PANTEION UNIVERSITY OF SOCIAL AND POLITICAL SCIENCES

DEPARTMENTS OF COMMUNICATION, MEDIA AND CULTURE
AND
INTERNATIONAL & EUROPEAN STUDIES

MA PROGRAM
"DIGITAL TRANSFORMATION"

SPECIALIZATION: DIGITAL LAW

Privatizing digital warfare:

How private actors complicate compliance with IHL and HRL

DISSERTATION

NIKOLAOS SAMARAS

Nicosia, 2026

Supervisor

Maria Daniella Marouda, Associate Professor at Panteion University of Social and Political Sciences.

To all those who contributed
physically, mentally and digitally

Declaration of Non-Plagiarism and Assumption of Personal Responsibility

I declare that the work submitted as part of my academic studies is the result of my original research. I affirm that it does not make use of the intellectual property of third parties, or any text generated by generative AI applications without proper and necessary referencing. I further confirm that any use of AI in the preparation of this work has been strictly limited to editing and proofreading purposes, without contributing to the creation of substantive content. I acknowledge and assume full legal and administrative responsibility for any instances of plagiarism or academic dishonesty that may arise from this work.

Contents

Abbreviations

AI	Artificial Intelligence
CCD COE	Cooperative Cyber Defence Centre of Excellence
CCW	Convention on Certain Conventional Weapons
CDOC	Cyber Defence Operations Centre
CISA	Cybersecurity and Infrastructure Security Agency
CoE	Council of Europe
CFR	Charter of Fundamental Rights
DPH	Direct part in hostilities
ENISA	European Network and Information Security Agency
EU	European Union
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
GGE	Group of Governmental Experts
HRL	Human Rights Law
ICCPR	International Covenant on Civil and Political Rights
ICESCR	International Covenant on Economic, Social and Cultural Rights
ICJ	International Court of Justice
ICRC	International Committee of the Red Cross
ICT	Information and Communication Technology
ICTY	International Criminal Tribunal for the former Yugoslavia
IHL	International Humanitarian Law
ILC	International Law Commission
LAWS	Lethal Autonomous Weapon Systems
MDF	Montreux Document Forum
NATO	North Atlantic Treaty Organization
OEWG	Open Ended Working Group
OEIGWG	Open-Ended Intergovernmental Working Group
PPP	Public – Private Partnership

PMSC	Private Military and Security Company
UNGPs	United Nations Guiding Principles on Business and Human Rights
UAV	Unmanned Aerial Vehicle
UAS	Unmanned Aircraft System
UDHR	Universal Declaration of Human Rights
USA	United States of America
UN	United Nations

Abstract

This digitalization of our lives has influenced warfare, by redefining the distribution of power and responsibility in global security governance. Once a strictly state-driven domain, the increasing dependency on the private domain for expertise, resources and operational execution has led to a privatization of war, which exposes the structural durability of IHL and HRL. These traditional frameworks, drafted and applied for kinetic operations, are called to regulate behaviors in the digital domain, which is characterized by speed, anonymity and transborder nature.

In this current technological disruption, human rights are the ethical compass which will drive humanity through these uncharted waters. The need for translation in a new, digital *alphabet*, which will consist of algorithms, *black boxes* and automated code, is present. To paraphrase a Hollywood quote, *with greater power comes greater responsibility*. Yet, in this ominous future, the task for us and the coming decades is not to discard traditional law but to recalibrate it, aligning its structures with the realities of a world where sovereignty, security, and technology are inseparable. Privatizing digital warfare does not merely complicate compliance with existing law; it challenges the very ontology of responsibility. When power is distributed among code, corporations, and states, responsibility must follow the same distributed logic, so as to balance state sovereignty, security, and accountability.

.

Keywords: International Humanitarian Law, Human Rights Law, privatization, digital warfare, accountability

Introduction

Background and Research Problem

Technology advancement has always been a progressive dynamic force throughout the evolution of human race, with impact on our surroundings. Leaps in the science field trigger changes in all aspects of our lives – health, education, work, war. Both tools and actors undergo constant changes, following evolution, efficiency and new reality.

Specifically in warfare, military operations have gone through several phases, from spears and gunpowder, to nuclear weapons and lasers. However, the infusion of the digital essence in military activities marks one of the most profound shifts in modern security and defence regime.

Modern military strategies, both defensive and offensive, include cyber capabilities and artificial intelligence that increase combativeness, speed and efficiency in delivering military advantage. The interconnectedness of advanced military applications with the Internet of Things forms a distinct category – that of Internet of Battlefield Things (Kott, Swami, & West, 2016).

However, innovation and technology advancements are usually exercised by private entities, which have more resources, expertise and transnational influence. The war in Ukraine offers a very illustrative example of how tech companies have shaped the theater of military operations, making private actors from innovators to participants (Carnegie Endowment for International Peace, 2025).

In USA, under the administration where venture capital and national security get connected, the next generation of command and control has risen, where four tech executives of Meta, OpenAI and Palantir officially joined a military corps, *Detachment 201*, which aims to provide advice on new technologies that can be used in combat (Dealbreaker, 2025).

This growing ecosystem of private entities performing traditionally state governed practices, however, challenges the established paradigms of international law. International Humanitarian Law (IHL) and International Human Rights Law (HRL) traditionally regulated the conduct of actors (combatants or non-combatants) during kinetic domains.

Yet, digital domain disrupts this status quo. Cyber-attacks can result in the same damage, death or injury as kinetic operations, thus triggering the need for regulating such action. The privatization of warfare is not a new phenomenon as private military and security companies have long operated in armed conflicts. What is new is the digital dimension of their engagement.

Usually having no physical presence in the battlefield, companies can influence the course of hostilities, since their decisions, which consist of lines of code and automated systems and weapons, affect the execution of military orders and the protection of civilians. Legal frameworks seem to be eligible for regulating this conduct – however, the nature of this convergence of digital transformation and privatized warfare creates a pressing legal and ethical problem. Do new weapons demand new rules?

Research Question

This dissertation seeks to explore how the increasing involvement of private entities in digital warfare complicates compliance with IHL and HRL. As states outsource to private actors for the development, maintenance, and operation of digital capabilities, fundamental questions arise concerning accountability, legality, and the safeguard of humanitarian and human rights principles in the conduct of hostilities and outside of it.

The central research question guiding this study can be expressed as follows: How does the participation of private actors in digital warfare challenge the implementation and enforcement of IHL and HRL?

To address this question, the dissertation will pursue the following objectives:

- To examine the evolution of private actors in the context of digital warfare and identify their involvement in crucial state functions, such as defense and security.
- To analyze how the principles of IHL and HRL apply to digital operations involving private entities, focusing on issues of attribution, responsibility, and due diligence.
- To assess the challenges emerging from public–private cooperation in military digital domains.
- To evaluate existing and proposed regulatory frameworks, including soft-law mechanisms that aim to address accountability gaps.
- To propose recommendations, under the light of future's technology for enhancing existing mechanisms to ensure that digital warfare remains consistent with international legal obligations and humanitarian values.

Academic Relevance to Digital (Transformation and International) Law

This analysis hopes to contribute in understanding the complexity of digital warfare which stands at the crossroads of technology and international governance. Digital risks are infinite in the borderless and intangible domain of cyber world and the area of law is a robust response to the expansive reach of Internet.

The digital transformation shapes our daily lives from a social, political, technological and legal point of view. Conflicting interests in the evolving ecosystem affect all functions, military sphere included. States are no longer the sole players in armed conflicts. Private actors are elevated due to their dominance in technology innovation - thus their interconnectedness constitutes a core dimension of the ongoing digital transformation.

From a legal perspective, this transformation demands a reconsideration of how traditional frameworks apply in the digital domain. Traditional concepts are recalibrated in

order to withstand the new dynamics of the modern reality. Accountability is considered to play a crucial role in preserving fundamental human rights - a notion that is blurred due to the fact that power has moved faster than law, and faster than the State, toward private actors in digital warfare.

Progress is always balanced with legal and moral responsibility. Understanding how these dynamics unfold within the context of armed conflict not only contributes to the theory and practice of international law but also informs the design of governance models capable of addressing the challenges of an increasingly digitalized world.

Methodology and Structure of the Thesis

This dissertation adopts a qualitative and analytical legal research methodology, drawing on both doctrinal and comparative approaches.

On the one hand, it examines how existing international legal frameworks – precisely the frameworks for humanitarian and human rights law - apply to the growing participation of private actors in digital warfare. It analyzes primary legal sources, including treaties, conventions, manuals as well as decisions of judicial bodies, alongside with secondary sources such as academic literature and scientific articles.

On the other hand, it involves the interpretation and evaluation of international legal frameworks, relevant to the operation of warfare, to human rights and to specific aspects of both, such as the state responsibility and accountability. Except from normative texts, the interaction of those with soft law instruments, enables a comprehensive understanding of both the strengths and the limitations of modern situation.

The thesis is organized into three main parts, each divided into chapters:

- *Part I - Context and Scope* sets the groundwork on which the analysis of the privatization of digital warfare develops, following the evolution from private actors to the modern state-private cyber collaborations.
- *Part II – Legal Frameworks and Analysis* is developed on the two main legal frameworks, IHL and HRL, following their interaction with other legal instruments and practices in digital domain.
- *Part III – Empirical application, Challenges, and Future Outlook* provides case studies, underscores the structural implications of outsourcing in digital warfare and presents current and future challenges, accompanied by holistic recommendations.

Part I Context and Scope

Chapter 1 Historical Evolution of Private Actors

The participation of private entities in war is as old as organized conflict itself. Long before the rise of the modern nation-state, private mercenaries were recruited in the Crusades and the American Revolution, depicting the important role of their employment (Baum & McGahan, 2009). Profit was the main purpose of their allegiance, and less the belief in a good common cause. These actors existed in the grey space between sovereignty and commerce, offering their military experience to the highest bidder and blurring the line between soldier and entrepreneur.

An important landmark on the evolution of private army can be traced back in 1648. The Peace of Westphalia set the foundation of the emergence of the modern state system, by institutionalizing the state as the sole (or the highest) legitimate wielder of force[1], through national militaries, governed by hierarchy, discipline, and public accountability.

However, besides the "legitimate" actors of enforcing violence, there are phenomena such as terrorists and private security companies (Munro, n.d.) that jeopardize the cohesion of societies. This equation gets even more complicated, considering the logistical complexity of modern conflict — from supply chains to weapons manufacturing, proving that the private sector never fully departed from the trenches of war, either physical or digital.

This outsourcing led to a significant resurgence of private military and security companies (PMSCs). Executive Outcomes (EO) in Sierra Leone (Goga, 2024) and Blackwater (Scahill, 2007) in Iraq and Afghanistan are two dominant examples of the late 20th and the dawn of 21st century that took advantage of political (and legal) gaps and developed their actions alongside the national forces, providing logistical and training services, armed protection and operational support.

