The increasing pace of development of current and future information technologies drastically changed the character of warfare and brought multiple challenges to human rights and humanitarian law. This thesis examines the global impact of digital warfare on privacy, freedom of expression, and civilian in/security, while analysing the legal and ethical challenges presented by cyber operations, misinformation strategies, and autonomous systems. Through the investigation of real-world case studies (e.g., Stuxnet, NotPetya, as well as Russian cyber strategies in Ukraine), the study highlights the vulnerabilities of essential infrastructures as well as the indiscriminate manner of cyber-attacks. Digging deeper, the paper notes critical limitations in IHL and IHRL standards in the face of specific digital conflicts, leading to the conclusion that existing legal frameworks are insufficient to address the unique legal problems raised by digital warfare. It also systematically analyses, for instance, the Tallinn Manual, a collective project of legal experts that emerged in this emergent conversation, to repurpose these frameworks to address the complexities of cyberspace. Recommendations include the creation of binding international treaties on how AI will be used and enhanced attribution mechanisms for actions taken by machines against human actors, as well as codes of ethics for the development of AI-based technologies to outline consequences of actions taken against human actors in conflict scenarios. The thesis ends with an appeal for multilateral engagement, creative public policy responses, and a sensible balance of security interests and the preservation of human rights. First, a better understanding of these challenges would empower the international community to promote a more stable, ethical, and resilient digital landscape in an age of extraordinary technological transformation.

Warfare in the Digital Era and its effect on human rights and Humanitarian Law

Athanasios Doukas

Table of Contents

I. Introduction

Background and Context

Warfare has always been closely connected with technological advancements[1]. They have always played a significant role in warfare. The adoption of iron weapons, like swords, spears and arrows, in the ancient world, the introduction of gunpowder weapons, like muskets and cannons, in the late medieval era and the incorporation of howitzers, machine guns and nuclear weapons in militaries during and after the two world wars of the 20th century show the effect of technology on warfare.[2] Today, we can observe more and more weapon systems that incorporate or exploit digital technologies and tools.

The 21st Century: The War in Cyberspace

The 21st century saw the advent of war in a digital domain. Digital warfare encompasses the utilization of cyber capabilities, artificial intelligence (AI), big data, autonomous weapons, and surveillance technologies to reach military or political goals.[3] Digital warfare, in contrast with many of its predecessors, is fought remotely, often invisibly and without kinetic harm, which distinguishes it from older forms of warfare.[4]

Digital technologies now constitute an essential component of both offensive and defensive military operations. Today, state and non-state actors utilize cyber-attacks to render critical infrastructure fully or partially unusable, influence information, and put national security, generally, in danger.[5] Artificial intelligence (AI) and autonomous weapons are some of these technologies that allow for decision-making with limited human input, altering military tactics and strategy and creating significant ethical questions.[6] The potential to engage in war without the requirement of sending actual troops across borders to the battlefield, thus drastically lowering the potential of losses in manpower, makes tools of digital warfare very appealing to both state and non-state actors. For example, the -discovered on 2010- Stuxnet cyber-attack against Iranian nuclear program[7] showed to the world how an operation conducted with digital means can achieve objectives previously thought achievable only through kinetic military action.[8]

---

[1] Singer, P. W., & Friedman, A. (2014). *Cybersecurity and cyberwar: what everyone needs to know.* Oxford, Oxford University Press.
[2] Dinstein, Y. (2016). *The Conduct of Hostilities under the Law of International Armed Conflict* (3rd ed.). Cambridge: Cambridge University Press.
[3] Schmitt, M. N. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press.
[4] Lin, H.S. (2012). Cyber conflict and international humanitarian law. *International Review of the Red Cross, 94*, 515 - 531.
[5] Anderson, K., & Waxman, M. C. (2013). Law and Ethics for Autonomous Weapon Systems: Why a Ban Won't Work and How the Laws of War Can. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2250126
[6] Akhgar, B., Saathoff, G. B., Arabnia, H. R., Hill, R., Staniforth, A., & Bayerl, P. S. (2015). *Application of Big Data for National Security: A Practitioner's Guide to Emerging technologies*. https://derby.openrepository.com/handle/10545/620925
[7] Brown, G.D. (2011). Why Iran Didn't Admit Stuxnet Was an Attack. Joint Force Quarterly, 63, 70-73.
[8] Schmitt, M. N. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press.

These technological progressions provide substantial strategic advantages, but they carry great risks as well. The gradual eradication of the Distinction between combatants and civilians , the difficulties in the determination of responsibility for cyber-attacks[9], and the potential for extensive and excessive harm inflicted on civilian infrastructure and the lives of civilians undermine the foundations of international peace and security.[10] Furthermore, digital warfare may endanger many core human rights, including the right to privacy, the freedom of expression, and the access to information[11], and may repulse certain customary standards of international humanitarian law (IHL)[12]. Limited geographical constraints and the rapid nature of digital operations create issues in terms of responsibility and enforcement.

Where is the Future of Warfare — Conventional or Digital?

Warfare has been traditionally characterized by physical combat, land seizure, and conventional munitions. Nuclear weapons and chemical weapons in the 20th century were another big evolution, increasing the scale of destruction and redefining geopolitical power.[13] But now, states, terrorist and rebel groups, can wage a new form of warfare using digital means as the digitization of infrastructure has led to the hybridisation (and in some cases the full digitalization) of new conflicts where military occupation or direct combat is no longer a prerequisite.[14] On the contrary, adversaries may identify vulnerabilities in the digital systems of the other side and try to manipulate those vulnerabilities to disrupt economies and societies, exploit and manipulate the public, and target critical infrastructure.[15]

Moreover, unlike conventional warfare, digital operations may take place in peacetime and escalate rapidly — often without warning.[16] Cyber-attacks are usually not noticed by the general population at their start.[17] They general population usually becomes aware of them when their consequences are visible, such as the now-infamous NotPetya (2017), which created significant problems for businesses and institutions across the whole world.[18]

---

[9] Lin, H.S. (2012). Cyber conflict and international humanitarian law. *International Review of the Red Cross, 94*, 515 - 531.
[10] Schmitt, M. N. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press.
[11] International Committee of the Red Cross. (2015). International humanitarian law and the challenges of contemporary armed conflicts. In *32nd INTERNATIONAL CONFERENCE OF THE RED CROSS AND RED CRESCENT*. https://www.icrc.org/sites/default/files/document/file_list/32ic-report-on-ihl-and-challenges-of-armed-conflicts.pdf
[12] Taddeo, M., Floridi, L., Taddeo, M., & Floridi, L. (Eds.). (2017). The responsibilities of online service providers. In Institute of Law and Technology, UAB, Spain & University of Bologna (Faculty of Law-CIRSFID) and European University Institute of Florence, Italy, *Law, Governance and Technology Series* (Vol. 31). https://doi.org/10.1007/978-3-319-47852-4.
[13] Rid, T. (2011). Cyber War Will Not Take Place. *Journal of Strategic Studies*, *35*(1), 5–32. https://doi.org/10.1080/01402390.2011.608939
[14] Nye, J. S., Jr. (2011). *The future of power*. PublicAffairs.
[15] Nye, J. S., Jr. (2011). *The future of power*. PublicAffairs.
[16] Schmitt, M. N. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press.
[17] Lin, H.S. (2012). Cyber conflict and international humanitarian law. *International Review of the Red Cross, 94*, 515 - 531.
[18] Greenberg, A., & Excerpt. (2018, August 22). The untold story of NotPetya, the most devastating cyberattack in history. *WIRED*. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Furthermore, the weaponization of misinformation, disinformation, and propaganda campaigns poses a significant challenge to democratic systems, undermines public trust in democratic institutions[19], and destabilizes societies.[20] Digital warfare and cyberweapons will lead to state military power no longer being defined just by conventional (or even nuclear) weapons[21] but also by how adept they are in digital programs,[22] their artificial intelligence capabilities, and their ability to operate within cyberspace.[23]

Relevance of Human Rights and Humanitarian Law to Armed Conflicts

International humanitarian law (IHL) and human rights law are the result of the efforts undertaken by intellectuals of the last two centuries, like Henry Dunant with the goal to mitigate the consequences of military conflicts[24]. International Humanitarian Law (IHL), codified in the Geneva Conventions, creates guidelines that stem from customary international practice of the past[25], including the protections that are required to be given to civilians by an occupying force, the principle of proportionality, and the principle of distinction between combatants and non-combatants.[26] Human rights law protects some fundamental individual freedoms[27] — like the right of a person to privacy, their freedom to express themselves[28], and their right to have free access to information and news.[29] These principles are becoming more and more relevant today as digital technologies are being increasingly used in military and subversive operations.[30]

---

[19] Bannelier, K., & Christakis, T. (2017, February 25). *Cyber-Attacks – Prevention-Reactions: The role of states and private actors*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2941988

[20] Singer, P. W., & Friedman, A. (2014). *Cybersecurity and cyberwar: what everyone needs to know.* Oxford, Oxford University Press.

[21] Rid, T. (2011). Cyber War Will Not Take Place. *Journal of Strategic Studies*, *35*(1), 5–32. https://doi.org/10.1080/01402390.2011.608939

[22] Nye, J. S., Jr. (2011). *The future of power*. PublicAffairs

[23] Taddeo, M., Floridi, L., Taddeo, M., & Floridi, L. (Eds.). (2017). The responsibilities of online service providers. In Institute of Law and Technology, UAB, Spain & University of Bologna (Faculty of Law-CIRSFID) and European University Institute of Florence, Italy, *Law, Governance and Technology Series* (Vol. 31). https://doi.org/10.1007/978-3-319-47852-4

[24] International Committee of the Red Cross. (2015). International humanitarian law and the challenges of contemporary armed conflicts. In *32nd INTERNATIONAL CONFERENCE OF THE RED CROSS AND RED CRESCENT*. https://www.icrc.org/sites/default/files/document/file_list/32ic-report-on-ihl-and-challenges-of-armed-conflicts.pdf

[25] Dinstein, Y. (2016). *The Conduct of Hostilities under the Law of International Armed Conflict* (3rd ed.). Cambridge: Cambridge University Press.

[26] Rejali, S., & Heiniger, Y. (2020). The role of digital technologies in humanitarian law, policy and action: Charting a path forward. *International Review of the Red Cross*, *102*(913), 1–22. doi:10.1017/S1816383121000114

[27] Walzer, M. (2006). *Just and unjust wars: A Moral Argument With Historical Illustrations*. Basic Books.

[28] Taddeo, M., Floridi, L., Taddeo, M., & Floridi, L. (Eds.). (2017). The responsibilities of online service providers. In Institute of Law and Technology, UAB, Spain & University of Bologna (Faculty of Law-CIRSFID) and European University Institute of Florence, Italy, *Law, Governance and Technology Series* (Vol. 31). https://doi.org/10.1007/978-3-319-47852-4.

[29] Chesterman, S. (2011, February 14). *One nation under surveillance: A new social contract to defend freedom without sacrificing liberty (Introduction)*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1761055

[30] United Nations High Commissioner for Human Rights. (2014). Annual report of the United Nations High Commissioner for Human Rights and reports of the Office of the High Commissioner and the Secretary-General. In *Human Rights Council* (Vol. 27, Issue 37, pp. 1–6) [Report]. https://www.ohchr.org/sites/default/files/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf

Nevertheless, the distinctive characteristics of digital warfare may potentially create serious problems about the application of these legal regimes.[31] Cyber-attacks against critical infrastructure, like hospitals, water distribution systems, power grids or power generation facilities, may inflict significant damage on civilian populations[32], however such attacks may not qualify as an armed attack under the traditional interpretations of international law.[33] Autonomous weapons that decide without human intervention pose deep ethical questions regarding accountability and proportionality[34]. Although justified for national security, surveillance technologies may infringe on individual privacy and freedom[35], particularly when implemented in authoritarian regimes.[36]

It's this gradual incorporation of digital tools in weapon systems and their potential use in warfare that places them firmly inside a potential legal grey area.[37] It poses questions about the way states and non-state actors should be held responsible for cyber confrontations, the rights of individuals that are targeted by digital attacks,[38] and the moral responsibility of decision makers when it comes to autonomous weapon systems.[39] The following thesis tries to address these challenges by analysing how adequate the current legal frameworks are and proposing new strategies to protect human rights and uphold humanitarian principles in the information age.

Problem Statement

The ever-increasing incorporation of digital tools in warfare is presenting legal, ethical, and humanitarian challenges for which existing frameworks are poorly suited. Cyber-attacks, autonomous weapons, and surveillance systems challenge traditional principles of international law by eroding the distinction between combatants and civilians, enabling violations of state sovereignty, and complicating attribution and accountability. This research seeks to explore whether existing (and evolving) legal frameworks and ethical principles can effectively manage the conduct of war in the digital age without sacrificing human rights or igniting greater suffering among civilian populations.

---

[31] Schmitt, M. N. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press

[32] Bannelier, K., & Christakis, T. (2017, February 25). *Cyber-Attacks – Prevention-Reactions: The role of states and private actors*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2941988

[33] Jensen, E. T. (2014, July 16). *Cyber Sovereignty: The way ahead*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2466904

[34] Corn, G. S. (2014). Autonomous weapon systems: legal consequences of taking the man out of the LOOPP. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2450640

[35] Ohlin, J.D. (2016). The Combatant's Stance: Autonomous Weapons on the Battlefield. *International law studies, 92*, 1.

[36] Anderson, K., & Waxman, M. C. (2013). Law and Ethics for Autonomous Weapon Systems: Why a Ban Won't Work and How the Laws of War Can. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2250126

[37] Oxford University Press. (n.d.). *Cyber operations and the use of force in international law : WestminsterResearch*. https://westminsterresearch.westminster.ac.uk/item/8yv62/cyber-operations-and-the-use-of-force-in-international-law

[38] Schmitt, M. N. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press

[39] Brenner, S. W. (2011). Cyber-Threats and the limits of bureaucratic control. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.1950725

Research Objectives

This research has several aims. Firstly, it seeks to determine how digital warfare affects the rights to privacy, freedom of expression, and civilian safety. Secondly, it seeks to study what challenges digital warfare represents for principles of humanitarian law, like distinction, proportionality, and liability. Thirdly, it tries to assess how sufficient are the existing international legal doctrinal responses to these challenges. Lastly, it aims to propose recommendations to strengthen the legal, ethical, and institutional mechanisms to regulate digital conflict.

Research Questions

This dissertation strives to answer a series of significantly important questions. Firstly, what are the most vital repercussions of digital warfare on human rights, specifically privacy, freedom of expression, and civilian safety? Secondly, what aspects of digital warfare challenge the applicability and enforcement of humanitarian law? Thirdly, it seeks to discover if the existing international legal frameworks are adequate to govern digital warfare and hold the actors accountable. Lastly, how can the legal and ethical frameworks governing digital conflicts be reinforced?

Methodology

The conducted research is of qualitative nature, combining legal analysis and case studies with interdisciplinary approaches. The study will explore international legal frameworks (e.g., the Geneva Conventions and the Tallinn Manual on Cyber Warfare) and academic literature (academic articles, reports, etc.) as well as case studies from the real world (e.g., Stuxnet, NotPetya, Russian cyber operations). However, a singular interdisciplinary approach is to ensure that diverse subject areas are interlinked, with Law, Technology, and Ethics being the core foundational pillars.

Thesis Structure

The thesis is structured as follows:

On Chapter II there will be an analysis of the Definitions, characteristics, technological innovations, and the key actors in the Warfare in the Digital Era. It will be followed by Chapter II where there will be an analysis of the Impact on Human Rights: Looks at privacy issues, misinformation, and harm to civilians. On Chapter IV the Challenges to Humanitarian Law: Discusses the legal application of IHL, ethical dilemmas, and accountability will be presented, While on Chapter V some Case Studies of cyber-attacks and the involvement of non-state actors will be presented. On Chapter VI there will be An Overview of the Law in Practice in order to Examine the strengths and shortcomings of applicable norms in IHL and human rights law. Chapter VII will offer Recommendations in legal, ethical, and policy aspects for the regulation of digital war. Chapter VIII will be the Conclusion that is going to Summarize the findings, and reflect on broader implications, and calls for action.

II. Warfare in the Digital Era

Key Features and Definition

In recent decades, as the world entered into what is called the digital (or information) era, warfare itself seems to have changed by the growing digitalisation of infrastructure.[40] This digitalisation of warfare has led to several new forms of operations[41] that in their totality should be called digital warfare.[42] Digital warfare involves the use of advanced digital technologies like cyber-weapons, autonomous or AI-guided weapons, misinformation campaigns[43], and advanced surveillance systems[44] to achieve military, political, or economic objectives[45]. Unlike traditional warfare, which depends on physical aggression through kinetic weapons, like rifles, machine guns or ICBMs[46], digital combat takes place in and through cyberspace[47] and involves advanced technical systems[48]. In this regard, a digital warrior can also exploit the increasingly interconnected nature of modern societies and technologies like social media and the internet[49], to achieve strategic goals and undermine (or potentially destroy) the critical infrastructure[50], the public trust or the social cohesion of its potential adversaries[51].

Features of Digital Warfare

Digital warfare has several features that need to be analysed before moving on to the rest of

---

[40] Schmitt, M. N. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press.
[41] Singer, P. W., & Friedman, A. (2014). *Cybersecurity and cyberwar: what everyone needs to know.* Oxford, Oxford University Press.
[42] Lin, H.S. (2012). Cyber conflict and international humanitarian law. *International Review of the Red Cross, 94*, 515 - 531.
[43] Jensen, E. T. (2014, July 16). *Cyber Sovereignty: The way ahead*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2466904
[44] Akhgar, B., Saathoff, G. B., Arabnia, H. R., Hill, R., Staniforth, A., & Bayerl, P. S. (2015). *Application of Big Data for National Security: A Practitioner's Guide to Emerging technologies*. https://derby.openrepository.com/handle/10545/620925
[45] Taddeo, M., Floridi, L., Taddeo, M., & Floridi, L. (Eds.). (2017). The responsibilities of online service providers. In Institute of Law and Technology, UAB, Spain & University of Bologna (Faculty of Law-CIRSFID) and European University Institute of Florence, Italy, *Law, Governance and Technology Series* (Vol. 31). https://doi.org/10.1007/978-3-319-47852-4.
[46] Rid, T. (2011). Cyber War Will Not Take Place. *Journal of Strategic Studies*, *35*(1), 5–32. https://doi.org/10.1080/01402390.2011.608939
[47] **Nye, J. S. (2011).** *The Future of Power.* PublicAffairs
[48] International Committee of the Red Cross. (2015). International humanitarian law and the challenges of contemporary armed conflicts. In *32nd INTERNATIONAL CONFERENCE OF THE RED CROSS AND RED CRESCENT*. https://www.icrc.org/sites/default/files/document/file_list/32ic-report-on-ihl-and-challenges-of-armed-conflicts.pdf
[49] Greenberg, A., & Excerpt. (2018, August 22). The untold story of NotPetya, the most devastating cyberattack in history. *WIRED*. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/
[50] Bannelier, K., & Christakis, T. (2017, February 25). *Cyber-Attacks – Prevention-Reactions: The role of states and private actors*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2941988
[51] Shackelford, S., Fort, T. L., & Prenkert, J. D. (2014). How businesses can promote Cyber Peace. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2393528

the analysis of this paper. One of the most important features that need to be analysed is their global reach and operational accessibility.[52] Digital operations are not bound by the traditional limitations of a physical operational space.[53] This grants to a potential adversaries the ability to interfere with, disrupt or even fully disable systems from anywhere in the world as a digital operation usually does not require physical proximity to be conducted.[54] As a result, the scope and complexity of military operations is expanded, allowing even small actors (potentially even a single person with the necessary knowledge) to carry out impactful operations.

Another vitally important aspect of digital warfare is their speed and scale.[55] Digital and Cyber-attacks can be carried out in mere seconds and can impact millions (in some extreme and not yet realised cases this number could rise to affect even billions) of people or several vital systems and infrastructure all at once.[56] The speed and magnitude at which these operations grow leave limited time (if any at all) for defensive strategies to be put in place, creating the absolute necessity for proactive cybersecurity[57].

Thirdly, when discussing digital warfare and cyber operations a key feature that should be discussed is their ambiguity[58]. The secretive and covert characteristics of digital operations along with the plausible deniability of international actors that they provide to the international actors engaging in them lead to legal ambiguity in whether an act is an act of war or a criminal act.[59] This opacity leads to problems for both attribution and the legal recourse, allowing perpetrators a degree of freedom to operate with relative impunity.[60]

Continuing on with the analysis of the characteristics of digital warfare, it is imperative to analyse the role of dual-use technologies.[61] A large number of digital tools utilised in military or subversive operations happen to also serve civilian purposes.[62] For example, critical communication or power infrastructures, such as internet servers or an electrical power plant,

---

[52] Lin, H.S. (2012). Cyber conflict and international humanitarian law. *International Review of the Red Cross, 94*, 515 - 531.

