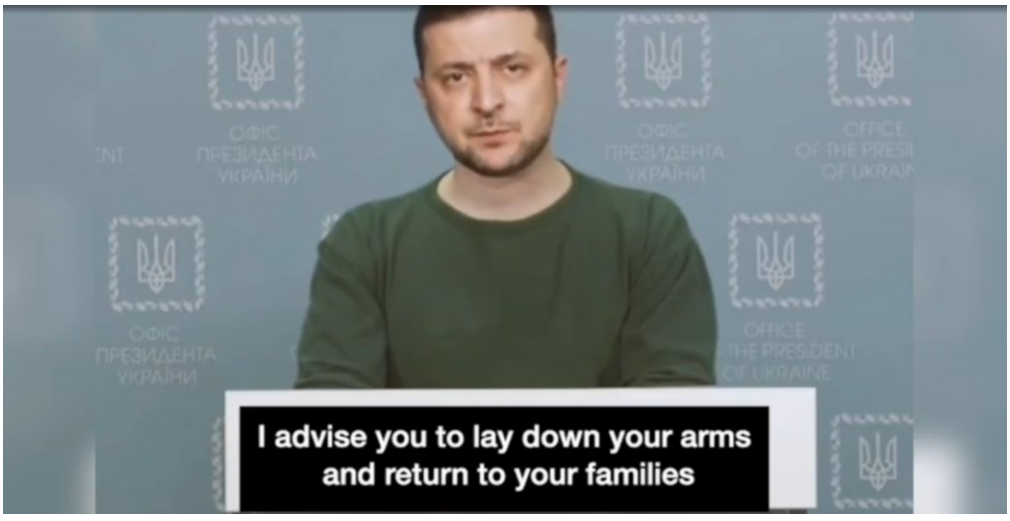
Credits: Hajj, Adnan. Photographs. Used in: Aspan, M. "Ease of Alteration Creates Woes for Picture Editors". *The New York Times.* 14 August 2006. https://www.nytimes.com/2006/08/14/technology/14photoshop.htm

Figure 3: Rescue workers carrying dead children after the Israeli missile strike in Kana on the 30th July 2006.

Credits: Nasser & Frayer, K. Associated Press. Photographs. Used in: The Associated Press. "Veracity of news photos in Lebanon questioned". *Nbcnews.* 2nd August 2006.

Figure 4: Deep fake video of the Ukrainian President Zelensky.

« Dear Ukrainians, dear defenders, it has not been easy to be the president. I have to make difficult decisions. First I decided to get us back Donbas. It is time to face the truth. It didn't work out. It only got worse, much worse. There is no more future, At least for me. And now I'm taking another hard decision to say goodbye to you. I advise you to lay down your arms and return to your families. You shouldn't die in this war. I advise you to live, and I'm going to do the same."



Credits: Miller, Joshua R. Deepfake video of Zelensky telling Ukrainians to surrender removed from social platforms. *The New York Times.* 17 March 2022.

https://nypost.com/2022/03/17/deepfake-video-shows-volodymyr-zelensky-telling-ukrainians-to-surrender/

Bibliography

Legal sources:

Additional Protocol to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts. Preamble, Art. 36, Art 48, Art 49(1), Art 51, Art 52(2), Art 56, Art 57(1) (1977)

Convention (IV) respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land. The Hague. Annex to the Convention: Regulations respecting the laws and customs of war on land - Section II: Hostilities - Chapter II: Spies - Regulations: Art. 31. (1907).

Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons, which may be deemed to be excessively Injurious or to have Indiscriminate Effects. (2003).

Draft Articles on the Responsibility of States for Internationally Wrongful Acts, Report of the International Law Commission on the Work of its Fifty-third Session, UN GAOR, 56th Sess, Supp No 10, p 43, UN Doc A/56/10 (2001).

Draft Articles on the Responsibility of States for Internationally Wrongful Acts. Commentaries. Art. 6, §3 (2001).

Final report to the Prosecutor by the Committee Established to Review the NATO Bombing Campaign Against the Federal Republic of Yugoslavia, June 13, 2000, PR/P.I.S./510-E. Available at: http://www.icty.org/sid/10052#IVB4

Geneva Conventions. Common Art 1. (1949).