[1] Max Weber would later distill as the monopoly on the legitimate use of violence, in *Politics as a vocation*

Institutions such as the United Nations (UN) and the International Committee of the Red Cross (ICRC) took action against these developments that created debates over legitimacy, accountability and the erosion of the aforementioned state's monopoly on force. The Montreux Document of 2008[2] sought to establish a text "containing rules and good practices relating to private military and security companies operating in armed conflict" – with its "soft law nature", however, being the *Achilles heel (Tougas, 2009).*

In our era, privatization entered a new frontier – the digital domain. Rifles and mortars are accompanied by algorithms and lines of codes, trenches and roadblocks by networks and firewalls. Today's private actors no longer operate in uniform; they operate behind keyboards, in laboratories or garages, and within cloud infrastructures. The state, once the architect and executor of war, now increasingly depends on these actors to design, maintain, and defend the virtual arsenals of the modern era.

The transition from traditional to digital privatization mirrors a broader economic and political logic: efficiency, expertise and plausible deniability. States consider PSMCs not only as force multipliers[3] but also as key players, who can be used as surrogates when political risk needs to be diffused. The same reasoning now applies to cyberspace, where digital contractors allow governments to conduct sensitive operations while maintaining strategic ambiguity, thus transforming security from a public to a private good.

Against the awe that futuristic theater of operations may cause and the tools of warfare have evolved, the main logic of privatization remains constant: states rely on private expertise to augment power and mitigate liability. As cyberspace emerged as the fifth domain of conflict (NATO Allied Command Transformation, n.d.), this logic found a new arena, where there are many attack surfaces; and it's available in all facets of a conflict, including

[2] UN General Assembly (A/63/467–S/2008/636)
[3] More for the supplementary services in Krieg, A. (2018). Defining remote warfare: The rise of the private military and security industry. Remote Warfare Program.

before the conflict (United States Space Force, 2024). The rise of private cyber contractors marks not merely a continuation but an evolution of this centuries-old trend, where the boundaries between statecraft and commerce have become more penetrable than ever.

Chapter 2 Rise of Cyber Mercenaries and Cybersecurity Firms

The proliferation of digital technologies functions as a catalyst in the rise of cyber mercenaries and cybersecurity firms. These new actors operate in a domain that knows nothing of physical borders and legal jurisdictions. Their capabilities vary from intelligence gathering, performing cyber-attacks or developing harmful software to exploit vulnerabilities (Astran, n.d.).

Either individually or organized in groups, private cyber mercenaries operate in a "grey-zone" of warfare, often outside the bounds of traditional military operations, blurring the line between public and private action. Examples include the Sandworm group allegedly associated with Russia's GRU (United States Congress, n.d.), or private Israeli firms such as NSO Group (OCCRP, n.d.), whose Pegasus spyware has been sold to governments worldwide and raised profound question in this blurred intersection between about corporate innovation and human rights violations.

Similarly, Palantir, which is considered a dystopian surveillance agency (Haskins, 2019), sells an AI-based platform that allows its users – among them, military and law enforcement agencies – to analyze personal data, including social media profiles, personal information and physical characteristics (Reich, 2025). This operation helps by fusing data in battlefield, which is vital in targeting, the core of warfare.

These are some of the examples that reaffirm the role of the private factor not as a strategic partner but rather as integral nodes in the architecture of modern warfare, thus granting them a share on the rights and responsibilities in real time and challenging core assumptions of international humanitarian and human rights law.

If PSMCs directly support a military operation, does it assume the legal obligations of a party to the conflict? And if such actions cause civilian harm, can affected individuals seek remedy through existing mechanisms? Can the legal frameworks designed for states withstand the struggle to capture the distributed, multi-actor reality of the digital battlefield?

On the other hand, PSMCs can be supporters of the defence capabilities of states. Companies such as Microsoft and Mandiant (Google) play pivotal roles in national defense and intelligence operations. Their expertise enables states to detect and respond to cyberattacks, conduct threat analysis, and even engage in active cyber defense.

For instance, Microsoft's Digital Crimes Unit (Microsoft, 2022) and Defender Threat Intelligence Center (Microsoft, n.d.) have taken action by collecting intelligence data, accurately and timely assessing them and respectively responding. However, this growing autonomy demonstrates how private firms have acquired seemingly sovereign capacities in the digital sphere (The Guardian, 2025).

The blurred boundaries between service provider and participant create complex accountability questions. Detecting and neutralizing threats are functions traditionally entitled to the states. But what is the status of PMSC staff under international humanitarian law? Are they considered mercenaries, within the context of the Geneva Convention (ICRC, n.d.)?

Except from the International Humanitarian Law, the commercial incentives driving these firms often collide with considerations related to human rights. Ethical or legal dilemmas are resurfacing in this profit-motioned operation. Can the pace of technological innovation and the secrecy of cyber operations respect, let alone not violate international norms? Or does the growing role of private actors in shaping digital conflicts reveal an expanding accountability vacuum that international law struggles to fill?

Chapter 3 Public–Private Partnerships in Digital Warfare

The ongoing complicated threats make the greater picture clearer, that the alliance between national security agencies and the private sector is not just a matter of convenience but a strategic imperative that strengthens the very fabric of a nation's security. Technological innovation is mostly achieved first by the private sector, for reasons that competition and capitalism can explain better.

By forming public–private partnerships (PPPs) in cybersecurity and defense, these collaborations recognize that the infrastructure, knowledge and essential technical and organizing tools to digital security are primarily owned and operated by private companies. The majority of strategic digital assets — data centers, cloud infrastructure and networks — lie in corporate rather than governmental hands.

Cybersecurity and Infrastructure Security Agency (CISA, n.d.) in USA or European Network and Information Security Agency (ENISA, n.d.) in Europe institutionalize cooperation between public authorities and private stakeholders. Collective resilience is the ultimate goal, so as the citizens to feel secure and be equipped against digital threats.

The rise, however, of the role of private actors in the dynamic domain of security hides some dangers. As the saying says, too many cooks spoil the broth, and here the broth is the vital interests of us all – the safety of our families, security within the borders of our country, our economic independence. Security governance seems to shift from a state and national aspect to a more multifaceted approach, whether profit or innovation play an important role.

But to what extent does outsourcing work? The European Union states in the Cybersecurity Strategy (Digital Strategy of the European Commission, n.d.) that "Governments, businesses and citizens will all share a responsibility in ensuring a cyber-secure digital transformation". Since 2004, EU is trying to use the single market as a Trojan

horse in order to “transnationalize” security issues, by stressing that computing and networking are now becoming ubiquitous utilities in the same way as electricity and water supply already are[4].

On the other side of the Atlantic waters, the 2023 U.S. National Cyber Strategy of Joe Biden’s administration explicitly acknowledge that state resilience depends on private-sector collaboration, and by doing so the responsibility for cybersecurity will be more effective and more equitable (White House, 2023). With the dawn of 2026, Trump administration aims to release the new national cybersecurity strategy which will develop on six pillars, such as deterring US adversaries and protecting critical infrastructure (White House, 2025).

Apart from political institutions, NATO, as the most advanced military alliance worldwide, also acknowledges the growing dependence on private partners for operational defense and situational awareness. With its Cooperative Cyber Defence Centre of Excellence (CCD COE, n.d.), the Alliance contributes with research, trainings and exercises in focus areas, such as Technology, Operations, Strategy and Law. One of the main acknowledgements to the global research for cyber issues is the Tallinn Manual, a continuously revised initiative, which functions not just as an appendix for *black letter* rules, as its preamble mentions, but as a comprehensive analysis of international law applicable to cyber operations.

However, the complexity of international law is augmented within the digital realm. The interdependence of PPPs complicates the enforcement of international law principles such as distinction and proportionality, which assume clear hierarchies of command and control. When the actors involved include multinational corporations, the traditional model of state-centered accountability becomes increasingly untenable. Accountability vacuums and

[4] European Parliament and European Council (2004) Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 Establishing the European Network and In-formation Security Agency (Brussels: European Parliament and European Council)

grey spaced areas need to be redefined, with the speed of evolution being detrimental to the legality.

The next part will examine how international law interprets this reality. The digital age has reconfigured not only how wars are fought but also who is bound by the laws of war. Private entities assume quasi-sovereign roles: protecting critical infrastructure and managing digital communication channels, restricting access to networks, suspending services, or sharing intelligence — can have humanitarian and political implications equivalent to those of state actions. Do the main pillars of IHL - distinction, proportionality, and state responsibility – as well as HRL require reinterpretation?

Part II Legal Framework and Analysis

Chapter 1: International Humanitarian Law and Private Actors

International Humanitarian Law, also known as the law of armed conflict, law of war or *jus in bello*, is a set of rules that regulates the conduct of hostilities and the protection of persons during armed conflict. Balancing military necessity with humanity considerations, IHL provisions ensure that even in times of war, violence remains regulated and monitored by law[5], functioning both as interpretive tools and as binding norms applicable to all parties engaged in armed conflict, whether international or non-international in character.

As a part of public international law, IHL is made up primarily of treaties, customary law and general principles of law[6]. The primary core of IHL consists of the four Geneva Conventions of 1949 and their Additional Protocols of 1977, complemented by customary rules developed through state practice and *opinio juris*.

As the predecessor[7] of modern IHL, the 1907 Hague Convention stated in article 22 that "the right of belligerents to adopt means of injuring the enemy is not unlimited". From this provision we can see the four interrelated principles stemming and transforming into the heart of IHL: distinction, proportionality, necessity, and humanity[8]. Despite the fact that these principles have been interpreted infinite times, presenting their meaning in this part serves as a way to set the four prisms through which the digital warfare will be examined.

The principle of distinction obliges belligerents to distinguish at all times between combatants and civilians, and between military objectives and civilian objects[9]. Only military

[5] In contrast with jus ad bellum, which legalized only two forms of violence (self-defense and Security Council authorization), IHL is applied whenever an armed conflict commences.
[6] Article 38 of the Statute of the International Court of Justice
[7] 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, 18 October 1907
[8] Glossary of the ICRC Database
[9] Article 48 of Additional Protocol I

objectives may be lawfully attacked, while civilian persons and objects enjoy protection from direct, indiscriminate[10] attack unless and for such time as they take a direct part in hostilities[11].

Proportionality prohibits attacks expected to cause incidental civilian harm that would be excessive in relation to the concrete and direct military advantage anticipated[12]. This principle reflects the effort to balance humanitarian protection with operational necessity, seeking to limit the effects of the means and methods of warfare and their collateral damage without undermining legitimate military objectives[13].

The principle of military necessity[14] allows only those measures of force that are indispensable for achieving a legitimate military purpose and are not otherwise prohibited by IHL. The main (legitimate) goal of a conflict is to weaken the military capacity of the adversary[15], thus IHL does not justify unlimited or indiscriminate violence but rather requires that all military actions serve this defined and lawful objective.

Finally, the principle of humanity[16] prohibits the infliction of suffering, injury, or destruction not justified by military necessity. The inability for a certain, watertight definition (Coupland, 2001) shows that, even in the absence of specific legal rules, combatants and commanders remain bound by the dictates of public conscience and principles of humanity. It is as Jean Pictet claimed, that it is "something understood but not actually expressed" (Le Moli, 2021).