[53] Jensen, E. T. (2014, July 16). *Cyber Sovereignty: The way ahead*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2466904

[54] Schmitt, M. N. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press.

[55] Singer, P. W., & Friedman, A. (2014). *Cybersecurity and cyberwar: what everyone needs to know.* Oxford, Oxford University Press.

[56] Bannelier, K., & Christakis, T. (2017, February 25). *Cyber-Attacks – Prevention-Reactions: The role of states and private actors*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2941988

[57] Greenberg, A., & Excerpt. (2018, August 22). The untold story of NotPetya, the most devastating cyberattack in history. *WIRED*. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

[58] Brenner, S. W. (2011). Cyber-Threats and the limits of bureaucratic control. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.1950725

[59] Schmitt, M. N. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press.

[60] Roscini, M., & Trust, L. (2014). *Cyber operations and the use of force in international law*. Oxford University Press, USA.

[61] International Committee of the Red Cross. (2015). International humanitarian law and the challenges of contemporary armed conflicts. In *32nd INTERNATIONAL CONFERENCE OF THE RED CROSS AND RED CRESCENT*. https://www.icrc.org/sites/default/files/document/file_list/32ic-report-on-ihl-and-challenges-of-armed-conflicts.pdf

[62] Anderson, K., & Waxman, M. C. (2013). Law and Ethics for Autonomous Weapon Systems: Why a Ban Won't Work and How the Laws of War Can. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2250126

can become both targets and tools in digital military operations.[63] This dual-use nature complicates the distinction between military and civilian targets, amplifying the potential of collateral damage and raising significant ethical questions about the justification of targeting such infrastructure.

The last key characteristic of digital warfare that should be analysed is its low barrier to entry.[64] Digital warfare usually involves far fewer resources than engaging in traditional military operations, thus, allowing smaller and potentially more diplomatically isolated states and non-state actors to wage war in a more effective and less costly manner than before the advent of the digital era.[65] This democratization of the military capabilities used in conflict creates wider and more unpredictable risks to global peace and security.[66]

Technological Innovations in Warfare

It is no secret that the digital age has led to a series of technological innovations and advancements that have altered the dynamics of war.

Cybersecurity and Cyber-Attacks

When talking about digital warfare, the first thing that comes to someone's mind is Cyberspace, Cybersecurity, Cyber-weapons and cyber-attacks.[67] Cyber-attacks, such as ransomware, distributed denial-of-service (DDoS) attacks, data leaks, and even some computer viruses (commonly referred to as malicious computer worms) are becoming, in recent years, essential weapons both for state and non-state actors.[68] These operations have the potential to cripple critical services and infrastructure, siphon sensitive, confidential and/or classified information, and paralyze communications, transport and power supply and as a result paralyze national security.[69] High-profile examples like the NotPetya and SolarWinds attacks illustrate the disruptive threat of cyber operations and their potential to topple whole institutions and do crippling damage to entire economies.[70] Furthermore, cyber-attacks directed towards critical infrastructure, like power grids, power generation facilities, or critical transportation systems, potentially leading to damage or even destruction of

---

[63] Bannelier, K., & Christakis, T. (2017, February 25). *Cyber-Attacks – Prevention-Reactions: The role of states and private actors*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2941988

[64] Rid, T. (2011). Cyber War Will Not Take Place. *Journal of Strategic Studies*, *35*(1), 5–32. https://doi.org/10.1080/01402390.2011.608939

[65] Shackelford, S., Fort, T. L., & Prenkert, J. D. (2014). How businesses can promote Cyber Peace. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2393528

[66] Ohlin, J.D. (2016). The Combatant's Stance: Autonomous Weapons on the Battlefield. *International law studies, 92*, 1.

[67] Schmitt, M. N. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press.

[68] Jensen, E. T. (2014, July 16). *Cyber Sovereignty: The way ahead*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2466904

[69] Shackelford, S., Fort, T. L., & Prenkert, J. D. (2014). How businesses can promote Cyber Peace. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2393528

[70] Brenner, S. W. (2011). Cyber-Threats and the limits of bureaucratic control. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.1950725

hospital facilities, provide evidence of their ability and potential to hurt the civilian population and create lasting inconvenience or damage.[71]

AI and Autonomous Weapons

Another, fairly recent, advancement in digital warfare is the introduction of Autonomous and AI-guided weapons systems.[72] Autonomous weapons systems (AWS) are weapons systems that, with the help of artificial intelligence (AI) in most cases, are capable of making decisions with minimal or even without human input.[73] These systems include but are not limited to drones and automated robotic platforms with the capability to autonomously identify and engage their targets.[74] Undoubtedly, these technologies have the potential to improve precision and minimize human casualties, however they still generate profound ethical and legal questions in regards to accountability, adherence to International Humanitarian Law (IHL)[75], and the handing over of life-and-death judgment to machines.[76] AI squadrons, or systems that work together under the guidance of a human commander, offer greater potential to both pursue strategy and appease potential ethical concerns in warfare, but swarm technologies take this development a step farther, potentially aggravating such ethical and legal concerns.[77]

Technologies of Big Data and Surveillance

Another technological development that is getting incorporated in the execution of digital military and subversive operations. It is through the analysis of massive datasets (big data) that military and intelligence agencies can gain meaningful insights into the behaviour, trends, and vulnerabilities of adversaries, both in regards to their society and in regards to the individuals that their government is comprised of.[78] When combined with surveillance technologies, these systems allow monitoring of individuals and groups on an unprecedented scale.[79] But their uses raise concerns about privacy, potential misuse of these technologies,

---

[71] Roscini, M., & Trust, L. (2014). *Cyber operations and the use of force in international law*. Oxford University Press, USA.
[72] Corn, G. S. (2014). Autonomous weapon systems: legal consequences of taking the man out of the LOOPP. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2450640
[73] Anderson, K., & Waxman, M. C. (2013). Law and Ethics for Autonomous Weapon Systems: Why a Ban Won't Work and How the Laws of War Can. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2250126
[74] Ohlin, J.D. (2016). The Combatant's Stance: Autonomous Weapons on the Battlefield. *International law studies, 92*, 1.
[75] International Committee of the Red Cross (ICRC). Autonomous Weapon Systems: Technical, Military, Legal, and Humanitarian Aspects. ICRC, 2016.

[76] Schmitt, M. N. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press.
[77] Winter, E. (2020). THE COMPATIBILITY OF AUTONOMOUS WEAPONS WITH THE PRINCIPLE OF DISTINCTION IN THE LAW OF ARMED CONFLICT. *International and Comparative Law Quarterly*, *69*(4), 845–876. doi:10.1017/S0020589320000378
[78] Akhgar, B., Saathoff, G. B., Arabnia, H. R., Hill, R., Staniforth, A., & Bayerl, P. S. (2015). *Application of Big Data for National Security: A Practitioner's Guide to Emerging technologies*. https://derby.openrepository.com/handle/10545/620925
[79] Macnish, K. (2017). The Ethics of Surveillance: An Introduction (1st ed.). Routledge. https://doi.org/10.4324/9781315162867

and the risk of the dissolution of democratic institutions by virtue of governmental authoritarian overreach.[80] Advanced data analytics can also make predictions about behaviour and while this can be advantageous for predicting adversaries' decisions and for proactive responses to negative behaviour, when applied for internal security reasons[81], there is a heightened risk of profiling and discrimination.[82]

Quantum Computing

Another, recent and not yet publicly proliferated technology that may be utilized in the enhancement of digital warfare capabilities is Quantum computing.[83] It provides far greater computational power than even the most advanced regular computers leading to interesting developments.[84] Quantum computing is a revolutionary technology that threatens to upend the world of national security operations, rendering even the most secure and classified communications and documents insecure.[85] Countries that achieve to obtain this technology and manage to build up their quantum computing capabilities will have a robust competitive edge when it comes to defensive (in regards to the safeguarding of their communications and therefore state secrets)[86] or offensive (in regards to the disruption of adversaries' infrastructure) cyber operations, significantly widening the gap for tech supremacy even further.[87] The implications of this would extend far beyond cryptography, with quantum technologies capable of simulating and identifying potential logistical and strategic oversights in cyber (and potentially traditional) operations on the one hand, while on the other hand revolutionizing intelligence in military settings—radically redefining strategic environments.[88]

Deepfakes and Manipulation of Information

A far more accessible application of such Technological advancements is the creation of Deepfakes by artificial intelligence programs.[89] While the photo of Pope Francis in a large white puffer jacket may be easy to identify as a Deepfake, this technology may have grave repercussions when more plausible and believable deepfake photographs, videos or even

---

[80] UN. Office of the High Commissioner for Human Rights. (2014, June 30). *The right to privacy in the digital age :: report of the Office of the United Nations High Commissioner for Human Rights*. United Nations Digital Library System. https://digitallibrary.un.org/record/777869?v=pdf

[81] Henschke, A. (2017). *Ethics in an Age of Surveillance: Personal Information and Virtual Identities*. Cambridge: Cambridge University Press.

[82] Zwitter, A. (2014). Big Data ethics. Big Data & Society, 1(2). https://doi.org/10.1177/2053951714559253

[83] International Telecommunication Union & Development Sector. (2020). *Global Cybersecurity Index 2020*. International Telecommunication Union.

[84] Bannelier, K., & Christakis, T. (2017, February 25). *Cyber-Attacks – Prevention-Reactions: The role of states and private actors*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2941988

[85] Kernighan, B. W. (2021). *Understanding the digital world: What You Need to Know about Computers, the Internet, Privacy, and Security, Second Edition*. Princeton University Press.

[86] European Union Agency for Cybersecurity (ENISA). Threat Landscape Report 2020. ENISA, 2020.

[87] **Nye, J. S. (2011).** *The Future of Power.* PublicAffairs

[88] Shackelford, S., Fort, T. L., & Prenkert, J. D. (2014). How businesses can promote Cyber Peace. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2393528

[89] Singer, P. W., & Friedman, A. (2014). *Cybersecurity and cyberwar: what everyone needs to know.* Oxford, Oxford University Press.

audio recordings start appearing.[90] It is important to note that the manipulation of information and psychological warfare have been some of the oldest and most important forms of tactical and strategic deception.[91] And by incorporating this technology in the war machine, psychological warfare has never been so easy and flexible with local videos or deepfakes.[92] Another application of these technologies by the intelligence services of some country can also be the production of realistic audio-visual fabrications that can be employed to sway opinion, spread false narratives, and further erode public trust in social and democratic institutions.[93] In wartime, deepfakes can sow distrust among allies, place significant obstacles for decision-making processes, or even sway civilian populations one way or another.[94] These tools are proliferating in ways that require strong countermeasures and public education on how to detect and counter their effects.[95]

Actors in Digital Warfare

Potential digital wars may feature a wide variety of actors with different and potentially contradictory goals and vastly differing capabilities.

State Actors

Despite the technological changes of the current era, State actors remain the most vital actors in the study of warfare and international law.[96] It is sovereignty and nationalism that weaves through the digital (as it did through the physical) domain, as nation-states emerge as the main actors committing acts of war, using technology to achieve obtaining military advantages through espionage and sabotage.[97] For that reason, state-sponsored cyber operations have increasingly been observed over the recent years, despite sometimes denying involvement in these.[98] State-sponsored cyber operations are most frequently directed against critical civilian or military infrastructure, political institutions, and economic systems. Interesting examples of such state sponsored cyber operations would be the Russian interference in the 2016 U.S. presidential elections and the Chinese cyber-espionage

---

[90] Amnesty International. (2019). SURVEILLANCE GIANTS: HOW THE BUSINESS MODEL OF GOOGLE AND FACEBOOK THREATENS HUMAN RIGHTS. In *Amnesty International*.

[91] International Committee of the Red Cross. (2015). International humanitarian law and the challenges of contemporary armed conflicts. In *32nd INTERNATIONAL CONFERENCE OF THE RED CROSS AND RED CRESCENT*. https://www.icrc.org/sites/default/files/document/file_list/32ic-report-on-ihl-and-challenges-of-armed-conflicts.pdf

[92] Bannelier, K., & Christakis, T. (2017, February 25). *Cyber-Attacks – Prevention-Reactions: The role of states and private actors*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2941988

[93] Rid, T. (2011). Cyber War Will Not Take Place. *Journal of Strategic Studies*, *35*(1), 5–32. https://doi.org/10.1080/01402390.2011.608939

[94] Henschke, A. (2017). *Ethics in an Age of Surveillance: Personal Information and Virtual Identities*. Cambridge: Cambridge University Press.

[95] Kernighan, B. W. (2021). *Understanding the digital world: What You Need to Know about Computers, the Internet, Privacy, and Security, Second Edition*. Princeton University Press.

[96] Roscini, M., & Trust, L. (2014). *Cyber operations and the use of force in international law*. Oxford University Press, USA.

[97] Jensen, E. T. (2014, July 16). *Cyber Sovereignty: The way ahead*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2466904

[98] Bannelier, K., & Christakis, T. (2017, February 25). *Cyber-Attacks – Prevention-Reactions: The role of states and private actors*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2941988

campaigns against the intellectual property of several western (primarily American) businesses.[99] These operations show how states use digital tools to achieve their geopolitical ends while avoiding entering a costly and expensive conventional war.[100]

Non-State Actors

Digital conflicts also involve the increasing involvement of non-state entities, such as terrorist organizations, hacktivist groups, and private corporations.[101] Digital platforms are utilized by terrorist groups for recruitment, propaganda, and coordination; hacktivists commit politically motivated cyber-attacks.[102] For their part, corporations are sometimes complicit in digital wars by creating or selling technologies that enable warring parties to conduct warfare.[103] Additionally, private organizations are not necessarily bound by the same ethical and regulatory constraints as state actors, leading to potential abuses of power in the development and deployment of offensive cyber capabilities.[104]

Proxy Actors

One of the most common types of conflicts during the Cold war and the post-Cold war era are the so-called Proxy wars. These are conflicts where a State employs another, weaker state or non-state actor to engage in a war against their actual adversary. In the digital era this would mean that States have recourse to proxy actors to execute cyber operations, allowing them to operate under plausible deniability.[105] In this case, proxies could be private corporations and contractors, criminal or terrorist groups, loose collections of people with common goals, or even another more obscure or isolated state.[106] Such a strategy fuses attribution and accountability, enabling states to efficiently engage in hostile operations while evading direct consequences for such actions.[107] In many cases, proxy actors obscure the distinction between state-sponsored campaigns and operations and independent actions by individuals or non-state actors, thus creating further complications for potential responses from the international community.[108]

---

[99] Schmitt, M. N. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press.
[100] **Nye, J. S. (2011).** *The Future of Power.* PublicAffairs
[101] Roscini, M., & Trust, L. (2014). *Cyber operations and the use of force in international law*. Oxford University Press, USA.

[102] Bannelier, K., & Christakis, T. (2017, February 25). *Cyber-Attacks – Prevention-Reactions: The role of states and private actors*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2941988
[103] hackelford, S., Fort, T. L., & Prenkert, J. D. (2014). How businesses can promote Cyber Peace. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2393528
[104] European Union Agency for Cybersecurity (ENISA). Threat Landscape Report 2020. ENISA, 2020.

[105] Jensen, E. T. (2014, July 16). *Cyber Sovereignty: The way ahead*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2466904
[106] Amnesty International. (2019). SURVEILLANCE GIANTS: HOW THE BUSINESS MODEL OF GOOGLE AND FACEBOOK THREATENS HUMAN RIGHTS. In *Amnesty International*.
[107] Bannelier, K., & Christakis, T. (2017, February 25). *Cyber-Attacks – Prevention-Reactions: The role of states and private actors*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2941988
[108] Schmitt, M. N. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press.

Multinational Organizations

The role of multinational organizations has always been important for the codification and creation of international customary norms, in a series of important matters for the international community.[109] As for the challenges posed by digital warfare, the role of these international institutions like NATO and the UN is of vital importance here as well.[110] The objective of these organizations is to establish international norms through the achievement of international consensus, to build international cooperation and understanding, and help mediate, prevent and resolve conflicts that arise from cyber operations.[111] Their function is pivotal in promoting international collaboration building on the mutual understanding between states and peoples, formulating cohesive structures for managing, preventing and resolving digital conflicts, before they escalate and reacting to breaches of cyber practices.[112]

Private Technology Companies

Private technology companies are a lot of the time one of the principal target of cyber operations, as their databases contain data for numerous people around the world, thus constituting an actor in the realm of digital warfare operations.[113] Tech companies like Microsoft and Google frequently identify and respond to cyber threats, in order to protect both themselves and their clients/users working in close cooperation and coordination with governments to safeguard critical communication infrastructure, with the goal to create tools to combat and potentially prevent misinformation and cyber-attacks.[114] However, their participation in this discourse also raises questions in regards to accountability, transparency, and the balance between the motives of profit and the general public good.[115]

Conclusion

This transition to hybrid and digital warfare has continued to evolve, incorporating as of late cyber-attacks, cyber espionage, and the myriad ways in which information can be weaponized and manipulated in the Information Age—leading to the creation of new, unprecedented and complicated challenges for states and societies alike. As technology is revolutionizing the battlefield once more, the challenges that digital warfare poses to the international community will need to be considered and addressed by states, organizations, and policymakers. By educating the population to its features, imposing some limited economic regulations to technical innovations, and promoting international collaboration and

---

[109] Amnesty International. (2019). SURVEILLANCE GIANTS: HOW THE BUSINESS MODEL OF GOOGLE AND FACEBOOK THREATENS HUMAN RIGHTS. In *Amnesty International*.
[110] European Union Agency for Cybersecurity (ENISA). Threat Landscape Report 2020. ENISA, 2020.
[111] Bannelier, K., & Christakis, T. (2017, February 25). *Cyber-Attacks – Prevention-Reactions: The role of states and private actors*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2941988
[112] THE INTERNATIONAL INSTITUTE FOR STRATEGIC STUDIES. (n.d.). *CYBER CAPABILITIES AND NATIONAL POWER: A net assessment*.
[113] Amnesty International. (2019). SURVEILLANCE GIANTS: HOW THE BUSINESS MODEL OF GOOGLE AND FACEBOOK THREATENS HUMAN RIGHTS. In *Amnesty International*.
[114] Shackelford, S., Fort, T. L., & Prenkert, J. D. (2014). How businesses can promote Cyber Peace. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2393528
[115] UN. Office of the High Commissioner for Human Rights. (2014, June 30). *The right to privacy in the digital age :: report of the Office of the United Nations High Commissioner for Human Rights*. United Nations Digital Library System. https://digitallibrary.un.org/record/777869?v=pdf

cooperation, the world can combat these new threats posed by the digital technologies' immeasurable future and the potential future applications. It will come down to governments establishing clear and robust regulatory measures and adherence and raising investments in systems that will protect their citizens from such cyber and informational warfare in an age where cyber security and access to correct information are of vital importance to a state's national security.[116]

[116] Schmitt, M. N. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press.