Human Rights Council resolution 45/18 (2020) *The safety of journalists*, A/HRC/RES/45/1.

Human Rights Council resolution 49/4. *Situation of human rights in the Democratic People's Republic of Korea*. A/HRC/49/L.4 (2022)

Human Rights Council resolution 49/21. *Role of States in countering the negative impact of disinformation on the enjoyment and realization of human rights*. A/HRC/RES/49/21. (2022).

International Criminal Court. *Prosecutor v. Dusko Tadic a/k/a 'Dule'* Decision on the defence motion for Interlocutory appeal on jurisdiction. 1995. §120.

International Criminal Tribunal for Rwanda. *The Prosecutor v. Georges Ruggiu*. 2000. §50.

International Criminal Tribunal on the former Yugoslavia. *The Prosecutor v. Galić*: A. Trial Chamber, Judgement and Opinion, 1998. §91–137, 208–597.

International Criminal Tribunal for the former Yugoslavia. Final report to the Prosecutor by the Committee Established to Review the NATO Bombing

Campaign Against the Federal Republic of Yugoslavia. 13 June 2000. Available at: http://www.icty.org/sid/10052#IVB4

International Committee of the Red Cross Commentary on the Additional Protocols of 8 June 1977. §2024

International Covenant on Civil and Political Rights. Art 20. (1966).

International Committee of the Red Cross Study on Customary International Humanitarian Law Database, Practice Relating to Rule 2. Violence Aimed at Spreading Terror among the Civilian Population, Practice Relating to Rule 14. Proportionality in Attack; Rule 20. Advance Warning. Rule 57. Ruses of war. Rule 74. Chemical weapons.

International Telecommunication Union, International Telecommunication Convention. Art 35. (1982).

San Remo Manual on International Law Applicable to Armed Conflicts at Sea. (1994)

Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Rule 92 §8, Rule 93 §5, Rule 105., Rule 122 §2 §5 §7(2017).

United Nations General Assembly draft resolution 53/L.17. *Developments in the field of information and telecommunications in the context of international security.* A/C.l/53/L.17. (1998).

United Nations General Assembly 53/70. *Developments in the field of information and telecommunications in the context of international security.* Res. A/53/70. (1999)

United Nations General Assembly 75/240. *Developments in the field of information and telecommunications in the context of international security*. A/RES/75/240. (2020).

United Nations Security Council resolution 2222 (2015). *On protection of journalists and associated media personnel in armed conflict.* S/RES/2222

United Nations Security Council resolution 1738 (2006) S/RES/1738.

Vienna convention on the law of treaties. Article 31. (1969).

Other sources:

AFP. 'Israeli 'hackers' target Hezbollah TV'. *Aljazeera.* 2 August 2006. https://www.aljazeera.com/news/2006/8/2/israeli-hackers-target-hezbollah-tv.

John Arquilla and David Ronfeldt, eds., In Athena's Camp: Preparing for Conflict in the Information Age. Santa Monica, CA: RAND Corporation. (1997).

Marie Baezner, Patrice Robin. « Cyber and information warfare in the Ukrainian conflict ». *Center for Security Studies.* (2018)*;*

Alexandre Balguygallois, « Protection des journalistes et des médias en période de conflit armé ». *International Review of the Red Cross*. Vol. 86, No. 853. (2004). pp. 37-68; https://casebook.icrc.org/case-study/protection-journalists.

Vincent Bernard. 'Editorial: Science cannot be placed above its consequences'. *International Review of the Red Cross.* Vol 94. No. 886. (2012).

Janis Berzins. 'Russia's New Generation Warfare in Ukraine: Implications for Defense Policy', *Military Operations*. Vol 2. No. 4. (2014). pp 4-7.

William Boothby. 'Some legal challenges posed by remote attack'. *International Review of the Red Cross.* Vol. 94. No. 886. (2012).