How these principles are present in the digital battlefield? The nature of cyber operations includes transboundary, instant and sometimes untraceable attacks – something

[10] Supra note 8
[11] Article 51(3) of the Additional Protocol I
[12] Article 51(5)(b) of the Additional Protocol I
[13] Supra note 8
[14] *Idem*
[15] Article 52(3) of the Additional Protocol I
[16] This principle is known as Martens Clause, derived from the preamble to 1907 Convention (IV) respecting the Laws and Customs of War on Land

completely different from the traditional conflicts, whose actions were characterized of kinetic, territorial and identifiable powers, with the effects being able in most cases to be measured. Distinction, proportionality and necessity develop into more complex aspects, given the decentralized participation of civilian and military digital infrastructures which are commonly interdependent.

In this context, the application of IHL to digital warfare, and particularly to private entities participating therein, raises fundamental questions about the adequacy of the existing normative framework. Whether these principles can effectively regulate conduct in a domain defined by anonymity, automation, and privatization forms the basis for the analysis that follows.

1.1 Application of International Humanitarian Law to Cyber Operations

Before examining the (need for) evolution of the traditional aforementioned principles, the main question needs to be answered - is the IHL applied to cyber operations? At first glance, the answer seems to be evident. However, the increasing militarization of ICTs[17] gives space to the appearance of opinions that take advantage of the absence of normative framework and create *ifs* and *hows*.

Yet, the behavior of actors isn't only regulated by treaties and agreements. The practice of States shows that there is a dispersed consensus that existing IHL rules apply to cyber space. Legal voids must be excluded, despite the fact that, given the periods of history from which they emerged, the cyber domain was absent during the drafting of IHL.

This new technological advancement isn't the first occasion when humanity, in modern times, faced an unprecedented, powerful and global danger. Nuclear weapons have a qualitative as well as quantitative difference in comparison with the conventional weapons.

[17] Resolution ICRC 2024 (34IC/24/R2)

Yet, the International Court of Justice (ICJ) stated in *Legality of the Threat or Use of Nuclear Weapons* (1996, paras. 78, 95) that the humanitarian objective[18] of IHL "permeates the entire law of armed conflict and applies to al1 forms of warfare and to al1 kinds of weapons, those of the past, those of the present and those of the future" – granting extension of IHL to subsequent notions and phenomena.

The continuity of IHL must be constant, irrespective of technological change as it is innate element within the human nature with adaptation being the key factor, applying familiar notions to new sets of facts and new technologies. In this struggle of regulating the always changing complicated cyber space, there are initiatives by institutions, which contribute with their expertise, research and developing state collaboration.

One of the main stakeholders in this effort is the CCD COE of NATO, in Estonia, which provides probably the most comprehensive articulation of how IHL might apply to cyber activities. With interoperability being in the core principles of the Alliance, legal alignment is equally essential, in order coordination and collective resilience to be achieved.

Since 2013, the Centre produced the *Tallinn Manual on the International Law Applicable to Cyber Operations* which addressed the most severe cyber operations – those that violate the prohibition of the use of force, entitle states to exercise their right of self-defence or occur during armed conflict.

State practice, technological advancements and the dominant position of ICT in modern fora necessitated an update of the Manual in 2017 *(Tallinn Manual 2.0)* while a new round of update is ongoing, with 2026 expected to be the launch year of the 3rd edition.

Despite the fact that the Manual is not a legally binding work, it represents a significant scholarly and state-endorsed effort to interpret IHL principles in light of digital

[18] "to mitigate and circumscribe the cruelty of war for humanitarian reasons" (New Zealand, Written Statement, p. 15, paras. 63-64)

realities, drafted by distinguished international law academics and practitioners. The central essence of the IHL application is the armed conflicts, a situation where attacks occur. In cyber space, the relevant question concerns what a "cyber-attack" under IHL constitutes.

According to Rule 92 of the Tallinn Manual 2.0 *(*whose wording remained unchanged since Rule 30 of the first edition), a cyber operation qualifies as an attack when "the operation, offensive or defensive, is reasonably expected to cause injury or death to persons or damage or destruction to objects".

However, how do IHL foundational principles operate within a cyber-attack? How can we adapt their interpretation of the aforementioned principles, while their humanitarian rationale remains technological neutral, especially in light of increasing participation of private entities?

Operating interoperable civilian and military digital infrastructure disrupts the principle of distinction. Dual-use objects and systems pose challenges, blurring the line between military targets and civilian objects. Cloud servers and telecommunications networks, largely (if not completely) operated by companies, can be considered as lawful military targets, despite their importance to civilian life. This new reality necessitates a case by case and effects-based assessment of cyber targets, adapting traditional criteria without allowing the civilian protection that distinction seeks to guarantee to be detrimentally put aside.

The participation of the private sector also challenges the proportionality principle. Cyber operations may generate indirect and cascading effects that temporally extended beyond immediate physical damage, if there is even any of such. The very technical architecture of such systems jeopardize the function of interconnected platforms, related to health systems, bank accounts or energy distribution, disruption of which can have incidental

civilian harm. The inability of foreseeable consequences of digital operations must be excluded when assessing the nature of attacks with in the IHL framework.

Outsourcing cyber capabilities, outside the limits of state harbors, risks the reinterpretation of the principle of military necessity detrimentally to the IHL. The low cost, the speed and the reusability of modern services may shift the purpose of operations, from a restrained spectrum of lawful military action (whose only goal is the military advantage) to a commercial, economical conduct. Only an interpretation that retains necessity anchored to the requirement of indispensable military advantage can be accepted.

Finally, the principle of humanity remains central in cyberspace, where prolonged or systemic disruption of civilian life may produce severe humanitarian consequences. The private companies are not present just in developing weapons and military systems - they are dominating in every aspect of our daily life, making them at the epicenter of civilian life.

However, as it was mentioned, it was affirmed by the ICJ that IHL's humanitarian objective permeates all forms of warfare, including those shaped by emerging technologies. This ongoing reliance on private entities therefore reinforces the need to interpret humanity in a manner that accounts for modern technological dependencies and prevents the infliction of unnecessary suffering through systemic or prolonged digital disruption.

In this process of adaptation, undefined areas need to be addressed. During the sessions of the Group of Governmental Experts (GGE), under the auspices of the United Nations, on the Convention on Certain Conventional Weapons (CCW) and on emerging technologies in the area of lethal autonomous weapons systems (LAWS), there were divergent views and debated positions on subjects relevant to IHL, such as the threshold of armed attack (particularly when the resulting harm is functional rather than physical), autonomous judgement and control. What is important, however, is that delegations in these

sessions welcomed broadly and reiterated the importance of referencing existing IHL and previously agreed language – thus solidifying the opinion that IHL applies to cyberspace.

The evolution of IHL brings us to the next question; what is a private actor for IHL – this new element in the cyber operations? Their activity ranges from developing, operating and controlling the functions of systems and infrastructure – thus, making them an integral part of applying IHL. Is this opinion contradictory since IHL addresses the conduct of States? Are they included in the notion of *combatants* or are they civilians who directly take part in hostilities? Ultimately, who is to blame for IHL violations – States or private entities? This ambiguity forms the foundation for subsequent discussion on the legal status of private actors and the challenges of attribution under international law.

1.2 Legal Status of Private Actors

Despite the arms races and the infinite ammunition that is used during a conflict, the real protagonists are the humans, whose action or omission create consequences, the impact of which is the true measure of war. The cornerstone of IHL is the determination of the status of individuals and entities, with this categorization being meaningful and having legal consequences.

Historically, IHL has been formulated to regulate conflicts mainly between States, and specifically between armed forces, bearing the flag of their country, performing operations by executing orders, under a chain of command. The determination between civilians and combatants is pivotal under the Geneva Conventions (and customary law, as well), since it exemplifies the lawfulness of the participation in conflict and this “separation of armies and peaceful inhabitants into two distinct classes is perhaps the greatest triumph of international law” (Schondorf, 2005).

Under Article 43(2) of Additional Protocol I[19], combatant status is limited to members of the armed forces of a Party to the conflict and certain organized resistance movements meeting specified criteria: responsible command, subject to an internal disciplinary system and complying with IHL. Combatants have the right to participate directly in hostilities and if captured, they are granted the status of Prisoners of War, enjoying immunity from prosecution for lawful acts of war.

Negatively defined, civilians are all those who are not considered as combatants, they are protected[20] from direct attack unless and for such time as they take a direct part in hostilities (DPH)[21].

The growing involvement of private actors in digital warfare, however, has blurred these categories and raised complex questions regarding their status and obligations. PMSCs and by extension all digital contractors are neither formally incorporated into the armed forces nor subject to the chain of command nor disciplinary structures required by IHL. As such, they fall out of the term combatants.

Yet, can they be considered civilians? Can their support exceed the threshold of engaging into hostilities, thus making them lawful targets? With the principle of distinction being widely recognized as treaty and customary law, all belligerents abide by it. But civilian suppliers, in the context of cyber operations, are far different than the traditional logistic support. Could they qualify as civilians who DPH?

[19] Article 4 of Geneva Convention III requires additional criteria, such as wearing a fixed distinctive sign and carry arms openly

[20] While IHL protects all civilians without discrimination, certain groups are singled out for special mention. In wartime, women and children, the elderly and the sick are highly vulnerable. So too are those who flee their homes and become internally displaced or refugees. IHL prohibits forcing displacement by intimidation, violence or starvation.

[21] Article 51(3) of Additional Protocol I

The International Committee of the Red Cross (ICRC) *Interpretive Guidance on Direct Participation in Hostilities* (2009) states that the constitutive elements of DPH (for which there is no a precise definition) consist of:

- acts likely to adversely affect the military operations or military capacity of a party to the conflict, or to inflict death, injury or destruction on persons or objects protected against direct attack (threshold of harm).
- direct causal link between the act and the harm likely to result either from that act, or from a coordinated military operation of which that act constitutes an integral part (direct causation)
- the act must be specifically designed to directly cause the required threshold of harm in support of a party to the conflict and to the detriment of another (belligerent nexus)

Applying this framework to the digital domain, several complexities arise. A software engineer designing or maintaining a weapon in cyberspace; a big data analyst who provides real-time data to military commanders and decision makers; a network defender deploying cyber defence under state instruction – they could all meet the functional criteria for DPH. Yet, their participation often occurs remotely, far from the theatre of operations on the battlefield. Can this *virtual participation* constitute DPH, within the wording of Article 51(3) AP I?

The Tallinn Manual in Rule 91 acknowledges and accepts the aforementioned criteria for an act to be qualified as DPH. Additionally, it clarifies that there is not a requirement for physical damage – thus a disruption of the Military HQs network, caused by a hacker by his personal computer can be considered as DHP.

However, the Manual also acknowledges that determining what qualifies as DPH in cyberspace remains ambiguous, since network operations are far more complex than kinetic

engagement. For instance, can the expert that does the annual maintenance of the computer in a military compound be considered civilian who participates in hostilities or when does the participation in hostilities end? The complexity of the digital cyberspace is obvious even on the issue of whether a presumption against DPH applies, where the International Group of Experts of the CCD COE were divided[22].