III. Impact on Human Rights

Privacy and Surveillance

In today's information era that is characterized by digital warfare and its rapid proliferation in more and more states in the world, the new technologies of surveillance have breached the realm, scale, and authority of individual privacy.[117] Governments and other actors now use more and more often digital tools to monitor civilian communications, track people's movements, and harvest personal data[118] on a colossal and unprecedented scale.[119] These activities are most of the time justified in the name of national security, yet, more often than not, they violate even the most basic human rights and civil liberties.[120]

Mass surveillance programs, for example, as it was exposed by whistle-blowers like Edward Snowden, have revealed the ways digital technologies have been used to vastly enhance the capacity of state actors to monitor individuals anywhere in the world.[121] In such cases, when surveillance is performed on a massive scale an in the absence of meaningful oversight, accountability, and well-defined legal frameworks, it has the potential to erode the trust between individuals in these societies and to significantly weaken the social contract between governments and the citizens of their states.[122] In conflict zones, surveillance technologies are reappropriated as guidance and targeting systems for weapons in order to target well defined populations, leading to the undermining of individuals' sense of personal safety and autonomy—and decimating vulnerable (most of the time civilian) populations.[123]

This is further exacerbated by the introduction of biometric and facial recognition technologies.[124] These tools, that are most commonly used in border control, urban policing, or public security, have also the potential to be abused by their users in order to profile people with regard to their ethnicity, faith, or political beliefs, further reinforcing and exacerbating existing social inequalities.[125] Certain regimes have utilized facial recognition technologies to isolate individuals branded by an authoritarian government as dangerous, monitor members of the political opposition, and firmly maintain the authoritarian control of the state.[126] In

---

[117] Amnesty International. (2019). SURVEILLANCE GIANTS: HOW THE BUSINESS MODEL OF GOOGLE AND FACEBOOK THREATENS HUMAN RIGHTS. In *Amnesty International*.
[118] Human Rights Watch. World Report 2023: Events of 2022. Human Rights Watch, 2023.
[119] Chesterman, S. (2011, February 14). *One nation under surveillance: A new social contract to defend freedom without sacrificing liberty (Introduction)*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1761055
[120] Henschke, A. (2017). *Ethics in an Age of Surveillance: Personal Information and Virtual Identities*. Cambridge: Cambridge University Press.
[121] European Union Agency for Cybersecurity (ENISA). Threat Landscape Report 2020. ENISA, 2020
[122] UN. Office of the High Commissioner for Human Rights. (2014, June 30). *The right to privacy in the digital age :: report of the Office of the United Nations High Commissioner for Human Rights*. United Nations Digital Library System. https://digitallibrary.un.org/record/777869?v=pdf
[123] International Committee of the Red Cross. (2015). International humanitarian law and the challenges of contemporary armed conflicts. In *32nd INTERNATIONAL CONFERENCE OF THE RED CROSS AND RED CRESCENT*. https://www.icrc.org/sites/default/files/document/file_list/32ic-report-on-ihl-and-challenges-of-armed-conflicts.pdf
[124] THE INTERNATIONAL INSTITUTE FOR STRATEGIC STUDIES. (n.d.). *CYBER CAPABILITIES AND NATIONAL POWER: A net assessment*.
[125] Henschke, A. (2017). *Ethics in an Age of Surveillance: Personal Information and Virtual Identities*. Cambridge: Cambridge University Press.
[126] European Union Agency for Cybersecurity (ENISA). Threat Landscape Report 2020. ENISA, 2020

addition, the use of artificial intelligence (AI) in surveillance systems introduces risks such as potential inaccuracies, the continuation and exacerbation of systemic discrimination and inequalities, and mass abuse of fundamental human rights in authoritarian regimes and systems. Automated surveillance lacks the necessary transparency and is often very difficult (if not impossible) to challenge if you think that such a system has been misused, misinterpreted or has shown simply the wrong output.[127]

Freedom of Information, Misinformation

One of the most common new forms of warfare is what is called informational warfare. It is the effort to control and spin certain narratives to suit those of the originator. As such, warfare in the digital domain has changed the information landscape, creating new ways to engage in information war by launching disinformation and misinformation campaigns,[128] with severe consequences for the freedom of expression and the access to accurate information.[129] The use of misinformation, disinformation and propaganda campaigns as a weapon is now a cornerstone of contemporary conflicts, eroding trust, both between states and between governments and their people, distorting public perceptions, and destabilizing societies.[130] Disinformation and misinformation campaigns are sometimes accompanied by the spreading of false narratives, causing distortions in public opinion and fomenting divisions in communities, and the battle with disinformation has become an urgent global challenge.[131] Many threats have occurred already—for example, the misinformation campaigns during the 2016 U.S. presidential elections and similar operations in Europe—to give us knowledge about the way digital tools have the potential to disrupt otherwise firmly entrenched democratic processes.[132] The mass use of bots, troll farms, and algorithms to amplify divisive content undermines public discourse, a core pillar of democratic principles, weakening the trust in democratic institutions, and exacerbating polarization within societies.[133] The victims of such campaigns are often left confused about the situation of their country, alienated with the democratic political systems, and lacking faith in traditional information sources, which is the perfect breeding ground for the rise of extremist ideologies and conspiracy theories.[134]

---

[127] Chesterman, S. (2011, February 14). *One nation under surveillance: A new social contract to defend freedom without sacrificing liberty (Introduction)*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1761055

[128] NATO Strategic Communications Centre of Excellence. Robotrolling 2021/2: Online Influence Operations in an Era of Automation. NATO StratCom COE, 2021.

[129] Schmitt, M. N. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press.

[130] Amnesty International. (2019). SURVEILLANCE GIANTS: HOW THE BUSINESS MODEL OF GOOGLE AND FACEBOOK THREATENS HUMAN RIGHTS. In *Amnesty International*.

[131] European Union Agency for Cybersecurity (ENISA). Threat Landscape Report 2020. ENISA, 2020

[132] Henschke, A. (2020). Privacy, the Internet of Things and State Surveillance: Handling Personal Information within an Inhuman System. *Moral Philosophy and Politics*, *7*(1), 123-149. https://doi.org/10.1515/mopp-2019-0056

[133] UN. Office of the High Commissioner for Human Rights. (2014, June 30). *The right to privacy in the digital age :: report of the Office of the United Nations High Commissioner for Human Rights*. United Nations Digital Library System. https://digitallibrary.un.org/record/777869?v=pdf

[134] Kernighan, B. W. (2021). *Understanding the digital world: What You Need to Know about Computers, the Internet, Privacy, and Security, Second Edition*. Princeton University Press.

Deepfakes: Taking Misinformation to Another Level

Deepfakes, either fully generated by AI or artificially augmented with AI, can become an extremely important tool for a disinformation campaign[135]. That is because deepfakes have the potential to mislead audiences during an electoral campaign and therefore disturb important deliberative processes by producing extremely believable, yet fake, audio-visual material.[136] There have been cases where a real negative comment by a political figure surfaces and it leads to a political crisis.[137] Should Man-made videos of political figures making inflammatory statements, for instance, see the surface, if it seems like they are real, they may spark violent social outrage, damage international relations, and even undermine the integrity of electoral processes.[138] Tackling these issues will need to involve extensive collaboration among governments, tech firms, and civil society in order to promote media literacy, create investigatory bodies that monitor news on content hosting platforms, and create technologies that can detect and combat misinformation in real-time, even when deepfakes are used.[139]

Civilian Damage in a Digital War

One of the most concerning (if not the most concerning of all) aspects of digital warfare is its potential for disproportionate harm towards civilian populations.[140] Cyber-attacks aimed towards critical public infrastructure—like power grids and power generator facilities, water supply and distribution systems, transportation and road networks, and healthcare and medical facilities —have the potential to inflict excessive damage, shutting down essential for emergencies that may arise in everyday life services and gravely jeopardizing human lives.[141] The WannaCry ransomware attack in 2017 is an important example of this practice, because it caused widespread disruption in healthcare systems all around the world, with the result of delays in medical procedures, the endangerment of the patients, their lives and

---

[135] Schmitt, M. N. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press.

[136] Deeks, A. (2014b, September 1). *An international legal framework for surveillance*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2490700

[137] Henschke, A. (2020). Privacy, the Internet of Things and State Surveillance: Handling Personal Information within an Inhuman System. *Moral Philosophy and Politics*, *7*(1), 123-149. https://doi.org/10.1515/mopp-2019-0056

[138] Geiss, R., & Lahmann, H. (2021b, May 22). *Protection of data in armed conflict*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3851136

[139] Hathaway, Oona & Crootof, Rebecca & Levitz, Philip & Nix, Haley & Nowlan, Aileen & Perdue, William & Spiegel, Julia. (2011). The Law of Cyber-Attack. California Law Review. 100.

[140] Roscini, M., & Trust, L. (2014). *Cyber operations and the use of force in international law*. Oxford University Press, USA.

[141] International Committee of the Red Cross. (2015). International humanitarian law and the challenges of contemporary armed conflicts. In *32nd INTERNATIONAL CONFERENCE OF THE RED CROSS AND RED CRESCENT*. https://www.icrc.org/sites/default/files/document/file_list/32ic-report-on-ihl-and-challenges-of-armed-conflicts.pdf

safety, and the showing how fragile the modern, highly interconnected digitalised systems can become.[142]

Such attacks tend to, more often than not, breach the principles of proportionality as stipulated under Articles 51(5)(b) and 57(2)(b) of the Protocol I of the Geneva Conventions of 1949 which define an indiscriminate attack as "one causing excessive civilian loss of life injury or damage in relation to the concrete and direct military advantage that may be obtained"[143] and distinction as stipulated under Articles 48 which provides that "shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives"[144], 51(2) which provides that "The civilian population as such, as well as individual civilians, shall not be the object of attack. Acts or threats of violence the primary purpose of which is to spread terror among the civilian population are prohibited"[145] and 52(2) which provides that "military targets shall be those whose use makes an effective contribution to the military action" of the same Additional Protocol of the Geneva Conventions of 1949.[146] It should also be noted that under Article 36 of the 1977 Additional Protocol to the Geneva Conventions of 1949, it is stated that “In the study, development, acquisition or adoption of a new weapon, means or method of warfare” a state is obliged to “determine whether its employment would, in some or all circumstances, be prohibited by this Protocol or by any other rule of international law applicable”.[147] In addition, civilian services that depend on systems of dual use, like telecommunications infrastructure, for their basic needs can also be affected by the collateral damage of cyber operations. Additionally, the psychological burden of life under constant digital threat is not to be underestimated. Communities can be filled with heightened anxiety and fear for potential system failures, and uncertainty over the safety of life-sustaining structures, like power or medical facilities.[148] However, it should be noted that almost no Article of the Geneva Conventions or their Additional Protocols, specifically mentions the origin of an attack against the territory or the civilian population of the belligerent states, thus making the Conventions potentially applicable to cyber and digital attacks.[149]

---

[142] Greenberg, A., & Excerpt. (2018, August 22). The untold story of NotPetya, the most devastating cyberattack in history. *WIRED*. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/
[143] Editor (Ed.). (1994). *PROTOCOLS ADDITIONAL TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949*. https://www.icrc.org/en/doc/assets/files/other/icrc_002_0321.pdf
[144] Editor (Ed.). (1994). *PROTOCOLS ADDITIONAL TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949*. https://www.icrc.org/en/doc/assets/files/other/icrc_002_0321.pdf
[145] Editor (Ed.). (1994). *PROTOCOLS ADDITIONAL TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949*. https://www.icrc.org/en/doc/assets/files/other/icrc_002_0321.pdf
[146]Editor (Ed.). (1994). *PROTOCOLS ADDITIONAL TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949*. https://www.icrc.org/en/doc/assets/files/other/icrc_002_0321.pdf
[147] Editor (Ed.). (1994). *PROTOCOLS ADDITIONAL TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949*. https://www.icrc.org/en/doc/assets/files/other/icrc_002_0321.pdf
[148] Schmitt, M. N. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press.
[149] Editor (Ed.). (1994). *PROTOCOLS ADDITIONAL TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949*. https://www.icrc.org/en/doc/assets/files/other/icrc_002_0321.pdf

The economic ramifications of a cyber-attack are yet another important dimension of potential civilian harm in a situation of digital war.[150] Cyber-attacks can affect financial systems, causing widespread job losses, and lengthy periods of instability in their wake.[151] For example, ransomware attacks on small businesses can lead to the business to require to lay off personnel, cause temporary personal financial hardship or even lead to organizational or community-level closures and in extreme cases even the complete collapse of the business. Those at the lowest socioeconomic groups often suffer the most from such economic shocks especially when pre-existing inequalities are exacerbated, the recovery efforts are slowed down, and the social safety nets are either underpinned or even inexistant.

In addition, indirect consequences of cyber-attacks on supply chains, food distribution, emergency services, etc., could generate a sequential level of regional or even global crises that would cripple financially poorer nations and would affect with immediate effect the most vulnerable categories of the population.[152] For instance, a cyber-attack on transportation networks may delay medical supplies, food, or humanitarian aid in conflict areas, worsening the suffering of civilian populations in situations that are already dire.[153]

Finding a Footing Between Security and Human Rights

Digital Warfare and Human Rights: A Complex problem for the creation of Reasonable Policies

When it comes to almost every aspect of international relations, States have the responsibility to protect their national interests.[154] This could not be any different in the case of the digitalization of warfare.[155] As such, States have a legitimate role to play in the protection of their national security and countering any potential digital threats, but measures need to aim to achieve these objectives in a proportionate, transparent, and consistent with human rights way.[156] In order to strike this balance a multi-pronged approach is required.
Firstly, a clear legal oversight needs to be created as setting clear legal frameworks that are

---

[150] Choudhury, B., & Petrin, M. (2019). *Corporate duties to the public*. Cambridge University Press.

[151] Shackelford, S., Fort, T. L., & Prenkert, J. D. (2014). How businesses can promote Cyber Peace. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2393528

[152] Rejali, S., & Heiniger, Y. (2020). The role of digital technologies in humanitarian law, policy and action: Charting a path forward. *International Review of the Red Cross*, *102*(913), 1–22. doi:10.1017/S1816383121000114

[153] Geiss, R., & Lahmann, H. (2021b, May 22). *Protection of data in armed conflict*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3851136

[154] UN. Office of the High Commissioner for Human Rights. (2014, June 30). *The right to privacy in the digital age :: report of the Office of the United Nations High Commissioner for Human Rights*. United Nations Digital Library System. https://digitallibrary.un.org/record/777869?v=pdf

[155] Roscini, M., & Trust, L. (2014). *Cyber operations and the use of force in international law*. Oxford University Press, USA.

[156] Schmitt, M. N. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press.

enforceable around the use of surveillance technologies, cyber operations, and digital tools.[157] Such independent oversight mechanisms are essential to ensure accountability, transparency, and methods compliant with human rights, that are consistent with international human rights standards.[158]

Secondly, technological safeguards have to be established, in order to facilitate the development and deployment of security-enhancing technologies that preserve and respect the right to privacy and the freedom of expression.[159] Solutions may include ground-breaking privacy-enhancing cryptographic technologies, the creation of ethical AI frameworks, or even stronger cybersecurity protections.[160]

Thirdly, the approach to resolving these problems should be multilateral, by cooperating to establish global standards and agreements when managing the use of digital tools in warfare.[161] Projects like the Tallinn Manual and ongoing United Nations discourse surrounding responsible state conduct in cyberspace demonstrate the importance of cohesive international structures.[162]

At the same time, states should try to raise public awareness of such dangers. This could be achieved by fostering awareness and enhancing education on digital threats and standing up for rights in a digital world.[163] Some strategies may include media literacy campaigns, public awareness programs, and community-driven initiatives to build social resilience to misinformation and surveillance.[164]

Lastly, states should promote corporate responsibility in their respective private sectors.[165] As states and companies are equally faced with the implications of digital warfare, it could be beneficial to pressure technology companies to be more responsible rather than being enablers of digital warfare.[166] To bring this discussion towards a conclusion, private sector actors should be reminded that they are to lead with ethics, and maintaining transparency in

---

[157] Winter, E. (2020). THE COMPATIBILITY OF AUTONOMOUS WEAPONS WITH THE PRINCIPLE OF DISTINCTION IN THE LAW OF ARMED CONFLICT. *International and Comparative Law Quarterly*, *69*(4), 845–876. doi:10.1017/S0020589320000378

[158] Hathaway, Oona & Crootof, Rebecca & Levitz, Philip & Nix, Haley & Nowlan, Aileen & Perdue, William & Spiegel, Julia. (2011). The Law of Cyber-Attack. California Law Review. 100.

[159] Akhgar, B., Saathoff, G. B., Arabnia, H. R., Hill, R., Staniforth, A., & Bayerl, P. S. (2015). *Application of Big Data for National Security: A Practitioner's Guide to Emerging technologies*. https://derby.openrepository.com/handle/10545/620925

[160] Henschke, A. (2020). Privacy, the Internet of Things and State Surveillance: Handling Personal Information within an Inhuman System. *Moral Philosophy and Politics*, *7*(1), 123-149. https://doi.org/10.1515/mopp-2019-0056

[161] Bannelier, K., & Christakis, T. (2017, February 25). *Cyber-Attacks – Prevention-Reactions: The role of states and private actors*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2941988

[162] Shackelford, S., Fort, T. L., & Prenkert, J. D. (2014). How businesses can promote Cyber Peace. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2393528

[163] Friedewald, M., Burgess, J. P., Cas, J., & Bellanova, R. (2020). *Surveillance, privacy and security: Citizens Perspectives*. Routledge.

[164] Macnish, K. (2017). The Ethics of Surveillance: An Introduction (1st ed.). Routledge. https://doi.org/10.4324/9781315162867

[165] Choudhury, B., & Petrin, M. (2019). *Corporate duties to the public*. Cambridge University Press.

[166] Henschke, A. (2017). *Ethics in an Age of Surveillance: Personal Information and Virtual Identities*. Cambridge: Cambridge University Press.

their operations and work in collaboration with governments to counter global cyber threats.[167]

Conclusion

Digital warfare has a profound influence on human rights on several levels. The rapid advancement of digital technologies presents not only challenges and danger but also opportunities when it comes to conflict prevention and resolution;[168] it is, therefore, of vital importance that governments, international organizations, and civil society bodies meet this challenge head-on to ensure a more peaceful world and avoid exacerbating already existing conflicts around the globe.[169] Globally, it is considered possible to reduce the risks posed by digital warfare with an approach to digital security that respects human rights, strengthening legal and ethical safeguards, and inciting international collaboration.[170] Should the basic tenets of human dignity, liberty, and justice be respected, the result is going to be a technological advancement that serves humanity's needs and not one that deepens existing divides and chronic vulnerabilities.[171]

---

[167] International Institute for Strategic Studies (IISS). Cyber Capabilities and National Power: A Net Assessment. IISS, 2021.
[168] Schmitt, M. N. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press.
[169] Bannelier, K., & Christakis, T. (2017, February 25). *Cyber-Attacks – Prevention-Reactions: The role of states and private actors*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2941988
[170] Deeks, A. (2014b, September 1). *An international legal framework for surveillance*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2490700
[171] **Nye, J. S. (2011).** *The Future of Power.* PublicAffairs

IV. HUMANITARIAN LAW UNDER CHALLENGE

Coverage of Digital Warfare Under International Humanitarian Law (IHL)

As warfare has progressed into the digital landscape in the past few decades, the implications for International Humanitarian Law (IHL), which was designed for conventional wars in a time, when Cyberspace and small personal computers were more of a science fiction idea rather than an actual reality, are profound.[172] Key principles of IHL such as distinction, proportionality, and necessity face significant challenges within the cyber domain.[173] These principles, which are fundamental to the protection of civilians and ensuring the appropriate conduct in warfare, between belligerent powers, become more and more challenging in their enforcement when it comes to digital warfare.[174]

Principle of Distinction

The doctrine of distinction requires, according to the relevant articles of the Geneva Conventions of 1949 and their Protocols, specifically Articles 48, 51(2) and 52(2) of Protocol I[175], belligerents to distinguish between combatants and non-combatants and to only direct their military actions accordingly.[176] But when it comes to the digital domain, civilian and military infrastructure are often intermingled, making the potential application of this international norm.[177] As such, for example, a strike on a nation's power generation facilities could very likely render their military command centres non-operational, but could also leave hospitals, schools, and homes without power for a lengthy period of time. Such interconnections lead to ambiguity, which will make the realization of the principle of distinction difficult.[178]

---

[172] Roscini, M., & Trust, L. (2014). *Cyber operations and the use of force in international law*. Oxford University Press, USA.

[173] Hathaway, Oona & Crootof, Rebecca & Levitz, Philip & Nix, Haley & Nowlan, Aileen & Perdue, William & Spiegel, Julia. (2011). The Law of Cyber-Attack. California Law Review. 100.

[174] Melzer, N. (2013). Human rights implications of the usage of drones and unmanned robots in warfare. In European Parliament's Subcommittee on Human Rights, *Policy Department DG External Policies* (p. PE 410.220 EN). European Union. https://doi.org/10.2861/213

[175] Editor (Ed.). (1994). *PROTOCOLS ADDITIONAL TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949*. https://www.icrc.org/en/doc/assets/files/other/icrc_002_0321.pdf

[176] Schmitt, M. N. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press.

[177] International Committee of the Red Cross. (2015). International humanitarian law and the challenges of contemporary armed conflicts. In *32nd INTERNATIONAL CONFERENCE OF THE RED CROSS AND RED CRESCENT*. https://www.icrc.org/sites/default/files/document/file_list/32ic-report-on-ihl-and-challenges-of-armed-conflicts.pdf

[178] Hathaway, Oona & Crootof, Rebecca & Levitz, Philip & Nix, Haley & Nowlan, Aileen & Perdue, William & Spiegel, Julia. (2011). The Law of Cyber-Attack. California Law Review. 100.