Brunetti-Lihach, N. (2018). 'Information Warfare Past, Present, and Future'. *The Strategic Bridge*. November 14, 2018. https://thestrategybridge.org/the-bridge/2018/11/14/information-warfare-past-present-and-future.

Byrne, J. 2022. 'Deepfakes now a political weapon in the Ukrainian war'. *Thred.* 18 March 2022. https://thred.com/tech/deepfakes-now-a-political-weapon-in-the-ukrainian-war/

Center for Strategic & International Studies (2022) 'Russia's Crackdown on Independent Media and Access to Information Online'. *Center for Strategic & International Studies.* March 30, 2022.

von Clausewitz, C. *Vom Kriege*, Book 1, Chapter 3. « Nebel des Krieges". (1832).

Clarke, C. (2017)"How Hezbollah Came to Dominate Information Warfare". *The Rand Blog.* September 19, 2017. Available at: https://www.rand.org/blog/2017/09/how-hezbollah-came-to-dominate-information-warfare.html

Cohen, L. (2022) 'The new era of disinformation wars'. *Voelkerrechts blog.* 30 November 2020. https://voelkerrechtsblog.org/de/the-new-era-of-disinformation-wars/

Colonel S. G. Chekinov (Res.), Lieutenant General S. A. Bogdanov (Ret.), 'The Nature and Content of a New-Generation War,' *Military Thought* (2013).

Congressional Research Service Report for Congress. *Lebanon: the Israeli-Hamas-Hezbollah Conflict*, Congressional Research Service, The Library of Congress. (2006).

George Curtis. *The Law of Cybercrimes and their investigations.* CRC Press, Taylor & Francis Group. (2012). p.27.

Current Time. (2022) 'Court bans publication of information on Russian Military death toll in Ukraine'. *Radio Free Europe.* June 7, 2022.

M, Dixon. *Cases & Materials on International Law.* Oxford University Press. (2016).

David Elliott, Lawrence Greenberg, Kevin Soo Hoo. 'Strategic Information Warfare: A New Arena for Arms Control?' *Center for International Security and Cooperation.* (1997).

Pierre-Marie Dupuy, "Part II Interpretation of Treaties, 7 Evolutionary Interpretation of Treaties: Between Memory and Prophecy", in *The Law of Treaties Beyond the Vienna Convention.* Oxford Scholarly Authorities on International Law. 17 February 2011.

Emmott, R. 2022. 'EU to propose sanctions regime against disinformation'. *Reuters.* 8 March 2022. Available at: https://www.reuters.com/world/eu-propose-sanctions-regime-against-disinformation-2022-03-08/

European Commission, The EU Code of conduct on countering illegal hate speech online.

European Court on Human Rights. 'Guide on Article 2 of the European Convention on Human Rights: Right to Life' Updated on the 31rst December 2021. Available at: case-law

European External Action Service 'EU vs. Disinfo' initiative, available at: https://euvsdisinfo.eu/.

European Parliament. 2005. 'Parliamentary questions: Al-Manar Hizbullah Television' Charles Tannock (PPE-DE), Jana Hybášková (PPE-DE) and Jas Gawronski (PPE-DE) to the Commission 10 March 2005. E-0909/05. Available at: https://www.europarl.europa.eu/doceo/document/E-6-2005-0909_EN.html

Erlanger, S. (2000) 'Rights Group says NATO bombing in Yugoslavia violated law'. *New York Times.* June 8, 2000.

Reuven Erlicj, Yoram Kahati (2007) « Hezbollah as a case study of the battle for hearts and minds ». Intelligence and Terrorism Information Center at the Israel Intelligence Heritage & Commemoration Center.

Morand Fachot. The Media dimension in Foreign Interventions. *Options Politiques.* (2001).

Marina Favaro. 'Weapons of Mass Distortion: A new approach to emerging technologies, risk reduction and the global nuclear order'. *Centre for Science & Security Studies of King's College London.* (2021).

Fecteau, M. (2019). 'Understanding Information Operations & Information Warfare'. *Global Security Review.* 7 January 2019. Updated on 22 June 2022.

Fendel, Hillel. 2006. "Evidence Mounts that Kana "Massacre" Was a Fake". *Arutz Sheva*. 3 August 2006.