Cyberspace is a theater of operation that can jeopardize this ongoing effort of civilian-combatant distinction. Narrow interpretation can lead to legal insulating zones of individuals who play an important role in modern digital warfare, while an extensive interpretation could expand the list of lawful targets to computer sellers and maintenance workers. The threshold of when a civilian turns from supportive to participatory is blurred within lines of 1s and 0s – thus endangering the layers of protection that IHL's purpose stands for. Beyond the protective scope of IHL, however, this blurred situation is vital regarding the challenge of attribution of violation of the IHL.

1.3 Challenges of Attribution and State Responsibility

The principle of state responsibility constitutes a long standing rule of customary and treaty law, consisting a critical mechanism for enforcing compliance with IHL. It provides that states are internationally accountable for wrongful acts committed by their organs (armed forces included), agents, or other entities acting under their authority or control.

Such misconduct of private entities in cyber space poses significant challenges for various reasons. Cyber vigilantism (Trottier, 2016) is present longer than Artificial Intelligence has conquered our lives. The lack of experience or of the means to perform a digital operation can harm directly or incidentally civilians, can expose attackers and transform them to lawful targets (for example bombarding a garage of a cyber hacker, from

[22] See analysis in Rule 95 of Tallinn Manual

where the attack is launched) - thus blurring even more the distinction between combatants, civilians and civilians who DPH, with legal consequences.

Is there, however, a blatant hypocrisy, when modern world has not yet a legally binding instrument? Twenty five years after the adoption in 2001 by the UN ILC of the *Articles on the Responsibility of States for Internationally Wrongful Acts* and the international society seems contradictory, with judiciary bodies and State practice proving that some of the Articles are superseded (QIL QDI, n.d.). Despite this debated tug of war, however, the essence of the Articles should not be sacrificed as scapegoat, under political or other motives.

According to Articles 4 and 5, the conduct of any state organ — including the armed forces — is attributable to the state, even if the organ exceeds its authority or contravenes instructions[23], while attribution is extended to entities empowered by domestic law to exercise elements of governmental authority, provided they act in that capacity. These provisions are particularly relevant to privatized military or digital contractors performing inherently governmental functions, such as national defense or intelligence.

In cases when these entities do not formally exercise governmental authority, Article 8 states that the conduct of a private person or group shall be considered an act of the state if the entity is acting on the *instructions* of, or under the *direction* or *control* of that state.

Control of the State is a well-known notion in International Law, stemming out of the territorial sovereignty and display of authority of States. Tribunal decisions have contributed into defining in which degree this relationship must be, in order States to be accountable for entities.

The ICJ, in its *Nicaragua v. United States* (1986) judgment, established "effective control" as a prerequisite to attribute actions of entities to a state. With the *Nicaragua test*, the

[23] See par. 170 and 213-214 in *Armed Activities on the Territory of the Congo* (2005)

Court stated that the State must "direct or enforce the perpetration of acts" that violate the law (*Military and Paramilitary Activities in and against Nicaragua* 1986, par.115).

A broader concept of control was introduced by the International Criminal Tribunal for the former Yugoslavia (ICTY) in *Prosecutor v. Tadić* (1999, paras. 131 & 137), which adopted the test of "overall control", which resides not only in "equipping, financing or training and providing operational support but also coordinating or helping in the general planning".

Both thresholds make attribution difficult in digital world, due to the decentralized network of Blockchain technology, (pseudo)anonymity and spoofing (Vakulina, 2025). The analysis of Rule 17 in the Tallinn Manual states that the effective control "captures the scope of the concept". However, digital operations augment attribution difficulties, due to its political and technological assessments (U.S. Cyberspace Solarium Commission & American University, n.d.).

Unlike traditional attribution, cyber attackers exploit technological achievements and are capable of hiding their identities, besides remaining anonymous. The decentralization of operations, using nodes and systems around the globe, complicates the chain of evidence – thus diffusing control and weakening legal basis for attribution, by lowering the "portion" of effective control independently on each participant.

Additionally, in order for a State to attribute an attack to a State-sponsored entity demands at least an equal level of technological capacity, otherwise the results of an attack may appear much later than the conclusion of it. This can lead to misattribution (Control Engineering, n.d.) which may result in wrongful acts by the State resorting into defending through countermeasures.

Global efforts to regulate this evolving situation are constant. Initiatives such as the UN Open Ended Working Group (OEWG) are mandated to develop rules on the use of

information and communications technologies. In regional level, it is worth mentioning the Montreux Document Forum (MDF) efforts that has resulted in the Montreux Document on Private Military and Security Companies (2008) - a joint effort with the ICRC creating a blueprint for effectively regulating PMSCs. Although non-binding, it provides further guidance on the responsibilities of states hiring or hosting private actors.

The importance of the MDF is that, despite the fact that the Document was finalized in 2008, thus addressing traditional PMSCs, the MDF advances its contribution, following the technological developments and supporting UN's efforts for an international regulatory framework for PMSCs (Montreux Document Forum, n.d.). Its principles are increasingly invoked by analogy in international fora on digital contractors and cyber defense firms, reminding States that misconduct of PMSCs can be attributed to States as well.

The reality of digital era finds humanity with increasing participation of private actors in strategic roles of modern warfare, expanding the uncertainty due to the advanced complexity of the existing challenges. Current legal architecture seeks to keep up with technological progress while the traditional doctrine of State responsibility seems to be undermined, let alone the state sovereignty itself due to the participation of non-state actors in the core of governmental functions.

All stakeholders call for transparency, cooperation and shared responsibility – yet, lack of consensus on binding frameworks proveσ us all wrong. However, individuals cannot rely exclusively on the IHL during warfare. HRL can function as a complementary lens (to the *lex specialis* IHL[24]), through which normative gaps of IHL can be exposed and mitigated.

[24] Supra note 8

Chapter 2: Human Rights Law and Corporate Accountability

Unlike *jus in bello*, Human Rights Law is applied at all times, whether it is peace or war, providing a pivotal framework, which regulates conduct of all stakeholders. Due to the privatization of digital warfare however, outsourcing defence and intelligence capabilities can implicate the protection of human rights.

2.1 Human Rights Law Obligations in Cyberspace

As a permanent body of obligations, HRL offers a normative basis for dignity, liberty and protection against violations, detached by the existence of an armed conflict. The evolving nature of violations, however, due to the digital progress, pushes HRL into new domains, in order individuals' lives to be protected.

The bedrock of Human Rights, the Universal Declaration of Human Rights (UDHR, 1948) lays out three cardinal principles, that human rights belong to all of us (universality), cannot be ranked in importance (indivisibility) and cannot stand on their own (interdependence). Together with the International Covenant on Economic, Social and Cultural Rights (ICESCR, 1966) and the International Covenant on Civil and Political Rights (ICCPR, 1966)**,** they form the nucleus of HRL, enshrining rights and fundamental freedoms.

In a regional basis, the European Convention on Human Rights of the Council of Europe (ECHR, 1950) and the Charter of Fundamental rights of the European Union (CFR, 2000) are complementing the layers of protection from perpetrators against democracy, human rights and the rule of law.

The application of HRL into cyber domain is self-evident; wherever human exists, all the rights that are inherent with the nature of humanity apply. The right to life (Article 6 ICCPR; Article 2 ECHR), the right to privacy (Article 17 ICCPR; Article 8 ECHR) and the freedom of expression (Article 19 ICCPR; Article 10 ECHR) are some examples of human

rights that cyber operations, surveillance technologies and information control measures constantly challenge their application.

In particular, spyware technologies and disruptions of critical infrastructure (for example, hospitals and energy grids) may lead to endangerment of life and health, while biased algorithms and misinformation operations infringe the right of expression and equality.

Cyberspace distorts, additionally, the notion of jurisdiction, a debated subject traditionally connected with territoriality. In UN level, the Human Rights Committee precisely explained territoriality for Human rights through *effective control* prerequisite[25] while globalization and interconnectedness motivate stakeholders to multilaterally approach the extraterritorial application of human rights (OHCHR, 2022).

In regional level, the European Court of Human Rights (ECtHR) has adopted a similar view under Article 1 of the ECHR, holding in *Al-Skeini and Others v. United Kingdom* (2011) that jurisdiction may extend extraterritorially when a state exercises authority or control over persons or territory, suggesting that a functional rather than territorial conception of jurisdiction (Milano, 2013).

Even domestic courts' decision show this evolution. While In USA, cases such as the in *Kiobel v. Royal Dutch Petroleum Co.* (2013), with the Supreme Court reasserting a presumption against the extraterritorial application of US statutes (Loonam & Andreoli, 2025), the UK Supreme Court in *Vedanta Resources Plc v. Lungowe* (2019) held that parent companies may owe a duty of care for subsidiaries' overseas operations if they exert control or issue group-wide policies.

[25] (…) who are within its territory and all persons subject to its jurisdiction, that is, all persons over whose enjoyment of the right to life it exercises power or effective control. This includes persons located outside any territory effectively controlled by the State whose right to life is nonetheless affected by its military or other activities in a direct and reasonably foreseeable manner, Human Rights Committee, General comment no. 36 of 3 September 2019 on Article 6: right to life, UN Doc CCPR/C/GC/36, para. 63

In cyberspace, operations launched from one state's servers may violate rights abroad, even without physical control, The UN Human Rights Council[26] affirmed that the same rights that people have offline must also be protected online, regardless of frontiers due to the open nature of Internet.

This protective exercise of rights demands what CoE calls negative and positive obligations (ECHR Toolkit, n.d.), with the Court (*Åkerberg Fransson,* 2013) explaining the essence of the terms. Particularly against violations by private entities, the ECtHR has affirmed in multiple cases the obligation of the States to protect their individuals from rights infringements by private entities (*Guerra and Others v. Italy,* 1998 - *M.C. v. Bulgaria,* 2003 - *Öneryıldız v. Turkey* 2004). This positive dimension is crucial in digital warfare, where private sector dominates in infrastructure and expertise, through monopolies or oligopolies. Outsourcing capacities doesn't mean outsourcing responsibilities – states withhold the duty to ensure the lawful conduct of private entities.

2.2 Private Actors: Gatekeepers or Tyrants?

As we discussed in the previous chapter, the expanding role of private entities in digital security and warfare introduces both opportunities and dangers for human rights protection. Traditional governmental functions, such as security, defence and intelligence, are now operated by state - private collaborations and sometimes private entities alone. As every tool, however, it is the user who decides whether is for the sake of many or for the interests of few – for example, UAVs and UASs can scan the battlefield for mines but also can develop mass surveillance schemes.

A poster child case for the misuse of cyber tool is the NSO Group's Pegasus spyware, which was launched as a counterterrorism tool (Citizen Lab, 2018), but used by governments

[26] Resolution 20/8 2012

to surveil dissidents, journalists and politicians. Once established through spear-phishing messages, it turned the phone into a 24-hour surveillance device (Guardian 2021). Institutions, such as International Amnesty developed forensic methodology reports, in order to show how Pegasus infiltrated mobile devices (Amnesty International, 2021).