The situation is further complicated by the use of civilian networks as digital tools to meet military ends.[179] Cyber operations may co-opt civilian systems to launch attacks, rendering those systems targets in potential attacks.[180] This dual-use nature of infrastructure makes the protection of civilian entities difficult and aggravates the risk of collateral damage.[181] Furthermore, the proliferation of Internet of Things (IoT) devices further obscures the limits between civilian and military, and on-the-surface nonmilitary capabilities available in civilian devices may take on new utility within military mission plans, and thus compliance with the principle of distinction becomes even more difficult and challenging.[182]

Principle of Proportionality

When military operations are taking place, the principle of proportionality applies, according to the relevant articles of the Geneva Conventions of 1949 and their Additional Protocols, specifically Articles 51(5)(b) and 57(2)(b) of Protocol I[183], under which it is stipulated that the potential damage inflicted on civilians must not be out of proportion to the military advantage gained.[184] Cyber operations pose challenges for this principle because their effects are usually widespread, unpredictable, and disproportionate.[185] For example, a cyber-attack designed to disable an adversary's communication networks could inadvertently interfere with emergency services, financial institutions, or transportation systems and therefore, inflict damage far greater than the intended military target.[186]
Part of the problem is the fact that the determination of the likely degrees of collateral damage from cyber operations is extremely difficult.[187] The effects of cyber weapons, unlike conventional ones, do not always materialize in an instant and usually unfold in unexpected and unpredictable ways, disrupting interconnected systems resulting in cascading and

---

[179] Bannelier, K., & Christakis, T. (2017, February 25). *Cyber-Attacks – Prevention-Reactions: The role of states and private actors*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2941988
[180] Rejali, S., & Heiniger, Y. (2020). The role of digital technologies in humanitarian law, policy and action: Charting a path forward. *International Review of the Red Cross*, *102*(913), 1–22. doi:10.1017/S1816383121000114
[181] Melzer, N. (2013). Human rights implications of the usage of drones and unmanned robots in warfare. In European Parliament's Subcommittee on Human Rights, *Policy Department DG External Policies* (p. PE 410.220 EN). European Union. https://doi.org/10.2861/213

[182] Henschke, A. (2020). Privacy, the Internet of Things and State Surveillance: Handling Personal Information within an Inhuman System. *Moral Philosophy and Politics*, *7*(1), 123-149. https://doi.org/10.1515/mopp-2019-0056
[183] Editor (Ed.). (1994). *PROTOCOLS ADDITIONAL TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949*. https://www.icrc.org/en/doc/assets/files/other/icrc_002_0321.pdf
[184] Schmitt, M. N. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press.
[185] Hathaway, Oona & Crootof, Rebecca & Levitz, Philip & Nix, Haley & Nowlan, Aileen & Perdue, William & Spiegel, Julia. (2011). The Law of Cyber-Attack. California Law Review. 100.
[186] Geiss, R., & Lahmann, H. (2021b, May 22). *Protection of data in armed conflict*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3851136
[187] Bannelier, K., & Christakis, T. (2017, February 25). *Cyber-Attacks – Prevention-Reactions: The role of states and private actors*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2941988

failures.[188] Furthermore, the absence of comprehensive information about the degree of damage caused by prior cyber conflicts drastically limits the feasibility of the development of accurate predictive models for proportionality assessments in potential future conflicts.[189]

Principle of Necessity

The principle of necessity, as stipulated in the Geneva Conventions of 1949 and their Additional Protocols, the Hague Regulations of 1907 and the Rome Statute of the International Criminal Court of 1908, and specifically Articles 1(2), 35(1) and 52(2) of Geneva Conventions Protocol I[190], the Preamble and Article 23(g) of the Hague Regulations[191] and Article 8(2)(b)(iv) of the Rome Statute of the International Criminal Court[192], requires that military action must be necessary to accomplish a legitimate military objective.[193] The observance of this principle becomes even more complex in the realm of digital warfare, where cyber operations may be executed by a number of actors and be under several layers of obfuscation.[194] When those responsible operate in anonymity or when infrastructure that should be civilian is used for military purposes, it is difficult to determine if an operation is strictly necessary.[195]
Matters are further complicated by the fact that the clandestine nature of many cyber operations makes it hard to assess whether alternatives to a cyber-attack might accomplish the same goal, with less of a cost.[196] This level of secrecy severely limits the ability of legal actors to scrutinize the necessity of specific cyber acts.[197]

Ethical Issues of Autonomous Weapons

The development of Artificial intelligence has led to the creation of a weapon system that poses extremely important ethical questions and challenges for International Humanitarian

---

[188] Rejali, S., & Heiniger, Y. (2020). The role of digital technologies in humanitarian law, policy and action: Charting a path forward. *International Review of the Red Cross*, *102*(913), 1–22. doi:10.1017/S1816383121000114
[189] Brown, G.D. (2011). Why Iran Didn't Admit Stuxnet Was an Attack. Joint Force Quarterly, 63, 70-73.
[190] Editor (Ed.). (1994). *PROTOCOLS ADDITIONAL TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949*. https://www.icrc.org/en/doc/assets/files/other/icrc_002_0321.pdf
[191] Second International Peace Conference, The Hague, Convention (IV) Respecting the Laws and Customs of War on Land and Its Annex: Regulations Concerning the Laws and Customs of War on Land, -, International Conferences (The Hague), 18 October 1907, https://www.refworld.org/legal/agreements/hague/1907/en/31788
[192] International Criminal Court. (2021). Rome Statute of the International Criminal Court. In *Rome Statute of the International Criminal Court* [Book]. https://asp.icc-cpi.int/en_menus/asp/RomeStatute/pages/default.aspx
[193] Schmitt, M. N. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press.
[194] Hathaway, Oona & Crootof, Rebecca & Levitz, Philip & Nix, Haley & Nowlan, Aileen & Perdue, William & Spiegel, Julia. (2011). The Law of Cyber-Attack. California Law Review. 100.
[195] Bannelier, K., & Christakis, T. (2017, February 25). *Cyber-Attacks – Prevention-Reactions: The role of states and private actors*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2941988
[196] Rejali, S., & Heiniger, Y. (2020). The role of digital technologies in humanitarian law, policy and action: Charting a path forward. *International Review of the Red Cross*, *102*(913), 1–22. doi:10.1017/S1816383121000114
[197] Roscini, M., & Trust, L. (2014). *Cyber operations and the use of force in international law*. Oxford University Press, USA.

law.[198] These, Autonomous weapons systems (AWS) that are utilizing artificial intelligence (usually for guidance and target acquisition) are being fielded by armed forces in more and more instances in concurrent warfare.[199] These systems are capable of autonomously receiving information about their potential targets and selecting the most suitable option to engage these targets without human intervention and with minimal human input, creating a series of important ethical and legal implications under IHL.[200] These implications are analysed in the following sections.

Accountability and Responsibility

One of the most important implications under IHL in regards with AWS is that of accountability.[201] In the event where there is a malfunction in the guidance and/or the target acquisition system of the AWS and the autonomous weapon makes an unlawful decision, killing a number of innocent civilians, it is not clear who should be held responsible in such a case.[202] Should it be the responsibility of the programmer who developed and tested the guidance and the targeting algorithms? Should it be the responsibility of the company that manufactured the electronics and the weapon itself?[203] Should the responsibility fall on the operator of the weapon, who in practice may have limited or even no input on the AWS? Or should the responsibility fall on the state that deployed the faulty weapon?[204] This absence of clearly defined accountability not only does it shake the very foundations of the principles of IHL to their core and not only does it undermine the enforcement of IHL in war but also it may deny justice from victims.[205]

To further complicate matters, AWS would also likely create problems in the determination of a clear chain of command and establish a clear control framework, which could hinder even more the existing problems of accountability under IHL in the case of AWS. This lack of

---

[198] Winter, E. (2020). THE COMPATIBILITY OF AUTONOMOUS WEAPONS WITH THE PRINCIPLE OF DISTINCTION IN THE LAW OF ARMED CONFLICT. *International and Comparative Law Quarterly*, *69*(4), 845–876. doi:10.1017/S0020589320000378

[199] Ohlin, J.D. (2016). The Combatant's Stance: Autonomous Weapons on the Battlefield. *International law studies, 92*, 1.

[200] Melzer, N. (2013). Human rights implications of the usage of drones and unmanned robots in warfare. In European Parliament's Subcommittee on Human Rights, *Policy Department DG External Policies* (p. PE 410.220 EN). European Union. https://doi.org/10.2861/213

[201] Ohlin, J.D. (2016). The Combatant's Stance: Autonomous Weapons on the Battlefield. *International law studies, 92*, 1.

[202] Winter, E. (2020). THE COMPATIBILITY OF AUTONOMOUS WEAPONS WITH THE PRINCIPLE OF DISTINCTION IN THE LAW OF ARMED CONFLICT. *International and Comparative Law Quarterly*, *69*(4), 845–876. doi:10.1017/S0020589320000378

[203] Choudhury, B., & Petrin, M. (2019). *Corporate duties to the public*. Cambridge University Press.

[204] Melzer, N. (2013). Human rights implications of the usage of drones and unmanned robots in warfare. In European Parliament's Subcommittee on Human Rights, *Policy Department DG External Policies* (p. PE 410.220 EN). European Union. https://doi.org/10.2861/213

[205] Rejali, S., & Heiniger, Y. (2020). The role of digital technologies in humanitarian law, policy and action: Charting a path forward. *International Review of the Red Cross*, *102*(913), 1–22. doi:10.1017/S1816383121000114

consistent frameworks for accountability could lead state and non-state actors alike to deploy AWS without appropriate oversight (if any at all), drastically increasing the risk of misuse or unintended, unnecessary and disproportionate harm to civilians.[206]

Compliance with IHL

Autonomous weapons systems raise also a challenge against a fundamental norm of IHL, as they basically bypass IHL's requirement that it should be human judgment that should guide questions of proportionality and distinction, rather than algorithmic calculation.[207] Even though such systems could potentially limit the possibilities of human errors, their dependence on algorithms and machine learning creates a high level of unpredictability.[208] In addition, the utilization of AWS brings up ethical concerns regarding the programming of machines so that they may decide matters of life and death and leading to the overall degradation of the sanctity of human life.[209] It should be noted that the opposing side argues that the delegation of such a lethal choice to mere machines violates the very laws and even the highest morals of humanity as it removes from war the moral responsibility that is central to state and personal sovereignty.

There are also significant technical challenges in trying to integrate IHL compliance within the coding of AWS systems.[210] Encoding them into algorithms, however, is extremely hard for various reasons, such as the fact that they depend on subjective judgment (e.g., distinction and proportionality) between an autonomous system and its target.[211] This clash between the laws defining IHL, and the human-in-the-loop capabilities of AWS, is a key legal gap.

It should however be noted that, the international community has come to an agreement, that the human element is not going to be fully removed from conflict and warfare.[212]

Attribution in Cyber Warfare

---

[206] Anderson, K., & Waxman, M. C. (2013). Law and Ethics for Autonomous Weapon Systems: Why a Ban Won't Work and How the Laws of War Can. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2250126

[207] Winter, E. (2020). THE COMPATIBILITY OF AUTONOMOUS WEAPONS WITH THE PRINCIPLE OF DISTINCTION IN THE LAW OF ARMED CONFLICT. *International and Comparative Law Quarterly*, *69*(4), 845–876. doi:10.1017/S0020589320000378

[208] Melzer, N. (2013). Human rights implications of the usage of drones and unmanned robots in warfare. In European Parliament's Subcommittee on Human Rights, *Policy Department DG External Policies* (p. PE 410.220 EN). European Union. https://doi.org/10.2861/213

[209] International Committee of the Red Cross (ICRC). Autonomous Weapon Systems: Technical, Military, Legal, and Humanitarian Aspects. ICRC, 2016.

[210] Corn, G. S. (2014). Autonomous weapon systems: legal consequences of taking the man out of the LOOPP. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2450640

[211] Choudhury, B., & Petrin, M. (2019). *Corporate duties to the public*. Cambridge University Press.

[212] Rejali, S., & Heiniger, Y. (2020). The role of digital technologies in humanitarian law, policy and action: Charting a path forward. *International Review of the Red Cross*, *102*(913), 1–22. doi:10.1017/S1816383121000114

Attribution (the identification of the actor behind the attack) is one of the biggest challenges in the application of IHL to the cyber domain.[213] Since they are conducted anonymously, cyber-attacks and cyber operations typically use malicious techniques to aid the attacker in effectively hiding their identity and location of origin.[214] This near complete anonymity further complicates the determination of who is attributable for cyber-attacks to and hinders efforts to respond to these attacks by making enforcement and proportionality more challenging.[215]

False Flag Operations

Cyber operations frequently incorporate false flag techniques.[216] In these usually the attacker leaves deceptive clues so that the suspicion for the cyber-attack will fall to a state or non-state actor other than the one that actually ordered the cyber-attack.[217] This way the attacker is able to mask their activities making them seem like they were executed by someone completely different.[218] Not only do these tactics create obstacles for attribution, but they also threaten to escalate existing conflicts or create new ones based on the misidentification.[219] These campaigns take advantage of the intricacies of international relations in combination with the ambiguities of cyberspace to sow distrust among countries and make it harder to conduct diplomatic relations.[220]

False flag operations also jeopardize international stability by calling into question both confidence in attribution mechanisms and confidence between states.[221] This ambiguity may enable states to place the blame of a cyber-attack on another state and avoid taking

---

[213] Roscini, M., & Trust, L. (2014). *Cyber operations and the use of force in international law*. Oxford University Press, USA.

[214] Schmitt, M. N. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press.

[215] Bannelier, K., & Christakis, T. (2017, February 25). *Cyber-Attacks – Prevention-Reactions: The role of states and private actors*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2941988

[216] Hathaway, Oona & Crootof, Rebecca & Levitz, Philip & Nix, Haley & Nowlan, Aileen & Perdue, William & Spiegel, Julia. (2011). The Law of Cyber-Attack. California Law Review. 100.

[217] Roscini, M., & Trust, L. (2014). *Cyber operations and the use of force in international law*. Oxford University Press, USA.

[218] Schmitt, M. N. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press.

[219] Bannelier, K., & Christakis, T. (2017, February 25). *Cyber-Attacks – Prevention-Reactions: The role of states and private actors*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2941988

[220] Geiss, R., & Lahmann, H. (2021b, May 22). *Protection of data in armed conflict*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3851136

[221] Melzer, N. (2013). Human rights implications of the usage of drones and unmanned robots in warfare. In European Parliament's Subcommittee on Human Rights, *Policy Department DG External Policies* (p. PE 410.220 EN). European Union. https://doi.org/10.2861/213

responsibility for their actions.[222] This dynamic sets positive permissiveness for cyber aggression that may further destabilize the already unstable global security.[223]

Political and Diplomatic Ramifications

The absence of clear attribution mechanisms due to these false flag operations may have major legal and diplomatic ramifications.[224] In the absence of clear proof for the exact identity of the attacker, states could delay a potential response, worried that they would retaliate against the wrong state. Such uncertainty may weaken the deterrence effect of IHL and potentially hinders international efforts to hold violators of IHL accountable.[225]

Without robust attribution mechanisms, states can exploit this loophole in order to launch covert cyber operations with little to minimal risk of retaliation by the victim of the cyber-attack, a practice that drastically undermines the legitimacy of international law and encourages state and non-state actors to act out in an escalatory manner.[226]

New Norms and Legal Proposals

This analysis illustrates the necessity to propose new international norms and other legal proposals, so that the IHL can close the current loopholes that exist in its current codification. Faced by questions posed by digital and cyber warfare, it is imperative that an effort to update the international rules set needs to be made.[227] Fortunately, multiple legal intellectuals have proposed documents that could be the basis of a potential reform of the current IHL regime to incorporate norms and rules in order to regulate digital and cyber conflict:[228]

A first potential formulation of new norms could be done through the adaptation of current IHL treaties to Cyber Strategies.[229] Diplomatic efforts could be made either at the United Nations or at the national level to create new protocols under older international treaties like the Geneva Conventions that would explicitly address and regulate the warfare in the cyber

---

[222] Rejali, S., & Heiniger, Y. (2020). The role of digital technologies in humanitarian law, policy and action: Charting a path forward. *International Review of the Red Cross*, *102*(913), 1–22. doi:10.1017/S1816383121000114

[223] Roscini, M., & Trust, L. (2014). *Cyber operations and the use of force in international law*. Oxford University Press, USA.

[224] Michael Schmitt, Classification of Cyber Conflict, *Journal of Conflict and Security Law*, Volume 17, Issue 2, Summer 2012, Pages 245–260, https://doi.org/10.1093/jcsl/krs018

[225] Hathaway, Oona & Crootof, Rebecca & Levitz, Philip & Nix, Haley & Nowlan, Aileen & Perdue, William & Spiegel, Julia. (2011). The Law of Cyber-Attack. California Law Review. 100.

[226] Rejali, S., & Heiniger, Y. (2020). The role of digital technologies in humanitarian law, policy and action: Charting a path forward. *International Review of the Red Cross*, *102*(913), 1–22. doi:10.1017/S1816383121000114

[227] Roscini, M., & Trust, L. (2014). *Cyber operations and the use of force in international law*. Oxford University Press, USA.

[228] Schmitt, M. N. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press.

[229] Hathaway, Oona & Crootof, Rebecca & Levitz, Philip & Nix, Haley & Nowlan, Aileen & Perdue, William & Spiegel, Julia. (2011). The Law of Cyber-Attack. California Law Review. 100.

domain.[230] Such protocols could offer specific parameters for criteria of targeting, assessments of proportionality, and assessments for civilian cyber infrastructure.[231]

This could also happen by the reinforcement of International Laws. This could be led by the creation of new agreements and treaties at the state level in order to determine what should be considered acceptable behaviour both in cyber space and across borders, including protections for private civilian infrastructures.[232] All international laws mentioned above could also contain clauses that follow an approach to joint attribution methods to have better capabilities to hold parties accountable through transparency.[233]

Advanced Attribution Processes could be another solution, that would lead to strengthening investment in capacity-building technologies and international mechanisms that will improve processes of determining attribution and accountability in the case of cyber-attacks.[234] Emerging technologies like blockchain and AI-based forensic tools could become critical in strengthening the attribution capabilities.[235]

Regulations on Autonomous Weapons may be established through the implementation of an International Set of Standards.[236] This should be accomplished by formulating new international norms for the design, deployment, and utilization of AWS to assure adherence to IHL and address the ethical issues that have been raised.[237] Such rules may include stipulations about potential human oversight, frameworks for explicit attribution, and limitations on the deployment of completely autonomous systems in lethal capacities.[238] However, as mentioned earlier, for the time being, there is agreement among states that the human element will remain in the realm of warfare.[239]

---

[230] Bannelier, K., & Christakis, T. (2017, February 25). *Cyber-Attacks – Prevention-Reactions: The role of states and private actors*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2941988

[231] Rejali, S., & Heiniger, Y. (2020). The role of digital technologies in humanitarian law, policy and action: Charting a path forward. *International Review of the Red Cross*, *102*(913), 1–22. doi:10.1017/S1816383121000114

[232] Geiss, R., & Lahmann, H. (2021b, May 22). *Protection of data in armed conflict*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3851136

[233] Schmitt, M. N. (2011). Cyber operations and the jus ad bellum revisited. *Vill. L. Rev.*, *56*, 569.

[234] Melzer, N. (2013). Human rights implications of the usage of drones and unmanned robots in warfare. In European Parliament's Subcommittee on Human Rights, *Policy Department DG External Policies* (p. PE 410.220 EN). European Union. https://doi.org/10.2861/213

[235] Choudhury, B., & Petrin, M. (2019). *Corporate duties to the public*. Cambridge University Press.

[236] Ohlin, J.D. (2016). The Combatant's Stance: Autonomous Weapons on the Battlefield. *International law studies, 92*, 1.

[237] Winter, E. (2020). THE COMPATIBILITY OF AUTONOMOUS WEAPONS WITH THE PRINCIPLE OF DISTINCTION IN THE LAW OF ARMED CONFLICT. *International and Comparative Law Quarterly*, *69*(4), 845–876. doi:10.1017/S0020589320000378

[238] Anderson, K., & Waxman, M. C. (2013). Law and Ethics for Autonomous Weapon Systems: Why a Ban Won't Work and How the Laws of War Can. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2250126

[239] International Committee of the Red Cross (ICRC). Autonomous Weapon Systems: Technical, Military, Legal, and Humanitarian Aspects. ICRC, 2016.

Finally, the enhancement of potential bodies for International Cyber Governance could create new global institutions to manage and mitigate potential tensions derived by a cyber-attack, that would facilitate constructive dialogue between states to further the cooperation when it comes to the cyber domain,[240] and build consensus on the emerging challenges of digital warfare.[241] These institutions could help promote the adoption of new norms and coordinate responses to violations.[242]

Conclusion

It is true that, today International Humanitarian Law faces some of the greatest challenges due to the introduction of digital and cyber tools in warfare[243] and AI-powered autonomous weapons.[244] On the other hand, these challenges require that the international community finds the necessary consensus to adapt existing legal frameworks,[245] while developing new norms, and strengthening mechanisms that ensure accountability and attribution in the cyber and digital domain.[246] In doing so, it can ensure that the principles of distinction, proportionality, and necessity continue to safeguard civilian life and maintain the ethical conduct of warfare in the 21st century.[247] Robust international cooperation and innovation in both legal and technical spheres will be critical to closing the gap between traditional IHL and the realities of modern conflict.[248]

---

[240] Rejali, S., & Heiniger, Y. (2020). The role of digital technologies in humanitarian law, policy and action: Charting a path forward. *International Review of the Red Cross*, *102*(913), 1–22. doi:10.1017/S1816383121000114

[241] Bannelier, K., & Christakis, T. (2017, February 25). *Cyber-Attacks – Prevention-Reactions: The role of states and private actors*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2941988

[242] Schmitt, M. N. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press.