Lorenza Fontana. 'Hezbollah vs Israel: Confronting Information Strategies in the 2006 Lebanese War'. *University of Glasgow.* (2010).

Forum on Information & Democracy (2020) "Working Group on Infodemics: Policy Framework".

France24. "Echange de prisonniers entre Israël et le Hezbollah. » *France24.* 16 July 2008. https://www.france24.com/fr/20080716-echange-prisonniers-entre-israel-le-hezbollah-liban-israel

Robin Geiss, Henning Lahmann. 'Cyber warfare: applying the principle of distinction in an interconnected space'. *Israel Law Review*. Vol 45. No 3. (2012). pp. 381-399.

Gunthert, A. 2006. « L'affaire Adnan Hajj: première manipulation emblématique de l'ère numérique » 8 August 2006. *Le blog d'André Gunthert.* Available at : https://archive.wikiwix.com/cache/index2.php?url=http%3A%2F%2Fwww.arhv.lhivic.org%2Findex.php%2F2006%2F08%2F08%2F204#federation=archive.wikiwix.com

Eric Germain. 'Out of sight, out of reach: Moral issues in the globalization of the battlefield'. *International Review of the Red Cross.* Vol. 97. No 900. (2015).

Lawrence Greenberg, Seymour Goodman, Kevin Soo Hoo. 'Information Warfare and International Law', *National Defense University Press.* (1998).

Giles, K. (2011) 'Information Troops – A Russian Cyber Command?' 3rd International Conference on Cyber Conflict.

Goble, P. 'Russia: Analysis from Washington—A Real Battle on the Virtual Front,' *Radio Free Europe/Radio Liberty*. (1999).

Paul Goble. 'Defining Victory and Defeat: The Information War between Russia and Georgia'. in Svante Cornell & Frederick Starr. *The guns of August 2008: Russia's War in Georgia.* (Armonk, New York. 2009).

Laurent Gisel & Tilman Rodenhaüser. 'Cyber operations and international humanitarian law: fives key points'. *Humanitarian Law & Policy.* International Committee of the Red Cross. (2019).

Government of Israel. 2007. 'Behind the headlines: The Second Lebanon War - One year later.' Govt. Israel 12 Jul 2007. Available at: https://reliefweb.int/report/israel/behind-headlines-second-lebanon-war-one-year-later.

Andrew Hoskins, 'Media and compassion after digital war: Why digital media haven't transformed responses to human suffering in contemporary conflict'. *International Review of the Red Cross* (2020), Vol 102. No 913. pp 117–143.

House of Commons Defence Committee, 'Towards the Next Defence and Security Review: Part Two – NATO', (2014). p. 41.

Human Rights Council, Report of Commission of Inquiry on Lebanon pursuant to Human Rights Council resolution S-2/1, A/HRC/3/2, 23 November 2006,

available at http://www.ohchr.org/Documents/Publications/HR_in_armed_conflict.pdf

Human Rights Watch. 'Why They Died, Civilian Casualties in Lebanon during the 2006 War'. Human Rights Watch. (2007).

Emilio Iasiello. 'Russia's Improved Information Operations: From Georgia to Crimea' *Parameters 47*. No. 2. (2017).

Izenberg, D., Siegel-Itzkovich, J, Rosen, N. 2006. "Bloggers raise questions about Kana". *The Jerusalem Post.* 2 August 2006.

International Committee of the Red Cross. A Guide to the Legal Review of New Weapons, Means and Methods of Warfare, January 2006, available at: http://www.icrc.org/eng/assets/files/other/icrc_002_0902.pdf

International Committee of the Red Cross. Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law. 2009. Available at: https://shop.icrc.org/interpretive-guidance-on-the-notion-of-direct-participation-in-hostilities-under-international-humanitarian-law-pdf-en.html

International Committee of the Red Cross. 2019. 'International Humanitarian Law and Cyber Operations during Armed Conflicts'. Position paper submitted to the 'Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security' and the 'Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security'.

