

The Future of International Criminal Law: Adapting to New Forms of Warfare and Atrocity

<https://doi.org/10.23918/ilic10.50>

Lect. Hamad Kareem Hamad

Department of Law, College of Law, Knowledge University, Kirkuk Road, 44001

Erbil, Kurdistan Region, Iraq

hamad.kareem@knu.edu.iq

Abstract

International Criminal Law (ICL) stands at an important intersection as the nature and atrocities of war develop rapidly in the 21st century. The emergence of cyber warfare, autonomous weapons, and hybrid conflicts and constructing partnerships of non-governmental actors bear highlighted important intervals and boundaries in the flow sound Structure. This research provides a broad and intensive analysis of versatile challenges ahead of International Criminal Law (ICL) as it wants to be compatible with these new and complicated realities. It finds the problem of emerging forms of (ICL) real evolution warfare and atrocities and legal and normative gaps that rest in the flow police. In addition, the research examines the reactions of international institutions and courts for these challenges. Through doctrinal analysis and hypothesis testing of the fancy suit the clause proposes modern routes for advance and prospective book of instructions for (ICL). This research ends with practical recommendations for legal institutional and political reforms to ensure that ICL is becoming increasingly effective at providing justice and responsibility in the time of technical and geopolitical changes.

Keywords: International Criminal Law, Cyber Warfare, Autonomous Weapons, Non-State Actors, Legal Reform, Accountability.

Introduction

Research Statement: The impact of technological development and the dynamic face of armed conflict fundamentally transformed the face of international criminality. The conventional paradigms of International Criminal Law (ICL), which were crafted in the aftermath of the horrors of the 20th century, has become increasingly challenged by new forms of warfare and atrocity. The present research aims at critically analyzing the possibilities of how ICL can evolve in order to become an effective tool of justice and accountability in the 21st century.

Research Problem: This research focuses on the inability of ICL frameworks to confront new kinds of warfare and atrocity. The legal definitions of ICL, jurisdiction, and enforcement were designed for formal war and State. Hence, as cyber warfare, autonomous weapons, hybrid wars, and non-state actors have grown, conceptual and practical gaps have emerged. These developments raise concerns regarding ICL's ability to account for new categories of harm, attribution, jurisdiction, and legal and institutional reform.

Research Objectives: This research aims to examine the historical development and current limitations of International Criminal Law (ICL) in addressing new forms of warfare and atrocity. Additionally, it will search the challenge pose by technological and geopolitical changes, assess how international and national institution are respond, and provide detailed case study on the application program of ICL to cyber war and independent weapon. Therefore, the research will finish with guidelines for reforms to keep ICL powerful and relevant.

Research Importance: This research matters deeply to legal scholars, practitioners, policymakers, and international institutions. As conflicts and atrocities change over time, the likelihood increases that those responsible for new types of harm may evade accountability. ICL's capacity to adapt to these changes is essential, not only for protecting human rights, but also for preserving peace, advancing security, and ensuring justice for victims. This work supports the ongoing expansion of ICL and contributes to the larger movement for achieving international justice by analyzing modern problems and proposing practical solutions.

Research Methodology: The research utilizes a multi-faceted methodology, integrating doctrinal legal analysis, a comparative examination of international laws and case rulings, along with qualitative assessments of recent conflicts and advancements in technology. Key sources consist of international treaties, legislative texts, court rulings, and official documents. Scholarly publications, policy reports, and

expert analyses are classified as secondary sources. Additionally, the research incorporates case studies on the emergence of autonomous weapons and recent cyberattacks to highlight specific challenges and possible solutions.

Research Plan: There are six major sections to the research. The first section discusses the history and development of ICL. The latter half focuses on cyber warfare, autonomous weaponry, hybrid warfare, and non-state actors. The doctrinal and procedural flaws in ICL frameworks are covered in the last section. The fourth section looks at both domestic and foreign reactions. The fifth section discusses case studies of cyberwarfare and autonomous weaponry. Suggestions for ICL reform and future directions are provided in the sixth section. An overview of the results and some useful recommendations round up the piece.