[243] Roscini, M., & Trust, L. (2014). *Cyber operations and the use of force in international law*. Oxford University Press, USA.

[244] Ohlin, J.D. (2016). The Combatant's Stance: Autonomous Weapons on the Battlefield. *International law studies, 92*, 1.

[245] Bannelier, K., & Christakis, T. (2017, February 25). *Cyber-Attacks – Prevention-Reactions: The role of states and private actors*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2941988

[246] Schmitt, M. N. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press.

[247] Hathaway, Oona & Crootof, Rebecca & Levitz, Philip & Nix, Haley & Nowlan, Aileen & Perdue, William & Spiegel, Julia. (2011). The Law of Cyber-Attack. California Law Review. 100.

[248] Melzer, N. (2013). Human rights implications of the usage of drones and unmanned robots in warfare. In European Parliament's Subcommittee on Human Rights, *Policy Department DG External Policies* (p. PE 410.220 EN). European Union. https://doi.org/10.2861/213

V. Case Studies

Stuxnet and the Iranian Nuclear Facilities

Stuxnet may be the best-known cyber weapon in the brief history of digital and cyber warfare.[249] It is a canonical case study of how a single cyber weapon can take out critical infrastructure without having to fire a single bullet.[250] Uncovered in 2010, Stuxnet was a delicate computer worm purposely aimed at the programmable logic controllers (PLCs) controlling the centrifuges at Iran's nuclear enrichment facilities.[251] These facilities were crucial to Iran's nuclear program[252] while also supplying power to neighbouring regions, magnifying the attack's impact on civilian life.[253]

The operation, believed to have been executed by state-sponsored actors working for the United States and Israel, caused vast physical damage to the centrifuges by changing how quickly they operated[254] while making the PLCs falsely report to the monitoring systems that everything was normal with the devices.[255] This sabotage pushed Iran's nuclear program back by years, delaying its ability to enrich nuclear material and offering a massive strategic advantage to its adversaries in the region of the Middle East.[256] However, the impact of Stuxnet did not stay confined to its targeted effects, revealing the vulnerabilities of industrial control systems all around the world, leading to increased scrutiny of industrial cybersecurity practices in critical infrastructure sectors like energy, transportation, and manufacturing.[257]

Practices: The Legal and Ethical Implications of Stuxnet

Although the strike sought to accomplish a military goal with minimal human casualties, it created fundamental questions about the use of cyber weapons against so-called dual-use facilities — civilian infrastructure with military uses, as is the case in this cyber-attack.[258] The operation revealed the obscure limits between strategic purposes and IHL (International

---

[249] Schmitt, M. N. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press.

[250] Roscini, M., & Trust, L. (2014). *Cyber operations and the use of force in international law*. Oxford University Press, USA.

[251] Brown, G.D. (2011). Why Iran Didn't Admit Stuxnet Was an Attack. Joint Force Quarterly, 63, 70-73.

[252] Geiss, R., & Lahmann, H. (2021b, May 22). *Protection of data in armed conflict*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3851136

[253] Rejali, S., & Heiniger, Y. (2020). The role of digital technologies in humanitarian law, policy and action: Charting a path forward. *International Review of the Red Cross*, *102*(913), 1–22. doi:10.1017/S1816383121000114

[254] Bannelier, K., & Christakis, T. (2017, February 25). *Cyber-Attacks – Prevention-Reactions: The role of states and private actors*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2941988

[255] Brown, G.D. (2011). Why Iran Didn't Admit Stuxnet Was an Attack. Joint Force Quarterly, 63, 70-73.

[256] Brown, G.D. (2011). Why Iran Didn't Admit Stuxnet Was an Attack. Joint Force Quarterly, 63, 70-73.

[257] Ventre, D. (2012b). *Cyber conflict: Competing National Perspectives*. Wiley-ISTE.

[258] Schmitt, M. N. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press.

Humanitarian Law) violations, particularly in regards to proportionality and protection of civilian critical infrastructure.[259]

This not only represented a new form of warfare but also established a precedent for the use of cyberweapons that raised concerns about the proliferation of cyber and digital weapons and the potential weaponization of these technologies by both state and non-state actors.[260] Its success has spurred advances in cyber weaponry, leading to the development of similar even more advanced tools by allies and foes alike but raising fears of retaliatory attacks by adversaries including Iran.[261] It illustrated important lessons about the unintended consequences of cyber operations and the need for global norms governing them.[262]

NotPetya and the New World of Cyberwarfare

Another very important and somewhat well-known event in the history of digital and cyber warfare is the NotPetya cyber-attack, which originated in Ukraine in 2017.[263] At first operating under the guise of a ransomware attack, NotPetya was a destructive malware meant to erase data and cripple operations.[264] Even Though its primary target was against Ukrainian government institutions, energy production companies, and financial systems, its impact spread rapidly all around the world, disrupting multinational corporations and critical infrastructure across the globe.[265]

NotPetya, attributed to Russian state-sponsored actors, inflicted billions of dollars in damages.[266] Global multinational corporations operating in the sector of global transport of goods including Maersk, FedEx, and Merck suffered massive operational disruptions, leading to delays in logistical transports — a potent illustration of how interconnected the vulnerabilities of a globalized, digital network can be.[267] The indiscriminate nature of the assault illustrated how cyber operations can quickly escape the environment of their intended targets, infecting potentially in a rapid manner the entirety of global networks causing

---

[259] Roscini, M., & Trust, L. (2014). *Cyber operations and the use of force in international law*. Oxford University Press, USA.

[260] Hathaway, Oona & Crootof, Rebecca & Levitz, Philip & Nix, Haley & Nowlan, Aileen & Perdue, William & Spiegel, Julia. (2011). The Law of Cyber-Attack. California Law Review. 100.
[261] Brown, G.D. (2011). Why Iran Didn't Admit Stuxnet Was an Attack. Joint Force Quarterly, 63, 70-73.
[262] Rejali, S., & Heiniger, Y. (2020). The role of digital technologies in humanitarian law, policy and action: Charting a path forward. *International Review of the Red Cross*, *102*(913), 1–22. doi:10.1017/S1816383121000114
[263] Schmitt, M. N. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press.
[264] Roscini, M., & Trust, L. (2014). *Cyber operations and the use of force in international law*. Oxford University Press, USA.

[265] Greenberg, A., & Excerpt. (2018, August 22). The untold story of NotPetya, the most devastating cyberattack in history. *WIRED*. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/
[266] Hathaway, Oona & Crootof, Rebecca & Levitz, Philip & Nix, Haley & Nowlan, Aileen & Perdue, William & Spiegel, Julia. (2011). The Law of Cyber-Attack. California Law Review. 100.
[267] Geiss, R., & Lahmann, H. (2021b, May 22). *Protection of data in armed conflict*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3851136

collateral damage and financial harm to organizations that may not be even remotely related to the intended target.[268]

The legacy of NotPetya goes beyond the immediate financial and operational damage.[269] It pressed for international discourse on state accountability, demonstrating both the shortcomings of the extant legal frameworks to tackle cyber conflicts.[270] The attack paved the way for better resilience in corporate and governmental cybersecurity systems and led to major investments in prevention and response capability.[271]

The notorious cyberattack NotPetya has changed the landscape of global cyber threats, demonstrating the importance of collective defence mechanisms and more robust international standards in preventing future attacks.[272] It showed just how ill-prepared even advanced economies and companies were to respond to such threats, helping spur modernization of defences and closer international cooperation in international cyberspace.[273]

Hacking Back: A Legal Framework for Defensive Cyber Operations

Since 2014, Russia has used an expanded cyber strategy alongside its military operations in Ukraine, incorporating direct cyber-attacks, informational warfare, and electronic warfare in combination with conventional military operations.[274] The 2015 and 2016 power grid attacks were significant events for the evolution of cyber warfare,[275] with Russian operations having targets as diverse as Ukraine's energy grid, media outlets, and government institutions.[276]

The 2015 attack, the first known case of a cyber operation causing a power outage, left tens of thousands of Ukrainians without access to power inside the winter.[277] Hackers broke into power generators, using their systems to turn off the grid while stopping restoration.[278] The

---

[268] Greenberg, A., & Excerpt. (2018, August 22). The untold story of NotPetya, the most devastating cyberattack in history. *WIRED*. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/
[269] Bannelier, K., & Christakis, T. (2017, February 25). *Cyber-Attacks – Prevention-Reactions: The role of states and private actors*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2941988
[270] Rejali, S., & Heiniger, Y. (2020). The role of digital technologies in humanitarian law, policy and action: Charting a path forward. *International Review of the Red Cross*, *102*(913), 1–22. doi:10.1017/S1816383121000114
[271] Ventre, D. (2012b). *Cyber conflict: Competing National Perspectives*. Wiley-ISTE.
[272] Rejali, S., & Heiniger, Y. (2020). The role of digital technologies in humanitarian law, policy and action: Charting a path forward. *International Review of the Red Cross*, *102*(913), 1–22. doi:10.1017/S1816383121000114
[273] Henschke, A. (2020). Privacy, the Internet of Things and State Surveillance: Handling Personal Information within an Inhuman System. *Moral Philosophy and Politics*, *7*(1), 123-149. https://doi.org/10.1515/mopp-2019-0056
[274] Schmitt, M. N. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press.
[275] Roscini, M., & Trust, L. (2014). *Cyber operations and the use of force in international law*. Oxford University Press, USA.

[276] Greenberg, A., & Excerpt. (2018, August 22). The untold story of NotPetya, the most devastating cyberattack in history. *WIRED*. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/
[277] Hathaway, Oona & Crootof, Rebecca & Levitz, Philip & Nix, Haley & Nowlan, Aileen & Perdue, William & Spiegel, Julia. (2011). The Law of Cyber-Attack. California Law Review. 100.
[278] Geiss, R., & Lahmann, H. (2021b, May 22). *Protection of data in armed conflict*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3851136

attack showed how cyber tools can complement kinetic operations by damaging critical services, undermining public morale, and degrading a nation's ability to deal with physical threats.[279]

Russia has employed digital misinformation campaigns that have further cemented the role of cyber strategies in hybrid warfare.[280] The use of propaganda efforts to destabilize Ukraine's governance and impact international opinion demonstrates that cyber operations do not only target infrastructures; they can also be used to influence perceptions and narratives.[281] In this context, such campaigns explain why resilience is needed, not limited to physical infrastructure but also to public awareness and information ecosystems.[282]

Ukraine's experience highlights the importance of international cooperation and strong cybersecurity measures and response capabilities in combating state-sponsored cyber-attacks.[283] It also serves as a warning of the potential grave implications of cyber-enabled conflict, which would benefit from a coordinated international approach.[284]

The Role of Non-State Actors

Hacktivist Groups

In the realm of cyber, non-state actors like hacktivist groups such as Anonymous are becoming crucial players in cyber operations.[285] These types of organizations, themselves often ideologically motivated, may operate without regard to the dictates of the state, attacking those entities they view as corrupt or oppressive.[286] What comes to mind is that Anonymous has conducted cyber-attacks on government institutions, corporations, and organizations accused of committing human rights abuses.[287]

---

[279] Shackelford, S., Fort, T. L., & Prenkert, J. D. (2014). How businesses can promote Cyber Peace. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2393528

[280] Bannelier, K., & Christakis, T. (2017, February 25). *Cyber-Attacks – Prevention-Reactions: The role of states and private actors*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2941988

[281] Kernighan, B. W. (2021). *Understanding the digital world: What You Need to Know about Computers, the Internet, Privacy, and Security, Second Edition*. Princeton University Press.

[282] Geiss, R., & Lahmann, H. (2021b, May 22). *Protection of data in armed conflict*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3851136

[283] Rejali, S., & Heiniger, Y. (2020). The role of digital technologies in humanitarian law, policy and action: Charting a path forward. *International Review of the Red Cross*, *102*(913), 1–22. doi:10.1017/S1816383121000114

[284] Melzer, N. (2013). Human rights implications of the usage of drones and unmanned robots in warfare. In European Parliament's Subcommittee on Human Rights, *Policy Department DG External Policies* (p. PE 410.220 EN). European Union. https://doi.org/10.2861/213

[285] Schmitt, M. N. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press.

[286] Clapham, Andrew, Human Rights Obligations of Non-State Actors in Conflict Situations (September 30, 2006). International Review of the Red Cross, Vol. 88, No. 863, pp. 491-523, 2006, Available at SSRN: https://ssrn.com/abstract=1338653

[287] Hathaway, Oona & Crootof, Rebecca & Levitz, Philip & Nix, Haley & Nowlan, Aileen & Perdue, William & Spiegel, Julia. (2011). The Law of Cyber-Attack. California Law Review. 100.

While such actions are frequently hailed as digital activism, they have blurred the lines between legitimate dissent and cyber warfare.[288] As hacktivist operations are decentralized and are not bound by accountability measures, this environment is prone to unintended consequences, such as data breaches that affect innocent parties and amplify tensions.[289]

Cyber Terrorism of Extremist Organizations

Terrorist groups have turned more and more to digital means for recruiting, propaganda, and cyber-attacks.[290] Encrypted communications and social media have allowed groups such as ISIS to distribute propaganda and coordinate operations and radicalization.[291] Cyber terrorism includes the defacing of government websites, running distributed denial-of-service (DDoS) attacks, and spreading extremist ideologies.[292]

The internet, with its decentralized and borderless nature, makes these operations really difficult to contain, only amplifying the reach of these attacks.[293] Combating this type of techno-terrorism must involve technological advancements, overseas cooperation, and grassroots counter-radicalization projects.[294]

Lessons from Case Studies

The case studies of Stuxnet, NotPetya, Russian operations in Ukraine, and non-state actors reveal the following crucial lessons for the international community.[295] Today's digitally interconnected digital infrastructure has created global interconnected vulnerabilities.[296] The excessive dependence of the majority of modern societies on digital infrastructure means that cyber-attacks can cause cascading harm and damage on infrastructure across sectors and borders.[297]

---

[288] Geiss, R., & Lahmann, H. (2021b, May 22). *Protection of data in armed conflict*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3851136

[289] Clapham, Andrew, Human Rights Obligations of Non-State Actors in Conflict Situations (September 30, 2006). International Review of the Red Cross, Vol. 88, No. 863, pp. 491-523, 2006, Available at SSRN: https://ssrn.com/abstract=1338653

[290] Schmitt, M. N. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press.

[291] Hathaway, Oona & Crootof, Rebecca & Levitz, Philip & Nix, Haley & Nowlan, Aileen & Perdue, William & Spiegel, Julia. (2011). The Law of Cyber-Attack. California Law Review. 100.

[292] Bannelier, K., & Christakis, T. (2017, February 25). *Cyber-Attacks – Prevention-Reactions: The role of states and private actors*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2941988

[293] Geiss, R., & Lahmann, H. (2021b, May 22). *Protection of data in armed conflict*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3851136

[294] Shackelford, S., Fort, T. L., & Prenkert, J. D. (2014). How businesses can promote Cyber Peace. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2393528

[295] Schmitt, M. N. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press.

[296] Roscini, M., & Trust, L. (2014). *Cyber operations and the use of force in international law*. Oxford University Press, USA.

[297] Greenberg, A., & Excerpt. (2018, August 22). The untold story of NotPetya, the most devastating cyberattack in history. *WIRED*. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

International Standards need to be agreed upon, as it is underscored by Incidents like NotPetya so that global cybersecurity can be improved globally.[298]

The Ukrainian experience indicates that resilient infrastructure and robust cybersecurity defences need to be built and developed.[299]

[298] Bannelier, K., & Christakis, T. (2017, February 25). *Cyber-Attacks – Prevention-Reactions: The role of states and private actors*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2941988

[299] Rejali, S., & Heiniger, Y. (2020). The role of digital technologies in humanitarian law, policy and action: Charting a path forward. *International Review of the Red Cross*, *102*(913), 1–22. doi:10.1017/S1816383121000114

VI. Evaluating Existing Legal Structures

Evaluation of International Humanitarian Law (IHL)

Treaties, including the Geneva Conventions and other guiding principles, form the basis of International Humanitarian Law (IHL), providing a legal framework for the regulation of armed conflict.[300] However, the digital era, characterized by cyber warfare and sophisticated tech-enabled methods of engagement, has exposed critical weaknesses in the ability of IHL to address modern challenges, despite the possibility that the provisions of the treaties it encompasses can be interpreted to cover in some shape or form cyberspace.[301] While IHL continues to serve as a vital foundation for determining the legality of conduct during war, it struggles to handle the complexities of cyber operations, particularly in areas such as attribution, civilian protection, and proportionality.[302]

International Humanitarian Law Competes with Digital Warfare

Despite its limitations, IHL remains a cornerstone of the international legal regime in the digital age. Its enduring relevance can be attributed to several key factors, including its adaptability and global acceptance.[303]

First, the foundational principles of IHL—distinction, proportionality, and necessity—retain their importance in determining the legality of cyber operations.[304] These principles provide a moral and legal framework for navigating the intricacies of digital warfare. While the specifics of their application may differ, they offer a lens through which to assess the ethical and legal dimensions of cyber engagements.[305] In this regard, these principles can serve as a bridge between conventional conflicts and the novel challenges posed by digital engagements, helping states interpret and apply IHL in new ways.[306]

Second, the flexible language of IHL allows for its extension to new methods of warfare, including cyber operations.[307] This adaptability ensures that the international legal system

---

[300] Schmitt, M. N. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press.
[301] Hathaway, Oona & Crootof, Rebecca & Levitz, Philip & Nix, Haley & Nowlan, Aileen & Perdue, William & Spiegel, Julia. (2011). The Law of Cyber-Attack. California Law Review. 100.
[302] hackelford, S., Fort, T. L., & Prenkert, J. D. (2014). How businesses can promote Cyber Peace. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2393528
[303] International Committee of the Red Cross. (2015). International humanitarian law and the challenges of contemporary armed conflicts. In *32nd INTERNATIONAL CONFERENCE OF THE RED CROSS AND RED CRESCENT*. https://www.icrc.org/sites/default/files/document/file_list/32ic-report-on-ihl-and-challenges-of-armed-conflicts.pdf
[304] Hathaway, Oona & Crootof, Rebecca & Levitz, Philip & Nix, Haley & Nowlan, Aileen & Perdue, William & Spiegel, Julia. (2011). The Law of Cyber-Attack. California Law Review. 100.
[305] Bannelier, K., & Christakis, T. (2017, February 25). *Cyber-Attacks – Prevention-Reactions: The role of states and private actors*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2941988
[306] Geiss, R., & Lahmann, H. (2021b, May 22). *Protection of data in armed conflict*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3851136
[307] Rejali, S., & Heiniger, Y. (2020). The role of digital technologies in humanitarian law, policy and action: Charting a path forward. *International Review of the Red Cross*, *102*(913), 1–22. doi:10.1017/S1816383121000114

remains relevant despite the rapid pace of technological advancement.[308] By interpreting established principles to encompass emerging technologies, IHL provides a bridge between traditional and modern conflict paradigms.[309] However, this flexibility also presents challenges, as it can lead to inconsistencies in interpretation and application, particularly when different states or actors interpret principles in conflicting ways.[310]

Finally, IHL's universal recognition fosters international cooperation in addressing the challenges posed by digital warfare.[311] As a globally accepted framework, it offers a common platform for states to engage in dialogue and collaboration, promoting shared norms and standards.[312] This universality is particularly valuable in the context of cyberspace, where the interconnected nature of digital systems demands coordinated responses.[313] The global recognition of IHL strengthens its legitimacy and ensures that it remains a reference point for developing new legal frameworks to address cyber conflicts.[314]

Limitations and Gaps

Despite its strengths, IHL faces significant challenges in effectively regulating cyber operations.[315] These challenges arise from the unique characteristics of cyberspace, which complicate the application of traditional legal principles.[316]

The anonymity of cyber-attacks is one of the most pressing issues.[317] Cyberspace's decentralized and borderless nature enables attackers to operate without revealing their

---

[308] Shackelford, S., Fort, T. L., & Prenkert, J. D. (2014). How businesses can promote Cyber Peace. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2393528

[309] Schmitt, M. N. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press.