Another firm whose name has become synonym with dystopian surveil is Palantir technologies. Inspired by the "seeing stones" of Tolkien in *The Lord of the Rings*, Palantir is deployed in various countries, such as Israel and UK (McAlpine, 2025), while it played an important role in Ukraine's defenses - by combining, even fragmented, data sources and satellite images, Ukrainian military forces could accurately identify and destroy Russian weapons and equipment (United2media, n.d.).

Both examples show that intelligence is the most vital strategic resource, thus affirming what Clive Humby declared "data as the new oil"[27]. Increasing control over digital information affects the application of human rights. The existing asymmetry between States and private entities is enhanced, due to the fact that private firms have at their disposal more information, enabling themselves to form policies and dilute oversight.

Yet, not all corporate engagement is negative. Some technology firms actively defend human rights in cyberspace. Microsoft has developed the Cyber Defense Operations Center (CDOC) which has assisted in protecting hospitals and humanitarian agencies from cyberattacks during conflicts, such as in Ukraine (Cvetko, 2025). Likewise, companies such as Google (Google Inc., n.d.) and Apple (Apple Inc., 2020) have introduced human rights impact assessments and transparency reports, demonstrating a growing commitment to ethical digital governance. These initiatives show that private innovation can complement public accountability when guided by principled standards.

[27] For the profile of Clive Humby, see also https://sheffield.ac.uk/cs/people/academic-visitors/clive-humby

Ultimately, private actors occupy a paradoxical position: they can strengthen the resilience of human rights through innovation and protection, yet they can also undermine them through complicity, neglect, or abuse. Regulating this tension is central to the emerging global framework of corporate accountability.

2.3 Corporate Accountability Frameworks

While HRL primarily binds states, the blurring of boundaries between public and private authority in digital warfare has prompted an evolution in international governance. This interaction, however, isn't something completely new. Private sector has always been in our lives, affecting our rights – the digital era has just upgraded it.

Since 2011, UN Human Rights Council has adopted the Guiding principles on business and Human rights (UNGP), which center around three pillars:

- It is the duty of States to protect human rights
- It is the duty of Corporations sector to respect human rights
- Victims of abuses must have access to remedy.

This "Protect-Respect-Remedy" framework (Business & Human Rights Resource Centre, n.d.) sets out human rights due diligence, a process for identifying, preventing, mitigating, and accounting for human rights impacts. Despite the fact that the principles were welcomed by states, business actors and NGOs, the UNGP fall within the category of "soft law" (Assenza, 2025).

The non-binding character of this important soft law instrument has urged the global community to develop a binding internationally treaty. Since 2015, the Open-Ended Intergovernmental Working Group on transnational corporations and other business enterprises with respect to human rights (OEIGWG) has been drafting a UN Treaty on Business and Human Rights**,** with the latest version having been drafted in October 2025 (OHCHR, n.d.).

It is worth mentioning Article 8 of the draft Treaty which includes legal liability for legal and natural persons related to human right abuses, as well as Article 9 which states that a legal person is considered domiciled in any territory or jurisdiction in which it has, disjunctively, its:

- Place of incorporation or registration
- Principal assets or operations
- Central administration or management
- Or principal place of business or activity.

With this wording, territorial limitations seem to be mitigated, whereas restraining the doctrine of *forum non conveniens* meets reservations of participatory States, such as China, Brazil and Palestine.

In EU level, the scope of the Directive 2024/1760 (Directive on corporate sustainability due diligence) is to ensure that companies will address human rights impacts of their actions inside and outside Europe (Commission, 2024). Companies who intentionally or negligently fail to comply with the obligations set in the Directive are held civil liable, while the victims are eligible for full compensation. Alongside with national laws, such as Germany or France (DLA Piper, 2021), Europe is turning non-binding norms of UNGP into enforceable obligations.

The convergence of these international and regional frameworks show a common belief for shared responsibility. Performing state-like functions, private entities intersect with the obligation of States to protect human rights – a responsibility that seeks to burden private sector equally, from respecting human rights to protecting them. Collectively, they signal that private entities involved in digital warfare must operate within a framework of transparency, due diligence and respect for human dignity.

2.4 Access to Remedy and Enforcement Deficits in Cyber world

Related to the aforementioned tripartite of Protect-Respect-Remedy, corporate responsibility is increasingly recognized in normative level. Yet, if we don't ensure an effective remedy and consider it more than a procedural formality, human rights won't be protected efficiently.

Under international HRL, Article 8 of the UN Declaration and Article 2(3) of the ICCPR establish the right to an effective remedy against violations of rights, whereas in regional level Article 13 of the ECHR, Article 47 of the EU Charter and Article 25 of the American Convention on Human Rights safeguard the very same right.

In digital warfare, however, where speed, complexity and anonymity prevail, access to remedy can be constricted by technicalities and practicalities. Identifying the violator (whether a part of a company or an individual) can be difficult, let alone established the causal link between the harm suffered and the attacker. Algorithmic opacity and classification of information place individuals in disadvantageous position vis-à-vis both states and corporations.

This unfavorable position gets even more harmful, when the enforcement mechanism is rendered non-operational due to limited technological capacity. Even if issues, such as jurisdiction and extraterritoriality as mentioned before, can be settled, courts and institutions (*El-Masri v. the Former Yugoslav Republic of Macedonia*, 2012 - *Big Brother Watch and Others v. the United Kingdom*,2021) lack the expertise, tools or even the political independence to adjudicate claims involving security, defense or surveillance.

Private sector can offer a complementary protection, so as to counter this state-provided incapacity. End-to-end encryption deployed by Apple (Apple Inc., 2024) and Signal (Signal Messenger LLC, n.d.), transparency reports by Microsoft and platform-based mechanisms such as Oversight Board by Meta underscore the need for State mechanisms to

speed up with the progress. Otherwise, human rights protection may fall into the disposal of the private sector, totally in contrast with the public law authority set by HRL.

Part III Empirical Application, Challenges and Future Outlook

Chapter 1: Case Studies in Digital Warfare

The warfare landscape has transformed both by digital technologies and the privatization of cyber capabilities, reshaping the application of IHL and HRL. These developments are no longer merely theoretical conceptions but they are shaping our global order in our century.

In this chapter, through empirical application of what was mentioned before, we will see how a real cyber-attack demonstrates why neither IHL nor HRL alone is sufficient, with private entities exposing weaknesses in both regimes – thus making them crucial actors who can contribute with solutions, rather than creating problems at doctrinal and structural levels.

1.1 The NotPetya Attack

On June 27, 2017, major Ukrainian banks and government bodies announced a massive cyber-attack across the country. Hours later, reports of similar attacks across the Atlantic, affecting Canada and the United States, where a malware program locked computers, rendering them inaccessible (Cloudfare, n.d.).

Private experts estimated that the primary target was Ukraine, while other countries were affected as collateral damage, since the attack was affecting whomever does business in Ukraine (Borys, C. 2022).

A week after the attack, Ukraine's security services announced that there were traces of the attack that established a connection with Russia's security services - an allegation that Moscow denied, calling them unfounded (BBC.com 2017). A year later, CIA attributed the attack to Russian military hackers, considering it as an operation in the ongoing hybrid warfare of Russia against Ukraine, following the annexation of Crimea (Nakashima El. 2018).

Although no casualties or injuries were reported, the consequences of the attack were economic with the disruption of multinational corporations such as shipping and logistics causing losses estimated in billions of dollars.

However, the significance of the attack lies in the methods used (Krasznan C. 2020). Exploiting an officially approved tax return program in Ukraine, which was installed in the majority of the country's computers, the perpetrators of the attack demonstrated an upgraded version of the cyberattacks, exploiting civilian infrastructure.

From a legal perspective, the NotPetya case was not classified as a case of an armed attack, given experts, case law and analogous application of traditional frameworks related to self defence against kinetic attacks - thus, IHL applicability is contested. However, the attack demonstrated that foundational principles, such as distinction and proportionality were challenged in this privatized digital warfare, let alone attribution, a contentious subject, affected by technicalities and political considerations.

In terms of HRL, right to privacy, to property, to health and in some cases to life were affected, due to the widespread disruption of essential services, illustrating that even outside armed conflicts, humanitarian harm can be achieved. The victims of this harm, however, face difficulties in accessing effective remedies, due to the diffused attribution, the complexity of the attack and the political sensitivity.

Ultimately, NotPetya is regarded as a turning point: a demonstration that cyber operations can produce global civilian harm without crossing traditional thresholds, and that the privatization of response mechanisms has outpaced the adaptation of international law, with private entities being perpetrators (either state sponsored or not), victims as well as first responders.

Against the slow adaptation of state-centered frameworks, private actors seek to fill regulatory gaps on their own. Microsoft is an illustrative example, by proposing its bold

vision for an international binding treaty, a proposal that attracted attention and considered by many as a necessity of the 21st century (Guay & Rudnick, 2017).

1.2 Microsoft's "Digital Geneva Convention" Proposal

Around the same period as the NotPetya attack, Brad Smith, President and Chief Legal Officer of Microsoft, advanced his proposal for a *Digital Geneva Convention*, a set of principles to protect civilians from cyber-attacks (Smith 2017). To support his vision, he invoked the legacy of ICRC, calling tech companies to function as Digital Switzerland.

The Convention could be considered as a call for establishing norms developed in the last twenty years in cyber space. Through the cooperation of private and public sector, civilian infrastructure and intellectual property must be safeguarded. Moreover, he urged for the creation of an analogous to the International Atomic Energy Agency institution, in which experts from the private and public sector would participate, so as cyber-attacks to be assessed independently.

The importance of such a notion lies not in its potential binding force, but in its function as an example of a collaborative state-private entrepreneurship. Private actors have the capacity building, the resources and the innovative spirit to advance further and faster – these are the qualitative and quantitative elements that governments must take advantage of, so that normative gaps be mitigated.

However, this proposal was met with substantial criticism. Experts of the CCD COE (CCD COE, 2017) claimed that such a proposal is both legally confusing and politically unrealistic. Devoting effort to achieve a universal binding framework could be counterproductive, given the unfortunate, yet learning, experience of accepting what UN claimed since 2013, about the application of international law to cyberspace – instead, adapting (Piper, 2018) existing frameworks into modern standards, improving resilience of

infrastructure and amplifying the condemnation of human rights violation can have a gradual progress for the public sector to be up to date (Jeutner, 2019).

This mixed reception of Microsoft's proposal is indicative of the broader tug-of-war between the traditional state centered development of international law and the innovative-driven norm setting advanced by private actors.

1.3 Structural Implications of Privatized Digital Warfare

The examination of the NotPetya attack and Microsoft's proposal for a Digital Geneva Convention shows the broader shift of the execution and regulation of digital conflicts, with the consequential implications in international law – privatization is not an isolated development but an inseparable trait of the new era we have entered.

The classical IHL regimes of two distinctive categories, combatants and non-combatants and the traditional principles of distinction, proportionality and attribution, when combined with the diffused nature of internet and the interconnectedness of civilian and military infrastructure, are illustrative of how future wars will unfold.