Section 1: Historical Evolution of International Criminal Law

While international criminal law (ICL) traces its roots back to post-WWI, it was the horrific acts of WWII that truly drove the creation of a full legal system to hold individuals accountable for international crimes. The Nuremberg and Japanese capital Tribunals laid the foundational principle of ICL. These principles included defining war crimes, crimes against humanity, and crimes against peace as international offenses, rejecting immunity for heads of state, and establishing individual criminal responsibility⁽¹⁾. These ideas were further developed and detailed by the 1949 Geneva Conventions and their Additional Protocols, which set clear rules for protecting both soldiers and civilians during armed conflicts⁽²⁾.

The post-Cold War era saw new fascination with ICL, triggered by the atrocities that were committed in the ex-Yugoslavia and Rwanda. The establishment of the International Criminal Tribunal for the former Yugoslavia (ICTY) and the International Criminal Tribunal for Rwanda (ICTR) was a gigantic expansion of ICL both in the crimes to be prosecuted and the criminals to be prosecuted⁽³⁾. These courts set important jurisprudence on issues such as command responsibility, joint criminal enterprise, and charging sexual violence as a crime against humanity and war crime⁽⁴⁾.

The adoption of the Rome Statute in 1998 and the creation of the International Criminal Court (ICC) in 2002 marked a significant advancement in the institutional framework of International Criminal Law (ICL). The ICC was granted jurisdiction over the gravest offenses that concern the global community: genocide, crimes against humanity, war crimes, and the crime of aggression⁽⁵⁾. Additionally, the Rome Statute brought forth key procedural innovations, such as provisions for victim participation, reparations, and the principle of complementarity, which enables national courts to take precedence over the ICC in specific situations⁽⁶⁾.

Despite these advancements, the core concepts and practices of ICL remain rooted in 20th-century paradigms. The primary subjects of discussion have been conventional armed wars, governmental actors, and mass crimes utilizing conventional weaponry. The rapid advancement of technology and the changing nature of warfare in the twenty-first century have exposed the flaws in these frameworks, raising grave questions regarding ICL's ability to adapt to new types of atrocity and conflict⁽⁷⁾.

Section 2: New Forms of Warfare and Atrocity

New types of conflict have emerged in the twenty-first century that challenges the conventional ICL definitions and hypotheses. Cyberwarfare, for example, is a crucial element of contemporary conflicts as states and non-state actors employ digital technologies to destroy critical infrastructure, steal private

⁽¹⁾ Cassese, Antonio, *International Criminal Law*, 3rd ed., Oxford University Press, Oxford, 2013, p.

45. <https://doi.org/10.1093/he/9780199694921.001.0001>. Also, see Hamad, Hamad Kareem. "Sovereign Immunity and Its Development in International Law." *Qalaai Zanist Scientific Journal* 3.1 (2018): 1113-1129. <https://doi.org/10.25212/ifu.qzj.3.1.46>

⁽²⁾ Geneva Conventions of 1949 and Additional Protocols, ICRC, <https://ihl-databases.icrc.org/en/ihl-treaties/geneva-conventions-1949>

⁽³⁾ Schabas, William A., *An Introduction to the International Criminal Court*, 5th ed., Cambridge University Press, Cambridge, 2017, p. 12. <https://doi.org/10.1017/9781316459997>

⁽⁴⁾ Cryer, Robert et al., *An Introduction to International Criminal Law and Procedure*, 4th ed., Cambridge University Press, Cambridge, 2019, p. 67. <https://doi.org/10.1017/9781108680455>

⁽⁵⁾ Rome Statute of the International Criminal Court, 1998, <https://www.icc-cpi.int/resource-library/documents/rs-eng.pdf>

⁽⁶⁾ Suresh, Veena. "The Victims' Court? An Analysis of the Participation of Victims of Sexual Violence in International Criminal Proceedings." *Groningen Journal of International Law*, vol. 8, no. 2, Feb. 2021, pp. 244–269. Crossref, <https://doi.org/10.21827/grojil.8.2.244-269>