[310] International Committee of the Red Cross. (2015). International humanitarian law and the challenges of contemporary armed conflicts. In *32nd INTERNATIONAL CONFERENCE OF THE RED CROSS AND RED CRESCENT*. https://www.icrc.org/sites/default/files/document/file_list/32ic-report-on-ihl-and-challenges-of-armed-conflicts.pdf

[311] Melzer, N. (2013). Human rights implications of the usage of drones and unmanned robots in warfare. In European Parliament's Subcommittee on Human Rights, *Policy Department DG External Policies* (p. PE 410.220 EN). European Union. https://doi.org/10.2861/213

[312] Henschke, A. (2020). Privacy, the Internet of Things and State Surveillance: Handling Personal Information within an Inhuman System. *Moral Philosophy and Politics*, *7*(1), 123-149. https://doi.org/10.1515/mopp-2019-0056

[313] UN. Office of the High Commissioner for Human Rights. (2014, June 30). *The right to privacy in the digital age :: report of the Office of the United Nations High Commissioner for Human Rights*. United Nations Digital Library System. https://digitallibrary.un.org/record/777869?v=pdf

[314] Rid, T. (2011). Cyber War Will Not Take Place. *Journal of Strategic Studies*, *35*(1), 5–32. https://doi.org/10.1080/01402390.2011.608939

[315] International Committee of the Red Cross. (2015). International humanitarian law and the challenges of contemporary armed conflicts. In *32nd INTERNATIONAL CONFERENCE OF THE RED CROSS AND RED CRESCENT*. https://www.icrc.org/sites/default/files/document/file_list/32ic-report-on-ihl-and-challenges-of-armed-conflicts.pdf

[316] Schmitt, M. N. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press.

[317] Hathaway, Oona & Crootof, Rebecca & Levitz, Philip & Nix, Haley & Nowlan, Aileen & Perdue, William & Spiegel, Julia. (2011). The Law of Cyber-Attack. California Law Review. 100.

identities, making attribution difficult and fostering a culture of impunity.[318] This lack of accountability not only undermines the deterrent effect of IHL but also emboldens actors to exploit the anonymity of cyberspace for malicious purposes.[319] False flag operations further exacerbate these challenges, allowing attackers to manipulate geopolitical responses and erode trust among states.[320] This difficulty in attribution creates a climate where states and non-state actors can act with limited fear of consequences, undermining the principles of responsibility and accountability.[321]

Another critical issue is the dual-use nature of digital systems, where civilian and military infrastructures often overlap.[322] This interdependence makes it challenging to distinguish between legitimate military targets and civilian objects, which are protected under IHL.[323] For example, an attack on a military communication system might inadvertently disrupt civilian services, such as hospitals or power grids, raising questions about compliance with the principle of distinction.[324] These complexities demand a nuanced approach to targeting decisions in the cyber domain, where the interconnectedness of systems can blur the lines between acceptable and unacceptable targets.[325]

Proportionality assessments are similarly complicated by the unpredictable and cascading effects of cyber-attacks.[326] The interconnected nature of digital systems amplifies the potential for unintended collateral damage, making it difficult to ensure that the harm inflicted is proportionate to the anticipated military advantage.[327] These challenges highlight the need for more sophisticated tools and methodologies to evaluate proportionality in cyber

---

[318] Bannelier, K., & Christakis, T. (2017, February 25). *Cyber-Attacks – Prevention-Reactions: The role of states and private actors*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2941988

[319] Michael Schmitt, Classification of Cyber Conflict, *Journal of Conflict and Security Law*, Volume 17, Issue 2, Summer 2012, Pages 245–260, https://doi.org/10.1093/jcsl/krs018

[320] Schmitt, M. N. (2011). Cyber operations and the jus ad bellum revisited. *Vill. L. Rev.*, *56*, 569.

[321] Clapham, Andrew, Human Rights Obligations of Non-State Actors in Conflict Situations (September 30, 2006). International Review of the Red Cross, Vol. 88, No. 863, pp. 491-523, 2006, Available at SSRN: https://ssrn.com/abstract=1338653

[322] Melzer, N. (2013). Human rights implications of the usage of drones and unmanned robots in warfare. In European Parliament's Subcommittee on Human Rights, *Policy Department DG External Policies* (p. PE 410.220 EN). European Union. https://doi.org/10.2861/213

[323] Shackelford, S., Fort, T. L., & Prenkert, J. D. (2014). How businesses can promote Cyber Peace. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2393528

[324] Schmitt, M. N. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press.

[325] Bannelier, K., & Christakis, T. (2017, February 25). *Cyber-Attacks – Prevention-Reactions: The role of states and private actors*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2941988

[326] Schmitt, M. N. (2011). Cyber operations and the jus ad bellum revisited. *Vill. L. Rev.*, *56*, 569

[327] Schmitt, M. N. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press.

operations.[328] Moreover, the lack of historical precedents for assessing proportionality in digital conflicts exacerbates the difficulty of developing standardized practices.[329]

IHL also struggles to address the activities of non-state actors, such as hacktivists, cybercriminals, and terrorist organizations.[330] These individuals and groups exploit the anonymity of cyberspace to operate beyond the reach of traditional law enforcement, creating significant accountability gaps.[331] While IHL primarily regulates state actions, the growing involvement of non-state actors in cyber conflicts underscores the need for expanded legal frameworks to govern their behaviour.[332] This gap is particularly concerning given the increasing sophistication and coordination of cyber-attacks orchestrated by non-state actors.[333]

International Humanitarian Law (IHL) Remains Relevant

Reforming IHL to address these gaps is essential to ensure its continued relevance in the digital age.[334] Several proposals have been advanced to enhance its applicability to cyber operations.[335]

Targeting guidance for dual-use systems is a critical area for reform.[336] Clear protocols are needed to ensure that targeting decisions balance the potential military advantage against the risk of civilian harm.[337] By establishing guidelines for the proportionality assessments of dual-use targets, states can minimize collateral damage while achieving their military

---

[328] Melzer, N. (2013). Human rights implications of the usage of drones and unmanned robots in warfare. In European Parliament's Subcommittee on Human Rights, *Policy Department DG External Policies* (p. PE 410.220 EN). European Union. https://doi.org/10.2861/213

[329] Schmitt, M. N. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press.

[330] Bannelier, K., & Christakis, T. (2017, February 25). *Cyber-Attacks – Prevention-Reactions: The role of states and private actors*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2941988

[331] Rejali, S., & Heiniger, Y. (2020). The role of digital technologies in humanitarian law, policy and action: Charting a path forward. *International Review of the Red Cross*, *102*(913), 1–22. doi:10.1017/S1816383121000114

[332] Clapham, Andrew, Human Rights Obligations of Non-State Actors in Conflict Situations (September 30, 2006). International Review of the Red Cross, Vol. 88, No. 863, pp. 491-523, 2006, Available at SSRN: https://ssrn.com/abstract=1338653

[333] Clapham, Andrew, Human Rights Obligations of Non-State Actors in Conflict Situations (September 30, 2006). International Review of the Red Cross, Vol. 88, No. 863, pp. 491-523, 2006, Available at SSRN: https://ssrn.com/abstract=1338653

[334] Schmitt, M. N. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press.

[335] International Committee of the Red Cross. (2015). International humanitarian law and the challenges of contemporary armed conflicts. In *32nd INTERNATIONAL CONFERENCE OF THE RED CROSS AND RED CRESCENT*. https://www.icrc.org/sites/default/files/document/file_list/32ic-report-on-ihl-and-challenges-of-armed-conflicts.pdf

[336] Hathaway, Oona & Crootof, Rebecca & Levitz, Philip & Nix, Haley & Nowlan, Aileen & Perdue, William & Spiegel, Julia. (2011). The Law of Cyber-Attack. California Law Review. 100.

[337] Bannelier, K., & Christakis, T. (2017, February 25). *Cyber-Attacks – Prevention-Reactions: The role of states and private actors*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2941988

objectives.[338] These protocols must also account for the cascading effects of cyber operations, ensuring that the broader impact on civilian systems is considered in decision-making processes.[339]

Expanding the definitions within IHL to explicitly include cyber-attacks as acts of war is another important step.[340] This expansion would bring cyber operations within the purview of existing legal provisions, ensuring that they are subject to the same standards of accountability and oversight as traditional forms of conflict.[341] Such definitional clarity would also facilitate the development of enforcement mechanisms tailored to the unique challenges of cyberspace.[342] By incorporating cyber-attacks into established legal frameworks, states can create a consistent and cohesive approach to regulating digital conflicts.[343]

Engaging non-state actors in the regulatory framework of IHL is equally essential.[344] Adapting IHL principles to govern the actions of these actors can help establish accountability mechanisms and deter malicious behaviour.[345] International oversight mechanisms for monitoring cyber operations and promoting adherence to IHL principles could further enhance accountability on a global scale and prevent violations.[346] These oversight mechanisms must be equipped with the resources and authority necessary to investigate and address violations effectively.[347]

Relevant Legal Instruments and Their Jurisdiction

The Tallinn Manual

---

[338] Geiss, R., & Lahmann, H. (2021b, May 22). *Protection of data in armed conflict*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3851136

[339] Brown, G.D. (2011). Why Iran Didn't Admit Stuxnet Was an Attack. Joint Force Quarterly, 63, 70-73.

[340] Rejali, S., & Heiniger, Y. (2020). The role of digital technologies in humanitarian law, policy and action: Charting a path forward. *International Review of the Red Cross*, *102*(913), 1–22. doi:10.1017/S1816383121000114

[341] Shackelford, S., Fort, T. L., & Prenkert, J. D. (2014). How businesses can promote Cyber Peace. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2393528

[342] International Committee of the Red Cross. (2015). International humanitarian law and the challenges of contemporary armed conflicts. In *32nd INTERNATIONAL CONFERENCE OF THE RED CROSS AND RED CRESCENT*. https://www.icrc.org/sites/default/files/document/file_list/32ic-report-on-ihl-and-challenges-of-armed-conflicts.pdf

[343] Hathaway, Oona & Crootof, Rebecca & Levitz, Philip & Nix, Haley & Nowlan, Aileen & Perdue, William & Spiegel, Julia. (2011). The Law of Cyber-Attack. California Law Review. 100.

[344] Shackelford, S., Fort, T. L., & Prenkert, J. D. (2014). How businesses can promote Cyber Peace. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2393528

[345] Clapham, Andrew, Human Rights Obligations of Non-State Actors in Conflict Situations (September 30, 2006). International Review of the Red Cross, Vol. 88, No. 863, pp. 491-523, 2006, Available at SSRN: https://ssrn.com/abstract=1338653

[346] Rejali, S., & Heiniger, Y. (2020). The role of digital technologies in humanitarian law, policy and action: Charting a path forward. *International Review of the Red Cross*, *102*(913), 1–22. doi:10.1017/S1816383121000114

[347] International Committee of the Red Cross. (2015). International humanitarian law and the challenges of contemporary armed conflicts. In *32nd INTERNATIONAL CONFERENCE OF THE RED CROSS AND RED CRESCENT*. https://www.icrc.org/sites/default/files/document/file_list/32ic-report-on-ihl-and-challenges-of-armed-conflicts.pdf

The Tallinn Manual represents one of the most ambitious efforts to apply IHL to the context of cyber operations. Developed by a group of military and legal experts, this manual provides a comprehensive analysis of how existing international laws can apply to cyber warfare.[348] While non-binding, it has become a key reference for states grappling with the complexities of digital conflict.[349]

The manual's strengths lie in its practical guidance for interpreting IHL in the context of cyber operations.[350] It addresses critical issues such as sovereignty, attribution, and state accountability, offering a framework for managing cyber conflicts.[351] Additionally, it promotes the adoption of best practices in cyber conflict management, encouraging states to align their actions with established norms.[352] Its ability to provide a detailed, scenario-based approach to cyber operations has made it a valuable tool for legal scholars and practitioners alike.[353]

However, the Tallinn Manual also has limitations. As a non-binding document, it lacks the enforceability of a treaty, reducing its practical impact.[354] Its scope is also limited, as it is based on the perspectives of a relatively small group of states, which may not fully represent the diversity of challenges faced by the international community.[355] Furthermore, the manual has been criticized for its accessibility to states without extensive cyber capabilities, potentially exacerbating inequalities between technologically advanced and less-developed nations. These limitations highlight the need for a more inclusive and universally accepted approach to regulating cyber conflicts.[356]

The Geneva Conventions

---

[348] Roscini, M., & Trust, L. (2014). *Cyber operations and the use of force in international law*. Oxford University Press, USA.

[349] Schmitt, M. N. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press.

[350] Hathaway, Oona & Crootof, Rebecca & Levitz, Philip & Nix, Haley & Nowlan, Aileen & Perdue, William & Spiegel, Julia. (2011). The Law of Cyber-Attack. California Law Review. 100.

[351] Bannelier, K., & Christakis, T. (2017, February 25). *Cyber-Attacks – Prevention-Reactions: The role of states and private actors*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2941988

[352] International Committee of the Red Cross. (2015). International humanitarian law and the challenges of contemporary armed conflicts. In *32nd INTERNATIONAL CONFERENCE OF THE RED CROSS AND RED CRESCENT*. https://www.icrc.org/sites/default/files/document/file_list/32ic-report-on-ihl-and-challenges-of-armed-conflicts.pdf

[353] Schmitt, M. N. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press.

[354] Shackelford, S., Fort, T. L., & Prenkert, J. D. (2014). How businesses can promote Cyber Peace. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2393528

[355] Rejali, S., & Heiniger, Y. (2020). The role of digital technologies in humanitarian law, policy and action: Charting a path forward. *International Review of the Red Cross*, *102*(913), 1–22. doi:10.1017/S1816383121000114

[356] Melzer, N. (2013). Human rights implications of the usage of drones and unmanned robots in warfare. In European Parliament's Subcommittee on Human Rights, *Policy Department DG External Policies* (p. PE 410.220 EN). European Union. https://doi.org/10.2861/213

The Geneva Conventions and their Additional Protocols form the foundation of IHL, emphasizing the protection of civilians and regulating conduct during armed conflict.[357] While their principles remain relevant, the cyber domain poses unique challenges to their application.[358]

The conventions set strong standards for the protection of civilians, providing a robust framework for regulating hostilities.[359] Their widespread international acceptance enhances their legitimacy and reach, making them a cornerstone of the international legal regime.[360] The Geneva Conventions' focus on minimizing harm to civilians and ensuring ethical conduct during warfare provides a solid foundation for adapting to new challenges.

However, the conventions were designed with physical warfare in mind, creating ambiguities in their applicability to non-physical attacks, such as cyber-attacks on critical infrastructure.[361] The cascading effects of cyber operations complicate the application of principles like proportionality and distinction, while the generalities of the conventions limit their utility in addressing the specific challenges of the cyber battlefield.[362] To address these limitations, additional protocols specific to cyber operations should be developed, clarifying how the principles of the Geneva Conventions apply to digital conflicts.[363]

United Nations Efforts

The United Nations has played a crucial role in promoting dialogue on the applicability of international law to cyberspace.[364] Initiatives such as the Group of Governmental Experts (GGE) and the Open-Ended Working Group (OEWG) aim to establish norms for state conduct and facilitate global cooperation in addressing cyber threats.[365]

---

[357] Schmitt, M. N. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press.

[358] International Committee of the Red Cross. (2015). International humanitarian law and the challenges of contemporary armed conflicts. In *32nd INTERNATIONAL CONFERENCE OF THE RED CROSS AND RED CRESCENT*. https://www.icrc.org/sites/default/files/document/file_list/32ic-report-on-ihl-and-challenges-of-armed-conflicts.pdf

[359] Hathaway, Oona & Crootof, Rebecca & Levitz, Philip & Nix, Haley & Nowlan, Aileen & Perdue, William & Spiegel, Julia. (2011). The Law of Cyber-Attack. California Law Review. 100.

[360] Bannelier, K., & Christakis, T. (2017, February 25). *Cyber-Attacks – Prevention-Reactions: The role of states and private actors*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2941988

[361] Shackelford, S., Fort, T. L., & Prenkert, J. D. (2014). How businesses can promote Cyber Peace. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2393528

[362] Rejali, S., & Heiniger, Y. (2020). The role of digital technologies in humanitarian law, policy and action: Charting a path forward. *International Review of the Red Cross*, *102*(913), 1–22. doi:10.1017/S1816383121000114

[363] Melzer, N. (2013). Human rights implications of the usage of drones and unmanned robots in warfare. In European Parliament's Subcommittee on Human Rights, *Policy Department DG External Policies* (p. PE 410.220 EN). European Union. https://doi.org/10.2861/213

[364] Roscini, M., & Trust, L. (2014). *Cyber operations and the use of force in international law*. Oxford University Press, USA.

[365] Schmitt, M. N. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press.

These efforts have accelerated multilateral dialogue and consensus-building on cyber norms, encouraging confidence-building measures to reduce the risk of conflict.[366] They also promote the adoption of voluntary guidelines for state behaviour in cyberspace, fostering a collaborative approach to managing cyber threats.[367] The UN's role in facilitating dialogue and fostering trust among states has been instrumental in laying the groundwork for more formalized agreements.[368]

However, progress has been slow due to divisions among states on complex issues such as sovereignty and the governance of dual-use technologies.[369] The non-binding nature of the recommendations further limits their enforceability and impact.[370] To overcome these challenges, the UN must work to build broader consensus among states and transition from voluntary guidelines to binding agreements that address the realities of the digital age.[371]

Expanding UN Efforts

To enhance the effectiveness of UN initiatives, binding agreements should be introduced to transition from voluntary guidelines to enforceable treaties.[372] Regional cooperation can also be leveraged to develop localized strategies for addressing cyber threats, complementing global efforts.[373] Encouraging private sector partnerships is another critical step, as technology companies play a pivotal role in shaping the digital landscape.[374]

The UN should also focus on fostering public-private partnerships to address gaps in cybersecurity capabilities, particularly in resource-constrained regions.[375] These partnerships can facilitate the sharing of expertise and resources, enhancing global resilience to cyber

---

[366] UN. Office of the High Commissioner for Human Rights. (2014, June 30). *The right to privacy in the digital age :: report of the Office of the United Nations High Commissioner for Human Rights*. United Nations Digital Library System. https://digitallibrary.un.org/record/777869?v=pdf

[367] Bannelier, K., & Christakis, T. (2017, February 25). *Cyber-Attacks – Prevention-Reactions: The role of states and private actors*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2941988

[368] Shackelford, S., Fort, T. L., & Prenkert, J. D. (2014). How businesses can promote Cyber Peace. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2393528

[369] Geiss, R., & Lahmann, H. (2021b, May 22). *Protection of data in armed conflict*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3851136

[370] Rejali, S., & Heiniger, Y. (2020). The role of digital technologies in humanitarian law, policy and action: Charting a path forward. *International Review of the Red Cross*, *102*(913), 1–22. doi:10.1017/S1816383121000114

[371] Henschke, A. (2020). Privacy, the Internet of Things and State Surveillance: Handling Personal Information within an Inhuman System. *Moral Philosophy and Politics*, *7*(1), 123-149. https://doi.org/10.1515/mopp-2019-0056

[372] Roscini, M., & Trust, L. (2014). *Cyber operations and the use of force in international law*. Oxford University Press, USA.

[373] Bannelier, K., & Christakis, T. (2017, February 25). *Cyber-Attacks – Prevention-Reactions: The role of states and private actors*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2941988

[374] Melzer, N. (2013). Human rights implications of the usage of drones and unmanned robots in warfare. In European Parliament's Subcommittee on Human Rights, *Policy Department DG External Policies* (p. PE 410.220 EN). European Union. https://doi.org/10.2861/213

[375] Henschke, A. (2020). Privacy, the Internet of Things and State Surveillance: Handling Personal Information within an Inhuman System. *Moral Philosophy and Politics*, *7*(1), 123-149. https://doi.org/10.1515/mopp-2019-0056

threats.[376] By engaging with a diverse range of stakeholders, the UN can create a more inclusive and comprehensive approach to managing cyber conflicts.[377]

International Human Rights Law on Treatment of Human Rights

International Human Rights Law (IHRL) complements IHL by addressing individual rights during both peace and conflict. In the context of digital warfare, IHRL is essential for protecting privacy, freedom of expression, and access to information.[378]

Cyber wars often involve extensive surveillance and data collection, raising concerns about privacy and ethical use.[379] IHRL mandates oversight and transparency in these activities to prevent abuse and ensure accountability.[380] Similarly, cyber operations that spread misinformation or restrict access to information undermine freedom of expression and democratic processes, violating fundamental human rights.[381]

To address these challenges, targeted protocols should be developed to protect digital rights, including privacy and freedom of expression.[382] Independent authorities should be established to oversee violations of digital rights, while global agreements should prioritize the protection of human rights in digital contexts.[383] These measures must be supported by robust enforcement mechanisms to ensure compliance and accountability.[384]

Emerging Norms and Proposals

The development of cyber-specific treaties is increasingly recognized as a necessity.[385] A legally binding international cybersecurity treaty could define acceptable and unacceptable behaviour in cyberspace, hold states accountable for securing civilian infrastructure, and

---

[376] Schmitt, M. N. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press.
[377] Bannelier, K., & Christakis, T. (2017, February 25). *Cyber-Attacks – Prevention-Reactions: The role of states and private actors*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2941988
[378] UN. Office of the High Commissioner for Human Rights. (2014, June 30). *The right to privacy in the digital age :: report of the Office of the United Nations High Commissioner for Human Rights*. United Nations Digital Library System. https://digitallibrary.un.org/record/777869?v=pdf
[379] Shackelford, S., Fort, T. L., & Prenkert, J. D. (2014). How businesses can promote Cyber Peace. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2393528
[380] Schmitt, M. N. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press.
[381] Bannelier, K., & Christakis, T. (2017, February 25). *Cyber-Attacks – Prevention-Reactions: The role of states and private actors*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2941988
[382] Henschke, A. (2020). Privacy, the Internet of Things and State Surveillance: Handling Personal Information within an Inhuman System. *Moral Philosophy and Politics*, *7*(1), 123-149. https://doi.org/10.1515/mopp-2019-0056
[383] UN. Office of the High Commissioner for Human Rights. (2014, June 30). *The right to privacy in the digital age :: report of the Office of the United Nations High Commissioner for Human Rights*. United Nations Digital Library System. https://digitallibrary.un.org/record/777869?v=pdf
[384] Schmitt, M. N. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press.
[385] Roscini, M., & Trust, L. (2014). *Cyber operations and the use of force in international law*. Oxford University Press, USA.

provide mechanisms for attribution and accountability.[386] Guidelines for the use of AI in warfare are also critical to ensure compliance with IHL and IHRL, incorporating principles of accountability, human oversight, and ethics.[387]

Conclusion

While IHL and IHRL provide valuable principles, their limitations in addressing the complexities of cyber warfare highlight the need for innovation and reform.[388] Cyber-specific treaties, improved attribution tools, and enhanced international collaboration are essential to prevent the escalation of digital conflicts and protect civilians, human rights, and global stability.[389] By strengthening existing legal frameworks and fostering global cooperation, the international community can build a more secure and equitable digital future.[390]

---

[386] Bannelier, K., & Christakis, T. (2017, February 25). *Cyber-Attacks – Prevention-Reactions: The role of states and private actors*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2941988

[387] Schmitt, M. N. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press.