International Committee of the Red Cross. 2019. 'International Humanitarian Law and the Challenges of Contemporary Armed Conflicts'. 22 November 2019. p.26-34. Available at: https://www.icrc.org/sites/default/files/document/file_list/challenges-report_new-technologies-of-warfare.pdf.

International Committee of the Red Cross. 2020. 'Humanity after life: Respecting and Protecting the Dead' ICRC. Legal Factsheet.

International Council on Human Rights Policy (2002) *Journalism, Media and the Challenge of Human Rights Reporting*, Switzerland, p.16 quoting Marlise Simons, *Internatinal Herald Tribune* "Trial examines war crimes free speech and journalism" 5 March 2002

The Irish Times. (1999) 'Government stance on NATO bombing of Serbia criticised by opposition' *The Irish Times.* March 26, 1999.

Jackson, S. NATO Article 5 and Cyber Warfare: NATO's Ambiguous and Outdated Procedure for Determining When Cyber Aggression Qualifies as an Armed Attack. *Center for Insfrastructure Protection & Home Security.* August 16, 2016. https://cip.gmu.edu/2016/08/16/nato-article-5-cyber-warfare-natos-ambiguous-outdated-procedure-determining-cyber-aggression-qualifies-armed-attack/

M, Jaintner. “Russian Information Warfare: Lessons from Ukraine” in Geers, K. (2015) *Cyber War in Perspective: Russian Agression against Ukraine*, NATO CCD COE Publications. (2015)

M. Conde Jiminián, “The Principle of Distinction in Virtual War: Restraints and Precautionary Measures under International Humanitarian Law”, *Tilburg Law Review*, Vol. 15, No. 1, 2010.

Philipp Johnson. “Is it Time for a Treaty on Information Warfare?” *International Law Studies*. Vol 76. (2002) p.448.

Khan, I. 2019. “Article 38 of the Statute of the International Court of Justice: A Complete Reference Point for the Sources of International Law?” *The New Jurist.* 5 April 2019. https://newjurist.com/article-38-of-the-statute-of-the-international-court-of-justice.html

Khan, K.. ‘Statement of ICC Prosecutor, Karim A.A. Khan QC, on the Situation in Ukraine: Receipt of Referrals from 39 States Parties and the Opening of an Investigation’. *International Criminal Court. (*2022).

Keating, J. 2022. ‘A gruesome way of accounting’: The politics of body counts in Ukraine’. *Grid News.* 1 April 2022. https://www.grid.news/story/global/2022/04/01/a-gruesome-way-of-accounting-the-politics-of-body-counts-in-ukraine/

Klaudia Klonowska. “Shifting the narrative: not weapons, but technologies of warfare’. *Humanitarian Law & Policy.* International Committee of the Red Cross. (2022).

Król, A. 2017. ‘Russian Information Warfare in the Baltic States — Resources and Aims”. The Varsaw Institute Review. 20 July 2017.

Karl Kushner. ‘Legal and Practical Constraints on Information Warfare’ *The United States Naval War College*. (1996).

Lahmann, H. (2022) “Protecting the Global Information Space in Times of Armed Conflict”. *International Review of the Committee of the Red Cross*. No. 915.

Kathleen Lawand, ‘Reviewing the legality of new weapons, mean and methods of warfare’, *International Review of the Red Cross.* Vol. 88, No. 864. (2006). p. 926.

Rain Liivoja. ‘Technological change and the evolution of the law of war’ *International Review of the Red Cross.* Vol. 97. No 900. (2015).

Herbert Lin “The existential threat from cyber-enabled information Warfare”. Bulletin of the Atomic Scientists. Vol 75, No. 4 (2019). pp 187-196.

Miranda Lupion. The Gray War of Our Time: Information Warfare and the Kremlin’s Weaponization of Russian-Language Digital News, *The Journal of Slavic Military Studies*, Vol 31. No. 3. (2018) pp. 329-353.;

Ben Macintyre. Operation Mincemeat: The True Spy Story that Changed the Course of World War II. London: Bloomsbury. (2010).

Massimo Marelli. 'Hacking humanitarians: Defining the cyber perimeter and developing a cybersecurity strategy for international humanitarian organizations in digital transformation'. *International Review of the Red Cross*. No. 913. (2021).