Alongside with HRL, consequences of the attacks can extend beyond the theater of operations. Indiscriminate operations, the dominance of dual-use infrastructure and the lack of technical expertise are surrounding individuals with dangers, for which no effective remedies exist.

This structural tension is enhanced due to the fact that, on the one hand, private entities are indispensable to the designing, operating and monitoring the use of the digital environment while on the other hand they use their commercial dynamic position in order to form policies – a dangerous combination which could open Pandora's Box, with States bearing a responsibility of a power that is not in their hands.

Hybrid conflicts (such as NotPetya is considered to be part of Russia's hybrid war) demonstrate that privatizing warfare extends far beyond outsourcing logistics or

technology—it transforms the very architecture of accountability, the root of the problematic co-existence of private and public cooperation. Yet, diffusing power isn't accompanied by the same diffusion of responsibility - effective security and human rights in the digital era depend not only on state restraint but on the ethical and legal accountability of the private sector itself.

In this effort of filling potential *legal lacunae*, existing frameworks of IHL and HRL, while conceptually resilient, require adaptation to this new ecosystem. Otherwise, the future regulation of digital warfare, interacting with Artificial Intelligence, risks exacerbating existing weaknesses, with significant repercussions for civilian protection and effective application of international law.

Chapter 2: Challenges and Future Outlook

2.1 Accountability

Through the real-world cases presented in the previous Chapter, it was revealed that the central challenge of the privatized digital warfare lies not in the absence of binding legislation but the contemporary distribution of power. In the digital domain, the ability of States to exercise effective control over their actors, by monitoring and regulating their operation in the conflict (a condition for the effective application of IHL and HRL) is challenged.

States remain formally accountable for the misconduct of private actors, yet the participation of the latter in critical quasi-state functions, from national security to energy infrastructure, complicates their relationship. Their commercial orientation increases this complexity, blurring even more the gray zone of their operation, thus expanding the gap between responsibility and control, and ultimately weakening attribution.

In essence, even where attribution is possible in terms of technical feasibility, obstacles such as evidentiary thresholds, the transnational nature of the internet and political

considerations transform the gap from a procedural hindrance into a systemic challenge, without transforming responsibility into accountability.

The result seems drawn from a dystopian movie scenario – a fragmented digital governance, trying to keep up with the rapid innovation of a limited powerful *elite* of private actors, while societies, individuals and fundamental human rights fall prey to the commercial and unethical interests of the algorithmic decision-making.

Yet, this course is not irreversible. The same private actors whose technological superiority challenges the international status-quo, they also have the expertise, the resources and the global reach to mitigate the effects. Through human rights due diligence mechanisms, they can contribute to the global community, by establishing transparency, attribution and remedy processes. By enhancing their role, not as adversaries of the States but as fellow soldiers in this battle against digital challenges, companies can function as complementary tools, especially in domains where private innovation surpasses the traditional regulatory inertia of the states.

2.2 Outsourcing: a double-edged sword

Before advancing to this adaptation of our modern status quo, we should take into account two factors: firstly, why outsourcing of state function must be a part of a holistic strategy and not a last-minute and reflexive choice and secondly, how do future/present trends affect it, with Artificial Intelligence conquering our lives.

In the current broader political and economic environment, outsourcing of state functions is a piece of evidence for the efforts of States to keep up with private innovation. By saving money and facilitating the management of working time of public sector, delegating private actors can be a catalyst in meeting the evolving needs of the citizens. Through this state-private collaboration, the financial sector is expected to developed, with more innovation and more working places to be advanced (Gordon & Walsh, 1997).

However, there are considerations for which governments should be proactive, because, by mitigating risks, the result of the cooperation can be useful not only for the citizenry as a whole but for private economy as well (Council of the European Union, 2023).

Firstly, the participation of private actors in domains such as security, surveillance and defense can create public scrutiny, since, reflectively, whenever companies work with the governments, it is considered for the benefits of the former at the expense of the latter, and specifically of the citizens. Notwithstanding with the ambiguous (thus democratically deficient) status of such companies, the case of the Wagner Group, a private military company with close relations to the Russian government, despite the mixed reactions of public officials (Larsen, 2025), proves that public skepticism about public-private authority is not unfounded.

What is more, during national emergency crisis, such as armed conflicts, this diffusion of responsibilities can lead to the erosion of effective state control, a *sine qua non* factor for the application of IHL and HRL. Additionally, an ineffective performance during an armed attack can have catastrophic consequences for a state, since a complicated coordination between financial-driven companies and weakened sovereign state mechanisms can delay operational responses and undermine defense capabilities.

Ultimately, the structure and the *raison d'etre* for PSMCs are based on the existence of threats to national security and conflicts. This could lead to a misalignment of incentives (Baum & McGahan, 2009) – on the one hand, States struggling for the respect of rule of law, fundamental human rights, peace and prosperity while on the other hand their private collaborators approach operations with financial criteria.

Excluding private actors from digital services is neither a realistic solution nor a panacea. These risks just emphasize the need for imposing clear terms in this collaboration, without turning it into an augmenting factor of exploiting governance vulnerabilities.

2.3 Artificial Intelligence

When Antonio Guterres, the UN Secretary General, addressed (UN Press, 2025) the Security Council open debate on Artificial Intelligence and International peace and Security by claiming that "the question is not whether AI will influence international peace and security, but how we will shape that influence", it highlights that AI is no longer a future trend, but a part of our reality.

The next years, AI will be testing the adaptability of traditional regimes more than any technology has so far, in human history. Especially, AI in warfare is already changing the boundaries of battlefields. AI technology weapon systems can detect, analyze and form a command autonomously, making the decision process a millisecond procedure. Private companies can contribute with precise targeting and minimizing civilian/collateral harm.

However, depending on the levels of autonomy, the ability of algorithmic systems to determine who or what is targeted, questions arise regarding the legality and ethics (Klaus, 2024) around the warfare, with the principles of IHL and HRL being challenged even more. For the misidentification of a target or the disruption of dual use infrastructure, done autonomously without the proper application of the IHL principles, who bears responsibility: the programmer, the operator, or the state that harbors the private company?

What is more, the access of the companies in the vast amounts of data, unlike the State, can reverse the superiority of States as the primary and effective gatekeepers of the use of force. By depending more and more on private infrastructure and capacity, it could lead to the neutralization of States on forming, independently, national policies. A weakened State can result in an uncontrolled algorithmic process of what information is visible, depending on moderation mechanisms, thus influencing human rights such as freedom of expression[28].

[28] UN GA A/89/341

Challenges relevant to the data sovereignty, such as the algorithmic biases and the monetization of personal data (McKinsey & Company, n.d.) can create discriminatory practices, leading to violations of human rights, such as privacy, freedom of expression and ultimately, life.

As reliance on AI technologies increases, the existing challenges of digital warfare (as analyzed so far) are amplified, since AI does not, mostly, new legal problems but expands traditional ones. This is the reason why adaptation (or *shaping the influence* as Secretary Guterres said) of regulatory and institutional responses must be expedited, in an environment where private technological capacity is running with astronomical speed.

2.4 Policy and Legal Recommendations

This ambitious but necessary adaptation of existing frameworks is a multi-faceted process, demanding joint actions in state, companies and citizen level. Advanced technologies, infused by Artificial Intelligence, are considered, for the first time in human history, to be so dangerous that could cause human extinction (Watson, 2025).

In light of these findings, several practical and normative recommendations emerge, in regulatory, corporate and civilian level, since the worldwide collaboration of all stakeholders, (individuals, governments, institutions and corporations) is crucial, and vigilance is key.

In normative level, ongoing initiatives should develop into more tangible results. The efficient completion of the aforementioned draft for a legal binding UN Treaty on Business and Human Rights is a good step towards the recalibration of traditional framework. The absence, however, of terms within the draft, such as *cyber* or *digital* (instead, the word *transnational* is used) could be a hindrance in a without reservations application to digital world.

Instead of trying to reinvent the wheel, refinements of in effect frameworks should be prioritized. As CCD COE experts claimed, achieving universal consensus can be chimeric – what if this effort could aim for the creation of a new protocol, an annex to the Geneva Conventions that could clarify the application of humanitarian principles in cyberspace, having taken into account state practice, thus reflecting customary law as well? Such a text would codify obligations related to cyber targeting, dual-use infrastructure, and the participation of private entities, now being described in soft law instruments such as Tallinn Manual, functioning as an interpretive and moral tool for all stakeholders.

Additionally, applicable provisions, such as Article 36 of the Additional Protocol I to the Geneva conventions can function as a tool for meticulous assessment of any new weapon's development or manufacturing, digital sphere included. Even in the export of goods, there are initiatives, such as the Wassenaar Agreement, which promotes transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies.

Supplementarily, legal frameworks outside armed conflicts can contribute into developing a holistic approach. The International Law Commission's Draft Principles on the Protection of the Environment in Relation to Armed Conflicts (2022), though environmental in focus, affirm that corporations operating in conflict zones bear heightened due diligence responsibilities.

In corporate level, what the EU Directive on corporate sustainability due diligence obliges, should be a normal practice. Due diligence processes should be established in all corporates providing cyber services, intelligence and dual-use technologies, since, by incorporating human right standards, the possibility of future misuse of technology would be diminished.

As for the Artificial Intelligence in warfare context, methods like Collateral Damage Estimate Methodology (CDEM) of Schmitt (2013) could program a machine, so as to estimate the collateral damage, and the higher the probability of it, the higher the required level of command for approval. Autonomy should be subject to human-in-the-loop[29] requirements to preserve meaningful control and accountability and abolish any possibility of fully autonomous weapons[30].

In terms of accountability, the main challenge of digital warfare, states and corporations should share responsibility where actions are jointly undertaken or mutually dependent. Contract-based agreements should have clauses and security protocols for cyber operations. Monitoring mechanisms should be reinforced through the establishment of an independent oversight body[31], consisting of experts from government, tech companies and civil society either in regional or national level, which could ensure the constant assessment of the outsourcing collaboration, demanding compliance and attributing liability.

This multi-layered cooperation can lead to the public disclosure through transparency reports that could lead to efficient, and thus democratic, supervision, reduce public scrutiny and ensure the function of a democratic society.

Ultimately, when it comes to the non-state or corporate individuals, education is the cornerstone of each endeavor related to human. Being online has become modern human's second nature. The Council of Europe, through its Education Department and the Digital Citizenship Education project highlighted some digital domains of this engagement in the modern dimension: access and inclusion, learning and creativity and media/information

[29] For the full analysis of the different categories, see also B. Docherty, '*Losing Humanity: The Case Against Killer Robots'*, Human Rights Watch (November 2012)
[30] For more analysis on the relevant campaign, see also https://www.stopkillerrobots.org/about-us/
[31] Lessons taken from the application of Data Protection frameworks, such as the GDPR provisions for national bodies as well as the appointment of Data Protection Officers in lower organization level

literacy. It is relevant with what Habermas[32] conceptualized about public sphere – participation, nondiscrimination, autonomy and rational critical discourse.

By empowering people of all ages with the necessary knowledge, we can acquire the competences and increase our defenses against any malevolent digital action. This active participation in the digital realm is crucial, as it promotes both informed decision-making and ensures that democratic values are upheld within the digital space.