⁽⁷⁾ Bassiouni, M. Cherif, *Introduction to International Criminal Law*, 2nd ed., Brill, Leiden, 2012, p. 123. <https://doi.org/10.1163/9789004231696>

information, and wreak havoc⁽¹⁾. The ability for cyber operations to paralyze a modern society without a single shot being fired was illustrated by the 2007 cyberattacks on Estonia, which were largely attributed to Russian actors⁽²⁾. The devastating potential of cyberwarfare has been further brought to light by subsequent events like the NotPetya malware attack and the Stuxnet attack on Iran's nuclear facilities⁽³⁾.

Another major issue is the threat of killer robots, also known as autonomous weapon systems. Because these systems can select and engage targets without human intervention, they raise significant moral and legal questions regarding proportionality, accountability, and civilian protection⁽⁴⁾. The development and deployment of lethal autonomous weapons systems (LAWS) by major military powers is contentious in the international community, with some countries as well as civil society organizations pushing for a preemptive prohibition⁽⁵⁾.

Hybrid warfare, which combines traditional, unconventional, and cyber methods, complicates the legal environment even further. For instance, the conflict in Ukraine has included a combination of traditional military maneuvers, cyber warfare, disinformation campaigns, and the employment of proxy forces⁽⁶⁾. This blurring of the lines between war and peace, between combatants and between civilians, between state and non-state actors has made it far more difficult to implement ICL⁽⁷⁾.

Prominent non-state actors in recent conflicts include terrorist organizations, private military contractors, and transnational criminal networks. These performers frequently exploit legal and jurisdictional loopholes by conducting their business across national borders and utilizing cutting-edge technologies⁽⁸⁾. The need for things like the rise of ISIS, a group that has committed mass atrocities and utilized social media to recruit and encourage violence, highlights the need for ICL must adjust to the realities of current warfare⁽⁹⁾. The atrocities themselves have also changed. Social media is used to promote violence, as seen in Myanmar, and new technologies have made it possible to weaponized information, conduct mass surveillance, and carry out targeted killings. They all represent new types of harm that may not fit neatly into current legal classifications⁽¹⁰⁾. ICL's task is to make sure that these novel kinds of atrocities are not left unpunished because of legal loopholes.

Section 3: Legal Gaps and Doctrinal Challenges

The adaption of ICL to new forms of warfare and atrocity is hampered by significant doctrinal and procedural challenges. One of the core principles of criminal law is the principle of legitimacy (*nullum crimen sine lege*), which requires that crimes be easily defined in advance⁽¹¹⁾. Numerous new forms of detriment, similar as cyber- attacks or algorithmic targeting, don't fit neatly into existing legal definitions of war crimes, crimes against humanity, or genocide⁽¹²⁾. For illustration, a cyber-attack that disables a

⁽¹⁾ Schmitt, Michael N., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, Cambridge, 2017, p. 34. <https://doi.org/10.1017/9781316822524>

⁽²⁾ Ottis, Rain, "Analysis of the 2007 Cyber- attacks Against Estonia," NATO CCD COE Publications, Tallinn, 2008, p. 5. https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf

⁽³⁾ Aanonsen, Claudia Emilie. "Stuxnet, Revisited (Again): Producing the Strategic Relevance of Cyber Operations." *Journal of Cyber Policy*, vol. 10, no. 1, Jan. 2025, pp. 68–84. Crossref, <https://doi.org/10.1080/23738871.2025.2492570>

⁽⁴⁾ Umbrello, Steven, et al. "The Future of War: Could Lethal Autonomous Weapons Make Conflict More Ethical?" *AI & SOCIETY*, vol. 35, no. 1, Feb. 2019, pp. 273–282, <https://doi.org/10.1007/s00146-019-00879-x>

⁽⁵⁾ Human Rights Watch, "Losing Humanity: The Case Against Killer Robots," 2012, p. 12.