[388] International Committee of the Red Cross. (2015). International humanitarian law and the challenges of contemporary armed conflicts. In *32nd INTERNATIONAL CONFERENCE OF THE RED CROSS AND RED CRESCENT*. https://www.icrc.org/sites/default/files/document/file_list/32ic-report-on-ihl-and-challenges-of-armed-conflicts.pdf

[389] Bannelier, K., & Christakis, T. (2017, February 25). *Cyber-Attacks – Prevention-Reactions: The role of states and private actors*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2941988

[390] Schmitt, M. N. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press.

VII. Recommendations

Strengthening Legal Frameworks to Combat Cyber Warfare International treaties made alongside must enshrine legally binding, explicit prohibitions on cyber-attacks against critical civilian infrastructure such as hospitals, power grids and water supplies, and include clear norms around state behaviour online.[391] These treaties could feature provisions prohibiting false flag operations and the use of dual-use technologies, and include mechanisms to hold non-state actors accountable.[392] Additionally, long-term solutions to the impacts of cyber-attacks, from restoring disrupted or destroyed critical systems to compensating affected populations, and periodic treaty reviews to adjust to new technological trends and threats, must be packaged together. These treaties need to also require cross-border discussions on investigating and resolving sophisticated cyber incidents between countries.[393]

International Humanitarian Law (IHL) is an area that must be overhauled to be up to date with the digital era.[394] Refinement of traditional tenets, like distinction, proportionality, and necessity, is needed to properly address the dual-use nature of cyber systems, which do not always allow for clear differentiation between civilian and military infrastructure.[395] Clear and comprehensive rules and regulations need to be developed to ensure the ethical and legal use of cyber weapons, focusing on protecting civilians and limiting collateral damage. Updating these revisions would also involve including specific clauses related to artificial intelligence (AI) and autonomous systems that ensure that deployment is governed by ethical principles.[396] In addition, institutionalization of compliance monitoring mechanisms is required to ensure transparency and compliance with these revised norms. Resources must be set aside to train military personnel in the specifics of digital conflict, in order to further entrench the application of IHL in practice. Also included among these resources should be the funding of simulations and scenarios that familiarize actors with the contingencies of computer-based conflict.[397]

---

[391] Roscini, M., & Trust, L. (2014). *Cyber operations and the use of force in international law*. Oxford University Press, USA.

[392] Schmitt, M. N. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press.

[393] International Committee of the Red Cross. (2015). International humanitarian law and the challenges of contemporary armed conflicts. In *32nd INTERNATIONAL CONFERENCE OF THE RED CROSS AND RED CRESCENT*. https://www.icrc.org/sites/default/files/document/file_list/32ic-report-on-ihl-and-challenges-of-armed-conflicts.pdf

[394] Hathaway, Oona & Crootof, Rebecca & Levitz, Philip & Nix, Haley & Nowlan, Aileen & Perdue, William & Spiegel, Julia. (2011). The Law of Cyber-Attack. California Law Review. 100.

[395] Geiss, R., & Lahmann, H. (2021b, May 22). *Protection of data in armed conflict*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3851136

[396] Bannelier, K., & Christakis, T. (2017, February 25). *Cyber-Attacks – Prevention-Reactions: The role of states and private actors*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2941988

[397] Melzer, N. (2013). Human rights implications of the usage of drones and unmanned robots in warfare. In European Parliament's Subcommittee on Human Rights, *Policy Department DG External Policies* (p. PE 410.220 EN). European Union. https://doi.org/10.2861/213

Such measures are necessary to assure proper accountability of cyberspace and its behaviour. International bodies like the International Criminal Court should have jurisdiction over cyber violations.[398] International covenants should make the fixing of cybercriminals possible and ensure that the ill-intentioned people act properly, even if it is in another country.[399] Designating the resolution of cyber disputes to independent arbitration panels can create a neutral party for the mediation of such disputes, promoting timely resolutions and including provisions for restitution for victims to aid in post-attack recovery of those affected and rebuilding of their community. International cyber tribunals could also fill that role. Tribunals like these could also set a precedent for combating new wars emerging from technological development.[400]

Robust attribution mechanisms are essential to dissuading adversarial use and holding actors to account.[401] State and private sector collaboration on developing new technology that can reach a high level of accuracy in identifying where a cyber-attack originated.[402] The utilization of blockchain technologies and AI-enhanced forensic tools hold promise for improving the reliability and accuracy of attribution efforts.[403] Global repositories for cyber-attack data will provide a means to learn from each other and improve methodologies. Quantum-resistant cryptographic systems will also be shielded by investment to secure the future of attribution.[404] In addition, attribution endeavours should incorporate public reporting both to maximize transparency and, where appropriate, to encourage confidence in the findings. Such transparent reports could also incentivise greater collective accountability, as well as significantly strengthen global trust.[405]

Particularly, international partnership is crucial to address attribution difficulties. We need a globally recognized cyber-attribution body to investigate major incidents and publish impartial findings. It is future-proof and fits well with any international strategy at the

---

[398] UN. Office of the High Commissioner for Human Rights. (2014, June 30). *The right to privacy in the digital age :: report of the Office of the United Nations High Commissioner for Human Rights*. United Nations Digital Library System. https://digitallibrary.un.org/record/777869?v=pdf

[399] Rejali, S., & Heiniger, Y. (2020). The role of digital technologies in humanitarian law, policy and action: Charting a path forward. *International Review of the Red Cross*, *102*(913), 1–22. doi:10.1017/S1816383121000114

[400] UN. Office of the High Commissioner for Human Rights. (2014, June 30). *The right to privacy in the digital age :: report of the Office of the United Nations High Commissioner for Human Rights*. United Nations Digital Library System. https://digitallibrary.un.org/record/777869?v=pdf

[401] Roscini, M., & Trust, L. (2014). *Cyber operations and the use of force in international law*. Oxford University Press, USA.

[402] Schmitt, M. N. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press.

[403] Melzer, N. (2013). Human rights implications of the usage of drones and unmanned robots in warfare. In European Parliament's Subcommittee on Human Rights, *Policy Department DG External Policies* (p. PE 410.220 EN). European Union. https://doi.org/10.2861/213

[404] Shackelford, S., Fort, T. L., & Prenkert, J. D. (2014). How businesses can promote Cyber Peace. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2393528

[405] Bannelier, K., & Christakis, T. (2017, February 25). *Cyber-Attacks – Prevention-Reactions: The role of states and private actors*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2941988

attribution level, which needs to be conducted in the utmost transparency so that states trust each other sufficiently to prevent retaliatory blunders.[406] Conduct joint multinational cyber simulations and drills to test and refine coordination of response and attribution frameworks; Improved coordination in between governments and industry actors — both at the local national and global, working collectively to defend critical infrastructure at scale[407] — will be pivotal; having standardized protocols to exchange real-time information on cyber threats will allow for responses to take place at speed and scale vs point solutions that would have a marginal effect.[408] Protocol requiring before such responses must also be based on neighbourhood adaptation protocols at local vulnerabilities addressing global response so that local response protocols remain inclusive and taken in a regional/global context.[409]

Accountability for all state & non-state actors is essential for preserving the rule of law in cyberspace. States should be responsible for allowing or failing to prevent cyber operations in their territory, whether by agents of the state or by proxies.[410] There need to be substantive penalties on such states that fail to address cybercriminal actions based in their countries. International trade deals should include cyber accountability clauses to motivate compliance, and states should issue annual disclosures outlining their adherence to agreed norms and their efforts to mitigate cyber risks.[411] Over this, these disclosures have to be backed by independent audits to confirm their veracity and build credibility to reinforce trust in the mechanism of the international community.[412]

All attacks that impact states or social stability must have mechanisms to hold them accountable under laws materialized in international treaties to combat digital aggression.[413] Ethical responsibilities should also be cast into the regulatory frameworks that ought to bring technology companies within the scope of obligations designed to let the technology sector avoid complicity in the realm of digital war.[414] Well-recognized worldwide certification

---

[406] Schmitt, M. N. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press.
[407] UN. Office of the High Commissioner for Human Rights. (2014, June 30). *The right to privacy in the digital age :: report of the Office of the United Nations High Commissioner for Human Rights*. United Nations Digital Library System. https://digitallibrary.un.org/record/777869?v=pdf
[408] Geiss, R., & Lahmann, H. (2021b, May 22). *Protection of data in armed conflict*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3851136
[409] Bannelier, K., & Christakis, T. (2017, February 25). *Cyber-Attacks – Prevention-Reactions: The role of states and private actors*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2941988
[410] Schmitt, M. N. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press.
[411] UN. Office of the High Commissioner for Human Rights. (2014, June 30). *The right to privacy in the digital age :: report of the Office of the United Nations High Commissioner for Human Rights*. United Nations Digital Library System. https://digitallibrary.un.org/record/777869?v=pdf
[412] Rejali, S., & Heiniger, Y. (2020). The role of digital technologies in humanitarian law, policy and action: Charting a path forward. *International Review of the Red Cross*, *102*(913), 1–22. doi:10.1017/S1816383121000114
[413] Schmitt, M. N. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press.
[414] Taddeo, M., Floridi, L., Taddeo, M., & Floridi, L. (Eds.). (2017). The responsibilities of online service providers. In Institute of Law and Technology, UAB, Spain & University of Bologna (Faculty of Law-CIRSFID) and European University Institute of Florence, Italy, *Law, Governance and Technology Series* (Vol. 31). https://doi.org/10.1007/978-3-319-47852-4.

systems for the cybersecurity enterprises can define layers of practices and would facilitate accountability, whereas; harmonised legal frameworks, crossing borders, will ensure similar prosecution of the cyber offences, involving non-state actors.[415] Particularly on developing mechanisms for combating the use of cyber tools by terrorist organizations and other extreme organisms. Strengthening accountability and transparency of cyber tools through civil society partnerships can help counter the abuse of vulnerable demographics.[416]

While it is important to promote the development of new technologies, it is equally important to implement suitable regulations to prevent their abuse. International legal and ethical standards should be developed into global imperatives for the responsible design and application of AI-enabled systems and autonomous weapons.[417] This means that there should be always human presence or human oversight in combat when using autonomous systems to ensure compliance with humanitarian principles.[418] It is imperative to focus on explaining AI models to bridge gaps in accountability and build public trust in decision-making based on these algorithms. This will allow compliance with global standards to be coupled with international registries for the monitoring of the deployment of autonomous systems.[419] The registries need to contain thorough technical descriptions to provide for system being deployed that follows internationally accepted safety protocols. In addition, the evolving risks and technological advancements could also be catered to through an annual review mechanism for the registries.[420]

Funding research and development will be crucial for strengthening defence cybersecurity capabilities. The development of resilient infrastructure and advanced threat detection capabilities should be prioritized.[421] Collaborative efforts among academia, industry, and governments can accelerate cybersecurity advancements, while international funds supporting innovation in resource-constrained settings will promote global equity in technological development. Encouraging ethical practices within the private sector is equally important.[422] Technology firms should adopt voluntary codes of conduct aligned with

---

[415] Clapham, Andrew, Human Rights Obligations of Non-State Actors in Conflict Situations (September 30, 2006). International Review of the Red Cross, Vol. 88, No. 863, pp. 491-523, 2006, Available at SSRN: https://ssrn.com/abstract=1338653

[416] Rejali, S., & Heiniger, Y. (2020). The role of digital technologies in humanitarian law, policy and action: Charting a path forward. *International Review of the Red Cross*, *102*(913), 1–22. doi:10.1017/S1816383121000114

[417] UN. Office of the High Commissioner for Human Rights. (2014, June 30). *The right to privacy in the digital age :: report of the Office of the United Nations High Commissioner for Human Rights*. United Nations Digital Library System. https://digitallibrary.un.org/record/777869?v=pdf

[418] Geiss, R., & Lahmann, H. (2021b, May 22). *Protection of data in armed conflict*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3851136

[419] Winter, E. (2020). THE COMPATIBILITY OF AUTONOMOUS WEAPONS WITH THE PRINCIPLE OF DISTINCTION IN THE LAW OF ARMED CONFLICT. *International and Comparative Law Quarterly*, *69*(4), 845–876. doi:10.1017/S0020589320000378

[420] Ohlin, J.D. (2016). The Combatant's Stance: Autonomous Weapons on the Battlefield. *International law studies, 92*, 1.

[421] Shackelford, S., Fort, T. L., & Prenkert, J. D. (2014). How businesses can promote Cyber Peace. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2393528

[422] Amnesty International. (2019). SURVEILLANCE GIANTS: HOW THE BUSINESS MODEL OF GOOGLE AND FACEBOOK THREATENS HUMAN RIGHTS. In *Amnesty International*.

international norms, supported by fiscal incentives for companies that prioritize robust cybersecurity measures.[423] Public recognition programs for corporations demonstrating exemplary ethical practices will further reinforce these efforts. Dedicated global awards for ethical innovation could motivate broader adherence to responsible practices in the technology sector. Moreover, public-private partnerships should work on educational programs for emerging cybersecurity professionals to meet growing industry demands.[424]

Multilateral cooperation is a cornerstone for addressing the challenges of cyber warfare. Global institutions such as NATO and the United Nations should expand their mandates to include the multifaceted challenges posed by cyber threats.[425] Specialized divisions within these organizations can mediate conflicts and coordinate international responses. Establishing a cybersecurity council to oversee adherence to norms and recommend targeted measures against violators will strengthen global governance.[426] Introducing "cyber peacekeeping" units to mediate post-conflict recovery and de-escalate cyber disputes represents another innovative approach. These peacekeeping units could also serve as an intermediary to assist states in building their defensive capabilities and enhancing mutual understanding between conflicting parties in digital conflicts.[427]

Regional collaborations must also address localized cyber threats and optimize resource-sharing arrangements. These efforts should align with global frameworks to ensure consistency and effectiveness in governance and responses.[428] Standardized protocols for cross-border cyber incident responses will streamline cooperation during crises, while periodic regional summits will facilitate the evaluation of cybersecurity initiatives and refinement of strategies. Public-private partnerships are indispensable for leveraging expertise and resources to combat cyber threats effectively.[429] Governments, academic institutions, and the private sector should jointly develop and enforce cybersecurity standards. Task forces addressing specific challenges, such as ransomware or supply chain vulnerabilities, can utilize interdisciplinary expertise to maximize impact.[430] Regional partnerships must also focus on the unique vulnerabilities posed by emerging technologies

---

[423] Zwitter, A. (2014). Big Data ethics. Big Data & Society, 1(2). https://doi.org/10.1177/2053951714559253
[424] Shackelford, S., Fort, T. L., & Prenkert, J. D. (2014). How businesses can promote Cyber Peace. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2393528
[425] Schmitt, M. N. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press.
[426] International Committee of the Red Cross. (2015). International humanitarian law and the challenges of contemporary armed conflicts. In *32nd INTERNATIONAL CONFERENCE OF THE RED CROSS AND RED CRESCENT*. https://www.icrc.org/sites/default/files/document/file_list/32ic-report-on-ihl-and-challenges-of-armed-conflicts.pdf
[427] Bannelier, K., & Christakis, T. (2017, February 25). *Cyber-Attacks – Prevention-Reactions: The role of states and private actors*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2941988
[428] UN. Office of the High Commissioner for Human Rights. (2014, June 30). *The right to privacy in the digital age :: report of the Office of the United Nations High Commissioner for Human Rights*. United Nations Digital Library System. https://digitallibrary.un.org/record/777869?v=pdf
[429] Geiss, R., & Lahmann, H. (2021b, May 22). *Protection of data in armed conflict*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3851136
[430] Rejali, S., & Heiniger, Y. (2020). The role of digital technologies in humanitarian law, policy and action: Charting a path forward. *International Review of the Red Cross*, *102*(913), 1–22. doi:10.1017/S1816383121000114

and how they interact with existing infrastructure.[431] Collaborative action should extend to fostering relationships between developed and developing regions to share cybersecurity innovations equitably.[432]

Public awareness and education are integral to building resilient societies capable of withstanding cyber threats. Comprehensive media literacy campaigns should educate the public on identifying and mitigating misinformation and cyber risks.[433] Critical thinking skills must be promoted to reduce susceptibility to online manipulation. Partnerships with digital platforms can disseminate accessible and regionally tailored educational content. Expanding professional training programs will bridge workforce gaps in cybersecurity expertise, while interdisciplinary curricula in higher education should embed cybersecurity and ethical considerations to prepare future professionals.[434] Community engagement initiatives must empower grassroots organizations to enhance local cybersecurity literacy and ensure that vulnerable populations have access to resources for navigating cyber threats. These efforts should include the establishment of local cybersecurity resource centres offering training and tools for underserved communities, creating a more inclusive digital landscape.[435]

These recommendations provide a comprehensive framework for addressing the dynamic challenges of digital warfare.[436] They emphasize the importance of legal reforms, technological innovation, and collaborative efforts to safeguard human rights, uphold humanitarian principles, and foster global stability in the digital age.[437] Sustained commitment from states, international organizations, private corporations, and civil society is essential for navigating the complexities of cyber warfare. Through unified efforts and shared accountability, the international community can build a resilient, equitable, and ethically governed digital environment for future generations.[438] By prioritizing a forward-thinking

---

[431] UN. Office of the High Commissioner for Human Rights. (2014, June 30). *The right to privacy in the digital age :: report of the Office of the United Nations High Commissioner for Human Rights*. United Nations Digital Library System. https://digitallibrary.un.org/record/777869?v=pdf

[432] Bannelier, K., & Christakis, T. (2017, February 25). *Cyber-Attacks – Prevention-Reactions: The role of states and private actors*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2941988

[433] Melzer, N. (2013). Human rights implications of the usage of drones and unmanned robots in warfare. In European Parliament's Subcommittee on Human Rights, *Policy Department DG External Policies* (p. PE 410.220 EN). European Union. https://doi.org/10.2861/213

[434] Geiss, R., & Lahmann, H. (2021b, May 22). *Protection of data in armed conflict*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3851136

[435] Schmitt, M. N. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press.

[436] UN. Office of the High Commissioner for Human Rights. (2014, June 30). *The right to privacy in the digital age :: report of the Office of the United Nations High Commissioner for Human Rights*. United Nations Digital Library System. https://digitallibrary.un.org/record/777869?v=pdf

[437] Schmitt, M. N. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press.