All these proposals have at least one common element - the vigilance against a fast evolving global theater of operations. Policies should not solely provide reactive measures but anticipatory responses. By preserving accountability in an era where power is increasingly networked rather than centralized, the recalibration of international stakeholders' behavior (through normative and operational interventions) would not merely modernize international law—it would restore its normative authority.

[32] He considered the public sphere as ideally a platform where everyone (regardless of class, income, creed, gender, race and ethnicity) has a right to sit and share ideas with others on any socio-economic and political issues that are of public interest and concern, through fearless critical and 'rational' debate". Habermas, J., Lennox, S., & Lennox, F. (1974). The Public Sphere: An Encyclopedia Article (1964). *New German Critique*, 3, 49-50. https://doi.org/10.2307/487737

Conclusion

In his political farewell speech in 1961, President Dwight Eisenhower spoke about the dangers of the military-industrial complex, emphasizing the need for an alert and knowledgeable citizenry, so that security and liberty may prosper together[33]. Despite the absence of the digital context in those years, the same fears can be applied for every new challenge that future holds.

Since we live in a network society, as Manuel Castell (1996) claims, the whole social structure has changed. But now, it is not what theory is needed. The debates on whether we have the Web 1.0, 2.0 or 3.0 (Shivalingaiah & Naik, 2008) or whether McLuhan's Technological Determinism (1964) or Williams' Social Shaping Theory (1996) prevails, seem to be outdated.

This digitalization of our lives has influenced warfare as well, by redefining the distribution of power and responsibility in global security governance. Once a strictly state-driven domain, the increasing dependency on the private domain for expertise, resources and operational execution has led to a privatization of war, which exposes the structural durability of IHL and HRL. These traditional frameworks, drafted and applied for kinetic operations, are called to regulate behaviors in the digital domain, which is characterized by speed, anonymity and transborder nature.

This thesis examined how this privatization complicates the compliance with IHL and HRL in digital warfare, revealing that while law remains formally applicable, its effectiveness is undermined by the structural and normative shifts of the digital era. Fundamental principles and human rights, anchored in the very essence of human dignity, ethics and collective responsibility, are put in challenge. As a solution, the redefinition of

[33] His speech can be retrieved in https://www.archives.gov/milestone-documents/president-dwight-d-eisenhowers-farewell-address

existing notions, such as accountability, seems the only method to contribute to the empowerment of traditional frameworks against the dynamics of the advanced age.

The analysis traced the phenomenon from its origins in the outsourcing of military and intelligence functions to the present configuration of digital conflicts, in which private actors operate as designers, operators and supervisor of cyber operations. Consequently, the lines of accountability are increasingly blurred and mechanisms of traditional law struggle to keep pace with technological evolution.

Two are the main findings of the thesis: a) the erosion of the public-private divide and b) the disruption of accountability, both defined as disruptions of international law.

The interconnectedness of public and private sector has been augmented in the digital domain. The inequality of resources and expertise in state level has led the latter to develop outsourcing policies, in functions which traditionally were state governed, such as defence and security. The reality is that private corporations control the vast majority of the data and infrastructure, offering digital services. When private actors design, maintain, or defend military-grade cyber systems, they become operationally embedded in conflict rather than supporting operations. This fusion of roles challenges the application of one of the cornerstones of IHL — the distinction between combatants and civilians.

Accountability seems to be the main concern and challenge of privatizing warfare. While States are the traditional sovereign key players under international law, the complexity of cyber operations challenges the accountability structure. Regimes such as the *effective control* need adaptation. Otherwise, outsourcing functions to unsupervised private entities can result in serious dangers for the democratic function of societies.

In this challenging theater of operations, HRL is presented as a complementary lens through which protection can be safeguarded. Unlike IHL, HRL is applied in all

circumstances, below the threshold of armed conflict included, offering a multilayered assessment of behaviors of all stakeholders.

What is more, institutions (such as CCD COE of NATO) as well as corporations design their strategies, by proposing and integrating into their policies, good practices and mechanisms, through which due diligence standards function as a driving force in organizing levels. Alongside the ongoing normative procedures, such as the draft of a UN Treaty on Business and Human Rights or proposals such as Microsoft's vision for a Digital Geneva Convention, represent progress, but demand political expediency and corporal interests to align with real goals – the effective regulation of digital domain.

Ultimately, the thesis revealed that Artificial Intelligence works as a catalyst, intensifying the challenges, with algorithmic autonomy questioning even more the notions of control and liability. The privatization of warfare is not considered an isolated phenomenon – it is an aspect of the evolution to a hybrid governance, between states and private actors, with the latter being indispensable partners (and in some cases the dominant key players) in domains such as data sovereignty and critical digital infrastructure.

This is the reason why this thesis functions as a junction between digital transformation and international legal analysis. On the one hand, it shows how technological advancement signifies not just a partial technical evolution of specific domains – on the contrary, it is a widespread redistribution of power and thus authority, from state centered structures to decentralized private ecosystems. In this new reality, traditional notions are undergo assessment and the need of their adaptation is (or should be) constantly under monitoring.

On the other hand, it shows the fragility of fragmented normative responses against new threats. The complementarity of IHL and HRL, as well as regional and national initiatives, both of binding and soft law nature, increase the resilience and safeguards

fundamental principles, thus creating a vigilant responsive mechanism against malevolent actors. At the same time, judicial decisions show that the omnipotence of the private actors can be harness for the sake of security and protection (Politico, 2025).

In this current technological disruption, human rights are the ethical compass which will drive humanity through these uncharted waters. The need for translation in a new, digital *alphabet*, which will consist of algorithms, *black boxes* and automated code, is present. To paraphrase a Hollywood quote, *with greater power comes greater responsibility*. Yet, in this ominous future, the task for us and the coming decades is not to discard traditional law but to recalibrate it, aligning its structures with the realities of a world where sovereignty, security, and technology are inseparable. Privatizing digital warfare does not merely complicate compliance with existing law; it challenges the very ontology of responsibility. When power is distributed among code, corporations, and states, responsibility must follow the same distributed logic, so as to balance state sovereignty, security, and accountability.

Ultimately, both states and private actors, in macro and micro level, are obliged morally to collaborate so as to ensure respect for IHL and HRL in the digital era, far from political and economic expectancies. The legitimacy of the digital order will rest not on who controls the most advanced technology, but on who wields it with the greatest fidelity to human dignity. By continuing to adapt, the international community may succeed in mitigating the chaos of Pandora’s Box and ensure a safer digital future.

References

Amnesty International. (2021). *Forensic methodology report: How to catch NSO Group's Pegasus*. https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus

Apple Inc. (2020). *Apple human rights policy*. https://www.apple.com/compliance/pdfs/Apple-Human-Rights-Policy.pdf

Apple Inc. (2024). *iCloud data security overview*. Apple Support. https://support.apple.com/en-us/102651

Assenza, E. (2025). From international "soft" law to law in business and human rights: The role of the UNGPs in the development of formal sources of international law. In *Business and human rights* (pp. 13–54). https://doi.org/10.1163/9789004715158_003

Astran. (n.d.). Cyber mercenaries: Who, why, for who. https://www.astran.ai/blog/cyber-mercenaries-who-why-for-who

Baum, J. A. C., & McGahan, A. (2009). Outsourcing war: The evolution of the private military industry after the Cold War. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.1496498

BBC News. (2017, July 2). Russia behind cyber-attack, says Ukraine's security service. https://www.bbc.com/news/world-europe-40471310

Biden, J. (2023). *National cybersecurity strategy*. The White House. https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

Borys, C. (2022, February 24). The day a mysterious cyber-attack crippled Ukraine. *BBC Future*. https://www.bbc.com/future/article/20170704-the-day-a-mysterious-cyber-attack-crippled-ukraine

Business & Human Rights Resource Centre. (n.d.). Governing business & human rights: Human rights due diligence and impact assessment. https://www.business-humanrights.org/en/big-issues/governing-business-human-rights/human-rights-due-diligence-impact-assessment

Business & Human Rights Resource Centre. (n.d.). The "Protect, Respect and Remedy" framework. https://media.business-humanrights.org/media/documents/files/reports-and-materials/Ruggie-protect-respect-remedy-framework.pdf

Carnegie Endowment for International Peace. (2025). *Private tech companies, the state, and the new character of war*. https://carnegieendowment.org/research/2025/12/ukraine-war-tech-companies?lang=en

Castells, M. (1996). *The information age: Economy, society, and culture. Volume 1: The rise of the network society*. Wiley-Blackwell.

CCDCOE. (n.d.). NATO Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org/

CISA. (n.d.). Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/

Citizen Lab. (2018). *NSO Pegasus: Technical analysis and leaked documents*. DocumentCloud. https://embed.documentcloud.org/documents/4599753-NSO-Pegasus/

Cloudflare. (n.d.). *What are Petya and NotPetya?* https://www.cloudflare.com/learning/security/ransomware/petya-notpetya-ransomware/

Commission européenne. (n.d.). Vos droits fondamentaux dans l'UE. European Commission. https://commission.europa.eu/aid-development-cooperation-fundamental-rights/your-fundamental-rights-eu_en

Control Engineering. (n.d.). Throwback attack: Three teens stoke fears of a cyber war with the Solar Sunrise attack. https://www.controleng.com/throwback-attack-three-teens-stoke-fears-of-a-cyber-war-with-the-solar-sunrise-attack

Council of Europe. (n.d.). The Council of Europe at a glance. https://www.coe.int/en/web/portal/the-council-of-europe-at-a-glance

Council of the European Union. (2023, August 31). *The business of war: Growing risks from private military companies* (ART Research Paper). https://www.consilium.europa.eu/media/66700/private-military-companies-final-31-august.pdf

Coupland, R. (2001). Humanity: What is it and how does it influence international law? *International Review of the Red Cross, 83*(844), 969–989. https://doi.org/10.1017/S156077550018349X

Court of Justice of the European Union. (2013). *Åklagaren v. Hans Åkerberg Fransson*, Case C-617/10, Judgment of 26 February 2013. https://curia.europa.eu/juris/document/document.jsf?docid=134202

Cvetko, J. (2025, October 22). *Microsoft Digital Defense Report 2025: Extortion and ransomware drive over half of cyberattacks*. Microsoft News

Dealbreaker. (2025). *Palantir, Meta, OpenAI execs to commission into Army Reserve, form "Detachment 201"*. https://dealbreaker.com/2025/06/palantir-meta-openai-execs-to-commission-into-army-reserve-form-detachment-201

Digital Strategy of the European Commission. (n.d.). EU cybersecurity strategy. https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy

Docherty, B., Neunschwander, E., Karir, M., & Flinner, K. (2012). *Losing humanity: The case against killer robots*. Human Rights Watch.

DLA Piper. (2021, March). Human rights due diligence legislation in Europe. https://www.dlapiper.com/en/insights/publications/2021/03/human-rights-due-diligence-legislation-in-europe

Enisa. (n.d.). European Union Agency for Cybersecurity. https://www.enisa.europa.eu/

European Court of Human Rights. (1998). *Guerra and Others v. Italy*, Application No. 14967/89, Judgment.