Massimo Marelli, Adrian Perrig. "Hacking humanitarians: mapping the cyber environment and threat landscape" *Humanitarian Law & Policy.* International Committee of the Red Cross. (2020).

Justin McClelland. 'The Review of weapons in accordance with Article 36 of Additional Protocol I'. *International Review of the Red Cross.* Vol. 85. No. 850. (2003). p405.

Avril McDonald. *Yearbook of International Humanitarian Law - 2003.* Volume 6. Cambridge University Press. 31 December 2006.

Mijatović, D. (2022) 'Not a target – the need to reinforce the safety of journalists covering conflicts: Statement by the Council of Europe Commissioner for Human Rights'. 2 May 2022.

Mishra, S. 2021. 'Deep fakes: the next digital weapon with worrying implications for nuclear policy'. *European Leadership Network.* 3 November 2021. https://www.europeanleadershipnetwork.org/commentary/deep-fakes-the-next-digital-weapon-with-worrying-implications-for-nuclear-policy/

Andrew Monaghan, 'The "War" in Russia's 'Hybrid Warfare'. *Parameters 45*, no. 4 (2015) pp. 65–74.

Williamson Murray, *America and the Future of War.* Standford: Hoover Institution Press. (2017). pp 47-49.

Maria Luisa Nardi, 'Origin of Cyber Warfare and How the Espionage Changed: A historical Overview' in Luisa Dall'Acqua, Irene Maria Gironacci. *Transdisciplinary Perspectives on Risk Management and Cyber Intelligence.* (2020).

NATO. *'*Information warfare*'*. Available at: https://bit.ly/3OTwHMc

NATO (2010) BI-SC Input to a new NATO capstone concept for the military contribution to countering hybrid threats, 25th August 2010, p. 2

NATO StratCom of Excellence (2015) 'Analysis of Russia's Information Campaigns against Ukraine'.

The NATO Cooperative Cyber Defence Center of Excellence. 2020. 'International Cyber Law: Interactive Toolkit, "Scenario 19: Hate Speech", 1 October 2020, §16. available at: https://cyberlaw.ccdcoe.org/wiki/Scenario_19:_Hate_speech

The NATO Cooperative Cyber Defence Centre of Excellence. 'The Tallinn Manual' https://ccdcoe.org/research/tallinn-manual/

NATO, Press conference, NATO Spokesman Jamie Shea and Air Commodore David Wilby, 9 April 1999

NATO, Press Conference, Mr. Peter Daniel and Colonel Konrad Freytag, 1 May 1999,

Paulo Nunes. « »Impact of New Technologies in the Military Arena: Information Warfare." *Air Power.* Vol 2. No 2. (2007).

L'Obs, 'Bombardements, reddition de soldats ukrainiens démentie… Le point sur la situation a Mariupol » *L'Obs*. (2022).

Fridman Ofer (2018) *Russian 'Hybrid Warfare', Resurgence and Politicisation,* Hurst & Co. p.106.

OHCHR (2022) 'Russia: UN experts alarmed by 'chocking' information clampdown' *OHCHR Media Center.* 12 March 2022.

Oxford's Learners Dictionary. 'Post-Truth'. Available at: https://www.oxfordlearnersdictionaries.com/definition/english/post-truth

Sejal Parmer, The Legal Framework for Addressing 'Hate Speech' in Europe, *presented in* Addressing Hate Speech in the Media: The Role of Regulatory Authorities and the Judiciary, in the International Conference Organized by Council of Europe in Partnership with the Croatian Agency for Electronic Media (Nov. 6–7, 2018). Available at: https://bit.ly/3JA3YuM

Paresh, D (2022) 'Ukraine uses facial recognition to identify dead Russian soldiers, minister says' *Reuters.* 24 March 2022. https://www.swissinfo.ch/eng/ukraine-uses-facial-recognition-to-identify-dead-russian-soldiers--minister-says/47458538

Jared Prier. 'Commanding the Trend: Social Media as Information Warfare*'. Strategic Studies Quarterly.* Vol 11. No. 4 (2017) pp 50–85.