[438] Bannelier, K., & Christakis, T. (2017, February 25). *Cyber-Attacks – Prevention-Reactions: The role of states and private actors*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2941988

approach, these measures can ensure that digital technologies are harnessed for constructive purposes while minimizing their potential for harm.[439]

[439] Rejali, S., & Heiniger, Y. (2020). The role of digital technologies in humanitarian law, policy and action: Charting a path forward. *International Review of the Red Cross*, *102*(913), 1–22. doi:10.1017/S1816383121000114

VIII. Conclusion

Summary of Key Findings

Through the lens of digital warfare, this thesis has explored the impact of the postmodern era on human rights and humanitarian law in the 21st-century digital phenomenon. It has highlighted dire implications and challenges, resulting in key takeaways that should be prioritized now and acted on hereafter:

1. **Human Rights Implications**: Digital warfare has increased risks to individual privacy and the right to seek, receive and impart information. Misinformation campaigns against democratic structures have not just stifled civil liberties, but have also deepened societal polarization and hit state legitimacy.[440] This erosion necessitates urgent policy responses designed to protect civil freedoms while addressing the technological threats that threaten them.[441] If unchecked, such threats threaten to enshrine a norm in which individual rights are surrendered for fabricated claims of security. Additionally, these threats are further widening the gap between technologically rich and underdeveloped nations, deepening global disparities.[442]

2. **Challenges to Humanitarian Law**: The most basic principles of International Humanitarian Law (IHL)—distinction, proportionality, and necessity—face unprecedented tests in the age of digital warfare.[443] compliance with these principles is complicated by the integrated nature of civilian and military systems, while the pseudonymous nature of cyber operations presents formidable obstacles to accountability.[444] These challenges highlight the need for IHL to evolve, adopting new protocols that address the unique nature of cyber conflict while ensuring the protection of civilians remains a priority. Efforts must also focus on enhancing the training of military and legal practitioners to better navigate the complex intersections of traditional IHL and digital applications.[445]

---

[440] Kernighan, B. W. (2021). *Understanding the digital world: What You Need to Know about Computers, the Internet, Privacy, and Security, Second Edition*. Princeton University Press.
[441] Henschke, A. (2020). Privacy, the Internet of Things and State Surveillance: Handling Personal Information within an Inhuman System. *Moral Philosophy and Politics*, *7*(1), 123-149. https://doi.org/10.1515/mopp-2019-0056
[442] Geiss, R., & Lahmann, H. (2021b, May 22). *Protection of data in armed conflict*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3851136
[443] Hathaway, Oona & Crootof, Rebecca & Levitz, Philip & Nix, Haley & Nowlan, Aileen & Perdue, William & Spiegel, Julia. (2011). The Law of Cyber-Attack. California Law Review. 100.
[444] Bannelier, K., & Christakis, T. (2017, February 25). *Cyber-Attacks – Prevention-Reactions: The role of states and private actors*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2941988
[445] Melzer, N. (2013). Human rights implications of the usage of drones and unmanned robots in warfare. In European Parliament's Subcommittee on Human Rights, *Policy Department DG External Policies* (p. PE 410.220 EN). European Union. https://doi.org/10.2861/213

3. **Revealing Case Studies**: High-profile incidents like Stuxnet, NotPetya, and Russian cyber operations in Ukraine have exposed the fragility of critical infrastructure and the potential for indiscriminate use of cyber tools.[446] These cases illuminate the devastating consequences of unregulated cyber operations and highlight the urgent need for robust technical and legal responses.[447] The lessons they provide can form a basis for the development of frameworks to mitigate future risks and prevent the misuse of digital tools. They also stress the importance of resilience in national and international infrastructure, requiring proactive measures to protect essential systems.[448]

4. **Legal Gaps**: Significant updates to both IHL and International Human Rights Law (IHRL) need to be implemented in order to address the challenges created by digital warfare. The absence of enforceable international treaties regulating cyber operations creates a void in accountability and oversight.[449] This gap in the regulations not only hampers justice for victims but also emboldens actors to exploit these weaknesses, perpetuating a dangerous cycle of harm and impunity.[450] Legal reforms must address these deficiencies to ensure a more accountable and just framework. This also includes the establishment of cross-border agreements that bridge the gaps in cyber laws and enhance enforcement capabilities across jurisdictions.[451]

5. **Evolving Imperatives**: The ongoing war in Ukraine has highlighted the urgent need for new treaties and ethical frameworks addressing these emerging technologies, including AI-powered systems.[452] Enhanced mechanisms for attribution are essential for the deterrence of conflict, the promotion of accountability, and the advancement of international stability. These steps are essential to developing a cohesive global strategy that addresses the multifaceted threats posed by digital warfare. Additionally, greater emphasis must be placed on public-private partnerships to leverage technological innovation for defensive and preventative measures.[453]

---

[446] Greenberg, A., & Excerpt. (2018, August 22). The untold story of NotPetya, the most devastating cyberattack in history. *WIRED*. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

[447] Schmitt, M. N. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press.

[448] Brown, G.D. (2011). Why Iran Didn't Admit Stuxnet Was an Attack. Joint Force Quarterly, 63, 70-73.

[449] UN. Office of the High Commissioner for Human Rights. (2014, June 30). *The right to privacy in the digital age :: report of the Office of the United Nations High Commissioner for Human Rights*. United Nations Digital Library System. https://digitallibrary.un.org/record/777869?v=pdf

[450] International Committee of the Red Cross. (2015). International humanitarian law and the challenges of contemporary armed conflicts. In *32nd INTERNATIONAL CONFERENCE OF THE RED CROSS AND RED CRESCENT*. https://www.icrc.org/sites/default/files/document/file_list/32ic-report-on-ihl-and-challenges-of-armed-conflicts.pdf

[451] International Committee of the Red Cross (ICRC). Autonomous Weapon Systems: Technical, Military, Legal, and Humanitarian Aspects. ICRC, 2016.

[452] Schmitt, M. N. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press.

[453] Geiss, R., & Lahmann, H. (2021b, May 22). *Protection of data in armed conflict*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3851136

Final Reflections

Digital warfare marks a monumental change in the nature of conflict and warfare, challenging established norms of engagement and the legal frameworks that govern warfare. Its borderless execution, rapid escalation, and disproportionate impacts compared to traditional forms of conflict require urgent legal, ethical, and technological adaptations.[454] This new form of warfare introduces complex ethical considerations that require immediate attention to ensure the responsible use of technology in both military and civilian contexts.[455]

The implications of digital warfare go beyond state actors, affecting civilians, private organizations, and international institutions. The international community must take decisive actions to mitigate risks, protect the most vulnerable, and shape a future where security and human dignity are a priority. The following actions are particularly critical:

1. **Enhancing Legal Protections**: Both IHL and IHRL must explicitly address the realities of cyber operations. Specific protocols need to safeguard civilian infrastructure, establish accountability for violations, and maintain ethical principles in digital warfare.[456] These legal protections should include robust mechanisms for monitoring compliance and enforcing accountability, as well as provisions for victim restitution and rehabilitation.[457] Such efforts should also consider the long-term social and economic repercussions of cyber-attacks, ensuring comprehensive recovery measures are in place. Policymakers should also incorporate adaptive strategies to regularly update these protocols as technological landscapes change.[458]
2. **Strengthening Global Collaboration**: International cooperation is vital to establishing unified standards, exchanging critical intelligence, and creating joint reactions to cyber incursions.[459] Collaborative frameworks will enable states to mitigate threats more effectively and respond to incidents with quickness and precision. Multilateral agreements should also prioritize equitable resource-sharing and capacity-building, ensuring that all nations, regardless of their technological advancement, can participate in and benefit from global cybersecurity efforts.[460] Expanding such collaborations to include non-state actors, such as multinational

---

[454] Schmitt, M. N. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press.

[455] Roscini, M., & Trust, L. (2014). *Cyber operations and the use of force in international law*. Oxford University Press, USA.

[456] Hathaway, Oona & Crootof, Rebecca & Levitz, Philip & Nix, Haley & Nowlan, Aileen & Perdue, William & Spiegel, Julia. (2011). The Law of Cyber-Attack. California Law Review. 100.

[457] UN. Office of the High Commissioner for Human Rights. (2014, June 30). *The right to privacy in the digital age :: report of the Office of the United Nations High Commissioner for Human Rights*. United Nations Digital Library System. https://digitallibrary.un.org/record/777869?v=pdf

[458] Geiss, R., & Lahmann, H. (2021b, May 22). *Protection of data in armed conflict*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3851136

[459] Bannelier, K., & Christakis, T. (2017, February 25). *Cyber-Attacks – Prevention-Reactions: The role of states and private actors*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2941988

[460] Shackelford, S., Fort, T. L., & Prenkert, J. D. (2014). How businesses can promote Cyber Peace. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2393528

corporations and academic institutions, can further enhance the scope and depth of these efforts.[461]

3. **Restoring Accountability**: Strong systems of attribution and accountability are essential to the deterrence of malicious actors. New forensic technologies, in combination with international cooperation, can ensure the identification and prosecution of perpetrators under international law.[462] Transparent processes are essential to cultivating trust and fairness in the application of justice. Establishing specialized international cyber tribunals could provide a dedicated venue for addressing violations and reinforcing global norms. These tribunals should also include mechanisms to address the involvement of non-state actors and their role in perpetuating cyber conflicts. Furthermore, public reporting on the outcomes of such tribunals can serve as a deterrent and a means of building public trust in the system.[463]
4. **Protecting Rights While Doing So**: Efforts to counter cyber threats must align with fundamental human rights and values, including the principles of transparency, proportionality, and fairness.[464] Policymakers should ensure the careful calibration of security strategies to avoid infringing on the liberties they aim to protect. This balance is essential to maintain public trust and ensure that cybersecurity measures do not exacerbate existing inequalities or injustices.[465] Greater emphasis on participatory policymaking, where affected communities are involved in shaping cybersecurity laws, can help ensure that rights are respected. These participatory approaches must be inclusive, ensuring representation from marginalized and vulnerable populations to address their unique challenges.[466]

Call to Action

The international community stands at a critical juncture in its response to the threats created by digital warfare. The decisions taken today will influence the trajectory of future conflicts and their consequences for global stability.[467] Policymakers, technologists, legal experts, and

---

[461] Rejali, S., & Heiniger, Y. (2020). The role of digital technologies in humanitarian law, policy and action: Charting a path forward. *International Review of the Red Cross*, *102*(913), 1–22. doi:10.1017/S1816383121000114

[462] Schmitt, M. N. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press.

[463] UN. Office of the High Commissioner for Human Rights. (2014, June 30). *The right to privacy in the digital age :: report of the Office of the United Nations High Commissioner for Human Rights*. United Nations Digital Library System. https://digitallibrary.un.org/record/777869?v=pdf

[464] Geiss, R., & Lahmann, H. (2021b, May 22). *Protection of data in armed conflict*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3851136

[465] Bannelier, K., & Christakis, T. (2017, February 25). *Cyber-Attacks – Prevention-Reactions: The role of states and private actors*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2941988

[466] Melzer, N. (2013). Human rights implications of the usage of drones and unmanned robots in warfare. In European Parliament's Subcommittee on Human Rights, *Policy Department DG External Policies* (p. PE 410.220 EN). European Union. https://doi.org/10.2861/213

[467] Roscini, M., & Trust, L. (2014). *Cyber operations and the use of force in international law*. Oxford University Press, USA.

the civil society should collaborate and cooperate in the development of innovative solutions that prioritize peace, security, and the dignity of individuals.[468] This collaborative effort demands a forward-looking approach that anticipates the changing nature of threats and ensures the continued relevance and efficacy of international law.

Harnessing the potential of digital technologies while minimizing their risks requires a coordinated and proactive global response.[469] Key areas of focus include advancing public awareness and education, fostering inclusive dialogues on the ethical use of technology, and investing in research and development to build resilient systems. Establishing global norms that integrate ethical considerations into technological innovation will be critical to achieving these goals.[470] These norms must be supported by consistent enforcement mechanisms and transparent evaluation processes. Additionally, fostering a culture of accountability within the private sector through corporate governance reforms and incentivizing ethical practices can further reinforce global efforts.[471]

As we navigate an era of unprecedented change, the importance of solidarity, awareness, and moral responsibility has never been greater. By taking decisive and coordinated action, the global community can ensure that technological advancements serve as tools for progress rather than instruments of harm.[472] Together, we can create a future where security, equity, and human dignity are upheld, even in the face of evolving challenges.[473]

This moment calls for visionary leadership and collective resolve. It is only through unity and a shared commitment to ethical governance that we can address the complexities of digital warfare and ensure a safer, more just world for generations to come.[474] To secure this vision, continuous engagement, adaptive policymaking, and shared innovation must remain at the forefront of international efforts.[475]

---

[468] Schmitt, M. N. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press.
[469] UN. Office of the High Commissioner for Human Rights. (2014, June 30). *The right to privacy in the digital age :: report of the Office of the United Nations High Commissioner for Human Rights*. United Nations Digital Library System. https://digitallibrary.un.org/record/777869?v=pdf
[470] Geiss, R., & Lahmann, H. (2021b, May 22). *Protection of data in armed conflict*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3851136
[471] UN. Office of the High Commissioner for Human Rights. (2014, June 30). *The right to privacy in the digital age :: report of the Office of the United Nations High Commissioner for Human Rights*. United Nations Digital Library System. https://digitallibrary.un.org/record/777869?v=pdf
[472] Schmitt, M. N. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press.
[473] Hathaway, Oona & Crootof, Rebecca & Levitz, Philip & Nix, Haley & Nowlan, Aileen & Perdue, William & Spiegel, Julia. (2011). The Law of Cyber-Attack. California Law Review. 100.
[474] Bannelier, K., & Christakis, T. (2017, February 25). *Cyber-Attacks – Prevention-Reactions: The role of states and private actors*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2941988
[475] UN. Office of the High Commissioner for Human Rights. (2014, June 30). *The right to privacy in the digital age :: report of the Office of the United Nations High Commissioner for Human Rights*. United Nations Digital Library System. https://digitallibrary.un.org/record/777869?v=pdf

ANNEX

AI tools were used for the search of source material as well as the creation of summaries from the source material, which were then adapted to the text of this thesis.

IX. BIBLIOGRAPHY

Books

1. Schmitt, Michael N. (ed.). Tallinn Manual on the International Law Applicable to Cyber Warfare. Cambridge University Press, 2013.

2. Roscini, M., & Trust, L. (2014). *Cyber operations and the use of force in international law*. Oxford University Press, USA.

3. Singer, P. W., and Allan Friedman. Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford University Press, 2014.

4. Akhgar, Babak, et al. Application of Big Data for National Security: A Practitioner's Guide to Emerging Technologies. Butterworth-Heinemann, 2015.

5. Anderson, Kenneth. Law and Ethics for Autonomous Weapon Systems: Why a Ban Won't Work and How the Laws of War Can. Harvard University, 2013.

6. Kernighan, B. W. (2021). *Understanding the digital world: What You Need to Know about Computers, the Internet, Privacy, and Security, Second Edition*. Princeton University Press.

7. Chesterman, Simon. One Nation Under Surveillance: A New Social Contract to Defend Freedom Without Sacrificing Liberty. Oxford University Press, 2011.

8. Zwitter, Andrej. Big Data Ethics: Theoretical and Practical Perspectives. Springer, 2014.

9. Friedewald, M., Burgess, J. P., Cas, J., & Bellanova, R. (2020). *Surveillance, privacy and security: Citizens Perspectives*. Routledge.

10. Rid, Thomas. Cyber War Will Not Take Place. Oxford University Press, 2013.

11. Nye, Joseph S. The Future of Power. PublicAffairs, 2011.

12. Macnish, K. (2017). The Ethics of Surveillance: An Introduction (1st ed.). Routledge. https://doi.org/10.4324/9781315162867

13. Taddeo, Mariarosaria, and Luciano Floridi (Eds.). The Responsibilities of Online Service Providers. Springer, 2017.

14. Walzer, Michael. Just and Unjust Wars: A Moral Argument with Historical Illustrations. Basic Books, 2006.

15. Henschke, Adam. Ethics in an Age of Surveillance: Personal Information and Virtual Identities. Cambridge University Press, 2017.

16. Choudhury, B., & Petrin, M. (2019). *Corporate duties to the public*. Cambridge University Press.

17. Geiss, R., & Lahmann, H. (2021, May 22). *Protection of data in armed conflict*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3851136

18. Henschke, A. (2020). Privacy, the Internet of Things and State Surveillance: Handling Personal Information within an Inhuman System. *Moral Philosophy and Politics*, *7*(1), 123-149. https://doi.org/10.1515/mopp-2019-0056

19. Ventre, D. (2012b). *Cyber conflict: Competing National Perspectives*. Wiley-ISTE.

Articles

1. Clapham, Andrew. "Human Rights Obligations of Non-State Actors in Conflict Situations." International Review of the Red Cross, vol. 88, no. 863, 2006, pp. 491-523.

2. Schmitt, M. N. (2011). Cyber operations and the jus ad bellum revisited. *Vill. L. Rev.*, *56*, 569.

3. Corn, G. S. (2014b). Autonomous weapon systems: legal consequences of taking the man out of the LOOPP. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2450640

4. Brown, G. (2011, October 1). *Why Iran didn't admit Stuxnet was an attack.* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2485181

5. Deeks, A. (2014, September 1). *An international legal framework for surveillance*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2490700

6. Shackelford, S., Fort, T. L., & Prenkert, J. D. (2014b). How businesses can promote Cyber Peace. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2393528

7. Lin, H. (2012). Cyber conflict and international humanitarian law. In National Research Council (Ed.), *Volume 94 Number 886* [Journal-article]. https://doi.org/10.1017/S1816383112000811

8. Schmitt, M. (2012). Classification of cyber conflict. *Journal of Conflict and Security Law*, *17*(2), 245–260. https://doi.org/10.1093/jcsl/krs018

9. Eric Talbot Jensen, *Cyber Sovereignty: The Way Ahead*, 50 Tex. Int'l L. J. 275 (2014).

10. Bannelier, K., & Christakis, T. (2017, February 25). *Cyber-Attacks – Prevention-Reactions: The role of states and private actors*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2941988.

11. Brenner, S. W. (2011b). Cyber-Threats and the limits of bureaucratic control. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.1950725

12. Ohlin, J. D. (2016). The combatant's stance: autonomous weapons on the battlefield. *International Law Studies*, *92*, 1.

13. Rejali, S., & Heiniger, Y. (2020). The role of digital technologies in humanitarian law, policy and action: Charting a path forward. *International Review of the Red Cross*, *102*(913), 1–22. doi:10.1017/S1816383121000114

14. Greenberg, Andy. "The Untold Story of NotPetya, the Most Devastating Cyberattack in History." Wired, August 2018.

15. Hathaway, Oona & Crootof, Rebecca & Levitz, Philip & Nix, Haley & Nowlan, Aileen & Perdue, William & Spiegel, Julia. (2011). The Law of Cyber-Attack. California Law Review. 100.

16. Melzer, N. (2013). Human rights implications of the usage of drones and unmanned robots in warfare. In European Parliament's Subcommittee on Human Rights, *Policy Department DG External Policies* (p. PE 410.220 EN). European Union. https://doi.org/10.2861/213

Reports

1. International Committee of the Red Cross (ICRC). International Humanitarian Law and the Challenges of Contemporary Armed Conflicts. ICRC, 2015.

2. United Nations Human Rights Council. The Right to Privacy in the Digital Age. A/HRC/27/37, 2014.

3. European Union Agency for Cybersecurity (ENISA). Threat Landscape Report 2020. ENISA, 2020.

4. Amnesty International. Surveillance Giants: How the Business Model of Google and Facebook Threatens Human Rights. Amnesty International, 2019.

5. Human Rights Watch. World Report 2023: Events of 2022. Human Rights Watch, 2023.

6. NATO Strategic Communications Centre of Excellence. Robotrolling 2021/2: Online Influence Operations in an Era of Automation. NATO StratCom COE, 2021.

7. Wyatt Hoffman, "AI and the Future of Cyber Competition," (Center for Security and Emerging Technology, January 2021). https://doi.org/10.51593/2020CA007

8. United Nations. (2019). Surveillance and human rights. In *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression* (Report A/HRC/41/35; pp. 1–4).

9. International Institute for Strategic Studies (IISS). Cyber Capabilities and National Power: A Net Assessment. IISS, 2021.

10. International Telecommunication Union (ITU). Global Cybersecurity Index (GCI) 2020. ITU, 2020.

11. International Committee of the Red Cross (ICRC). Autonomous Weapon Systems: Technical, Military, Legal, and Humanitarian Aspects. ICRC, 2016.

12. Winter, E. (2020). THE COMPATIBILITY OF AUTONOMOUS WEAPONS WITH THE PRINCIPLE OF DISTINCTION IN THE LAW OF ARMED CONFLICT. *International and Comparative Law Quarterly*, *69*(4), 845–876. https://doi.org/10.1017/s0020589320000378

International Treaties and Protocols

1. Editor (Ed.). (1994). *PROTOCOLS ADDITIONAL TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949*. https://www.icrc.org/en/doc/assets/files/other/icrc_002_0321.pdf

2. Second International Peace Conference, The Hague, Convention (IV) Respecting the Laws and Customs of War on Land and Its Annex: Regulations Concerning the Laws and Customs of War on Land, -, International Conferences (The Hague), 18 October 1907, https://www.refworld.org/legal/agreements/hague/1907/en/31788

3. International Criminal Court. (2021). Rome Statute of the International Criminal Court. In *Rome Statute of the International Criminal Court* [Book]. https://asp.icc-cpi.int/en_menus/asp/RomeStatute/pages/default.aspx