European Court of Human Rights. (2003). *M.C. v. Bulgaria*, Application No. 39272/98, Judgment

European Court of Human Rights. (2004). *Öneryıldız v. Turkey*, Application No. 48939/99, Judgment (Grand Chamber).

European Court of Human Rights. (2012). *El-Masri v. the Former Yugoslav Republic of Macedonia*, Application No. 39630/09, Judgment (Grand Chamber).

European Court of Human Rights. (2021). *Big Brother Watch and Others v. the United Kingdom*, Applications Nos. 58170/13, 62322/14, and 24960/15, Judgment (Grand Chamber).

Goga, R. (2024). Hired guns in Sierra Leone: Mercenaries' enthralling role. *Studia Universitatis Babeș-Bolyai Studia Europaea*, 337–367. https://doi.org/10.24193/subbeuropaea.2024.2.15

Gordon, M. L., & Walsh, T. P. (1997). Outsourcing technology in government: Owned, controlled, or regulated institutions. *Journal of Government Information, 24*(4), 267–283. https://doi.org/10.1016/S1352-0237(97)00026-9

Guay, J., & Rudnick, L. (2017, June 25). *What the Digital Geneva Convention means for the future of humanitarian action*. UNHCR Innovation Service. https://www.unhcr.org/innovation/digital-geneva-convention-mean-future-humanitarian-action/

Habermas, J., Lennox, S., & Lennox, F. (1974). The public sphere: An encyclopedia article (1964). *New German Critique, 3*, 49–50. https://doi.org/10.2307/487737

ICRC. (n.d.). IHL and private military and security companies: FAQ. https://www.icrc.org/en/document/ihl-and-private-military-security-companies-faq

ICRC. (n.d.). ICRC casebook glossary. https://casebook.icrc.org/a_to_z/glossary

International Court of Justice. (1986). *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*, Merits, Judgment. *I.C.J. Reports 1986*, 14. https://www.icj-cij.org/case/70

International Court of Justice. (1996). *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, ICJ Reports 226. https://www.icj-cij.org/public/files/case-related/95/095-19960708-ADV-01-00-EN.pdf

International Court of Justice. (2005). *Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda)*, Judgment. *I.C.J. Reports 2005*, 168. https://www.icj-cij.org/case/116

International Criminal Tribunal for the Former Yugoslavia. (1999). *Prosecutor v. Duško Tadić*, Case No. IT-94-1-A, Appeals Chamber Judgment. https://www.icty.org/x/cases/tadic/acjug/en/tad-aj990715e.pdf

Jeutner, V. (2019). The Digital Geneva Convention. *Journal of International Humanitarian Legal Studies, 10*(1), 158–170. https://doi.org/10.1163/18781527-01001009

Klaus, M. (2024, September 24). *Transcending weapon systems: The ethical challenges of AI in military decision-support systems*. International Committee of the Red Cross (ICRC) – Humanitarian Law & Policy Blog. https://blogs.icrc.org/law-and-policy/2024/09/24/transcending-weapon-systems-the-ethical-challenges-of-ai-in-military-decision-support-systems/

Kott, A., Swami, A., & West, B. J. (2016). The Internet of Battle Things. *Computer, 49*(12), 70–75.

Krasznan, C. (2020). Case study: The NotPetya campaign. In B. Török (Ed.), *Információ- és kiberbiztonság* (pp. 485–499). Ludovika Egyetemi Kiadó.

Krieg, A. (2018). *Defining remote warfare: The rise of the private military and security industry*. Remote Warfare Programme.

Larsen, K. P. (2025, January 9). *The rise and fall of the Wagner Group: Russia is seeking control over its 'private' military companies*. Danish Institute for International Studies (DIIS). https://www.diis.dk/en/research/the-rise-and-fall-of-the-wagner-group

Learn Microsoft. (2018). FY18 security engineering strategy brief. https://learn.microsoft.com/en-us/security/engineering/fy18-strategy-brief

Le Moli, G. (2021). Human dignity in international humanitarian law. In *Human dignity in international law* (pp. 173–215). Cambridge University Press. https://doi.org/10.1017/9781009042765.005

Loonam, J. P., & Andreoli, R. J. (2025). *Extraterritoriality: The US perspective*. In The Practitioner's Guide to Global Investigations (10th ed.). Global Investigations Review. https://www.lexology.com/indepth/guide/the-practitioners-guide-global-investigations/2026/article/extraterritoriality-the-us-perspective

McAlpine, M. (2025, October 6). *Palantir's military role in Israel and Britain*. Bella Caledonia. https://bellacaledonia.org.uk/2025/10/06/palantirs-military-role-in-israel-and-britain/

McKinsey & Company. (n.d.). Intelligence at scale: Data monetization in the age of generative AI. https://www.mckinsey.com/capabilities/business-building/our-insights/intelligence-at-scale-data-monetization-in-the-age-of-gen-ai

McLuhan, M. (1964). *Understanding media: The extensions of man*. Gingko Press.

Microsoft. (2022, May 3). How Microsoft's Digital Crimes Unit fights cybercrime. https://news.microsoft.com/on-the-issues/2022/05/03/how-microsofts-digital-crimes-unit-fights-cybercrime

Microsoft. (2025). *Microsoft Digital Defense Report 2025: Extortion and ransomware drive over half of cyberattacks*. https://news.microsoft.com/source/emea/features/microsoft-digital-defense-report-2025-extortion-and-ransomware-drive-over-half-of-cyberattacks-2/

Microsoft. (n.d.). Microsoft Defender Threat Intelligence. https://www.microsoft.com/en-us/security/business/siem-and-xdr/microsoft-defender-threat-intelligence

Milano, E. (2013). *The deterritorialization of international law*. ESIL Reflections, 2(3). https://esil-sedi.eu/post_name-627/

Nakashima, E. (2018, January 12). Russian military was behind 'NotPetya' cyberattack in Ukraine, CIA concludes. *The Washington Post*. https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html

NATO Allied Command Transformation. (n.d.). Multi-domain operations. https://www.act.nato.int/activities/multi-domain-operations/

OCCRP. (n.d.). Where NSO Group came from and why it's just the tip of the iceberg. *Organized Crime and Corruption Reporting Project*. https://www.occrp.org/en/project/the-pegasus-project/where-nso-group-came-from-and-why-its-just-the-tip-of-the-iceberg

OHCHR. (2022, June). Extraterritorial application of human rights requires multilateral approach. *Office of the United Nations High Commissioner for Human Rights*. https://www.ohchr.org/en/press-releases/2022/06/extraterritorial-application-human-rights-requires-multilateral-approach-un

Piper, A. (2018). *Does the world need a digital Geneva Convention?* International Bar Association. https://www.ibanet.org/article/6FE8BE6C-D73C-42B6-BE50-5CE0781138A2

Politico. (2025, May 6). *Israeli spyware giant NSO Group ordered to pay nearly $170M to WhatsApp for hacking accounts*. M. Miller. https://www.politico.com/news/2025/05/06/nso-group-pegasus-whatsapp-hack-170-million-damages-00332155

QIL-QDI. (n.d.). The future of the articles on state responsibility: A matter of form or of substance? *Questions of International Law*. https://www.qil-qdi.org/the-future-of-the-articles-on-state-responsibility-a-matter-of-form-or-of-substance/

Schondorf, R. S. (2005). Extra-state armed conflicts: Is there a need for a new legal regime? *New York University Journal of Law and Politics, 37*(1), 1–62.

Scahill, J. (2007). *Blackwater: The rise of the world's most powerful mercenary army*. Nation Books.

Schmitt, M. N. (2013). Autonomous weapon systems and international humanitarian law: A reply to the critics. *Harvard National Security Journal, Features Online*, 1–21. https://doi.org/10.2139/ssrn.2184826

Shivalingaiah, D., & Naik, U. (2008, February 28). Comparative study of Web 1.0, Web 2.0 and Web 3.0. https://www.researchgate.net/publication/264845599_Comparative_Study_of_Web_10_Web_20_and_Web_30

Signal Messenger LLC. (n.d.). *Is it private? Can I trust it?* Signal Support. https://support.signal.org/hc/en-us/articles/360007320391-Is-it-private-Can-I-trust-it

Smith, B. (2017, February 14). *The need for a Digital Geneva Convention*. Microsoft On the Issues. https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/

The Guardian. (2021, July 18). What is Pegasus spyware and how does it hack phones? *The Guardian*. https://www.theguardian.com/news/2021/jul/18/what-is-pegasus-spyware-and-how-does-it-hack-phones

The Guardian. (2025, June 30). *Peter Thiel's Palantir poses a grave threat to Americans*. R. Reich. https://www.theguardian.com/commentisfree/2025/jun/30/peter-thiel-palantir-threat-to-americans

The Montreux Document. (2009). *The Montreux Document on pertinent international legal obligations and good practices for States related to operations of private military and security companies during armed conflict*.

Tougas, M.-L. (2009). Some comments and observations on the Montreux Document. *Yearbook of International Humanitarian Law, 12*, 321–345. https://doi.org/10.1017/S1389135909000129

Trottier, D. (2016). Digital vigilantism as weaponisation of visibility. *Philosophy & Technology, 30*(1), 55–72. https://doi.org/10.1007/s13347-016-0216-4

United Nations Foundation. (2023). The Universal Declaration of Human Rights is turning 75: Here's what you need to know. *United Nations Foundation*. https://unfoundation.org/blog/post/the-universal-declaration-of-human-rights-is-turning-75-heres-what-you-need-to-know

United States Space Force. (2024). Cyber expo highlights latest developments in fifth domain of warfare. https://www.ssc.spaceforce.mil/Newsroom/Article/4171028/cyber-expo-highlights-latest-developments-in-fifth-domain-of-warfare

United24 Media. (2025). *Palantir, the secretive tech giant shaping Ukraine's war effort*. D. Kosoy. https://united24media.com/war-in-ukraine/palantir-the-secretive-tech-giant-shaping-ukraines-war-effort-5519

U.S. Cyberspace Solarium Commission / American University. (n.d.). The evolution of cyber attribution. *American University, School of International Service*.

https://www.american.edu/sis/centers/security-technology/the-evolution-of-cyber-attribution.cfm

Vakulina, S. (2025, September 5). *Tackling Russia's hybrid war on Europe: Jamming and spoofing in the "grey zone"*. Euronews. https://www.euronews.com/2025/09/05/tackling-russias-hybrid-war-on-europe-jamming-and-spoofing-in-the-grey-zone

Watson, G. (2025). A godfather of AI remains concerned as ever about human extinction. *The Wall Street Journal*. https://www.wsj.com/articles/a-godfather-of-ai-remains-concerned-as-ever-about-human-extinction-ec0fe932

Williams, R., & Edge, D. (1996). The social shaping of technology. *Research Policy*, *25*(6), 865–899. https://doi.org/10.1016/0048-7333(96)00885-2

WIRED. (2019). *What does Palantir actually do?* C. Haskins. https://www.wired.com/story/palantir-what-the-company-does/