Priestap, Bill. 2017. 'Assessing Russian Activities and Intentions in Recent Elections*' fbi.gov.* 21 June 2017.

Waseem Qureshi. Information Warfare, International and the Changing Battlefield', *Fordham International Law Journal.* Vol 43. Issue 4. (2020).

Reuters. 2007. "Factbox – War in Lebanon, one year ago". 8 July 2007.

Michael J. Robbat. 'Resolving the legal issues concerning the use of information warfare in the international forum: the reach of the existing legal framework and the creation of a new paradigm. *Science and Technology.* (2000).

General Rogers, *Law on the Battlefield.* Manchester University Press. (1996)

Lev Rubinshtein 'obnazheniye priyema' *grani.ru.* 11 September 2008.

Fabio Rugge. 'MindHacking': Information warfare in the cyber age'. *Istituto per Gli Studi di Political Internazionale*. Analysis n°319. (2018)

RULAC. 'International armed conflict in Ukraine'. Available at: https://www.rulac.org/browse/conflicts/international-armed-conflict-in-ukraine

Yves Sandoz, Christophe Swinarski & Bruno Zimmermann (eds), Commentary to the Additional Protocols, International Committee of the Red Cross. §1516.

Marco Sassòli, Antoine Bouvier and Anne Quintin, How Does Law Protect in War?, 3rd ed., Vol. 1, ICRC, Geneva, 2011, p. 52.

Marco Sassoli. *International Humanitarian Law: Rules, Controversies, and Solutions to Problems arising in warfare*. Edward Elgar Publising Limited. (2019). p.173,541.

Dietrich Schindler. 'The *Different Types of Armed Conflicts*. According to the Geneva Conventions and Protocols', The Hague Academy Collected Courses, Vol. 63, (1979).

Singer, P. 'Winning the War of Words: Information Warfare in Afghanistan'. *Brookings.* (2001).

Sparrow, R. "Killer Robots". *Journal of Applied Philosop*hy, 24(1) pp. 62–77. (2007).

David Streckfuss. Truth on Trial in Thailand: Defamation, treason and lèse-majesté. (1st ed.). Routledge. (2010).

Stojanovic, M. 2021. Suspicions Persist About NATO's Deadly Bombing of Serbian TV. *Balkan Transitional Justice.* April 23, 2021. https://balkaninsight.com/2021/04/23/suspicions-persist-about-natos-deadly-bombing-of-serbian-tv/

Timothy Thomas. Thinking like a Russian Officer: Basic Factors and Contemporary Thinking on the Nature of War. *Foreign Military Studies*. (2016).

Alvin and Heidi Toffler, *War and anti-War: Survival at the Dawn of the 21 st Century.* New York: Warner Books. (1995).

United Nations General Assembly, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/70/174.

United Nations (2018). *'Securing our common future: An agenda for Disarmament'.* Office for Disarmament Affairs, New York.

Vergely, B. (2019) 'Vers des fakes de plus en plus nombreux et de moins en moins détectables : comment vivre à l'heure de la post-vérité ?' *Atlantico*, 6 janvier 2019.

Viner, K. (2016) « Comment le numérique a ébranlé notre rapport à la vérité », *Courrier international*, 9 septembre 2016.

World Economic Forum (2019) ‘António Guterres: Read the UN Secretary-General's Davos Speech in Full’, World Economic Forum. 24 January 2019.

World Health Organisation. ‘Infodemic’. Available at: https://www.who.int/health-topics/infodemic#tab=tab_1

Zivanovic, M. Haxhiaj, S. (2019). ‘78 days of fear: Remembering NATO’s Bombing of Yugoslavia’. *Balkaninisghts.com.* March 22, 2019.

zombie. 2006. "The Reuters Photo Scandal". *zombietime.com*. 8 August 2006.

‘Israel Hacks into Al Manar during lebanon war 2006’. Internet Archive. Uploaded : 15 November 2017 by LiveLeakDotCom2507792. Available at : https://archive.org/details/LiveLeakDotCom2507792