<https://www.hrw.org/report/2012/11/19/losing-humanity/case-against-killer-robots>

⁽⁶⁾ Kucyi, Aaron, et al. "Spontaneous Cognitive Processes and the Behavioral Validation of Time-Varying Brain Connectivity." *Network Neuroscience*, vol. 2, no. 4, Oct. 2018, pp. 397–417, https://doi.org/10.1162/netn_a_00037. Also, see Rahman, Halala Sleyman. "Criminalizing Forced Marriage in Iraqi Law and International Law." *QALAAI ZANIST SCIENTIFIC JOURNAL* 10.4 (2025): 1311-1331. <https://doi.org/10.25212/ifu.qzj.10.4.51>

⁽⁷⁾ Sassòli, Marco, *International Humanitarian Law: Rules, Controversies, and Solutions to Problems Arising in Warfare*, Edward Elgar, Cheltenham, 2019, p. 98. <https://doi.org/10.4337/9781786438553>

⁽⁸⁾ Jin young Hwang. "Sovereignty and Non-State Actors: The Rise of Transnational Influence." *Open Access Research Journal of Science and Technology*, vol. 9, no. 2, Apr. 2025, pp. 023–034. Crossref, <https://doi.org/10.53022/oarjms.2025.9.2.0025>

⁽⁹⁾ United Nations, "Report of the Independent International Fact-Finding Mission on Myanmar," A/HRC/39/64, 2018, p. 15. https://www.ohchr.org/sites/default/files/Documents/HRBodies/HRCouncil/FFM-Myanmar/A_HRC_39_64.pdf

⁽¹⁰⁾ Land, Molly K., and Jay D. Aronson. "Human Rights and Technology: New Challenges for Justice and Accountability." *Annual Review of Law and Social Science*, vol. 16, no. 1, July 2020, pp. 223–240, <https://doi.org/10.1146/annurev-lawsocsci-060220-081955>

⁽¹¹⁾ Melzer, Nils, *International Humanitarian Law: A Comprehensive Introduction*, ICRC, Geneva, 2016, p. 234. <https://eprints.gla.ac.uk/145960/>

⁽¹²⁾ Dinmiss, Heather Harrison, *Cyber Warfare and the Laws of War*, Cambridge University Press, Cambridge, 2012, p. 156 <https://doi.org/10.1017/CBO9780511894527>

hospital power supply, resulting in patient deaths, may not be covered by current delineations of war crimes, which concentrate on physical violence and traditional weapons⁽¹⁾.

Criterion is another major challenge. It is difficult to find offenders and establish intent ⁽²⁾ since cyber activities may be conducted anonymously, through intermediaries/proxies, or by performers working in several administrations. Often missing or hidden in distributed networks and independent systems⁽³⁾ is the foundation of ICL: the chain of command. The question of who's responsible when an autonomous weapon system commits a war crime whether it's the programmer, the commander, or the manufacturer remains unresolved⁽⁴⁾.

Jurisdictional issues further complicate the operation of ICL to new forms of warfare. The international nature of cyber warfare and the involvement of non-state actors challenge traditional sundries of territorial and particular jurisdiction⁽⁵⁾. The ICC and other international courts/tribunals may warrant the accreditation or capacity to make similar crimes, particularly when countries are unintentional or unfit to cooperate⁽⁶⁾.

Procedural challenges include the collection, preservation, and authentication of digital evidence, which is frequently volatile and vulnerable to manipulation⁽⁷⁾. The protection of evidences in virtual surroundings, the need for specialized moxie among investigators and judges, and the rapid-fire pace of technological change all pose significant obstacles to effective prosecution⁽⁸⁾.

The lack of clear legal delineations and criterion mechanisms has led to a situation where numerous new forms of detriment fall into a "legal slate zone," with perpetrators suitable to exploit gaps in the law to avoid accountability⁽⁹⁾. This undermines the deterrent effect of ICL and erodes confidence in the transnational justice system.

Section 4: Institutional Responses and Enforcement

International organizations have started to defy the issues brought about by arising types of warfare and atrocities, yet advancements have been gradational and inconsistent. While the International Criminal Court has not yet brought any cases to court⁽¹⁰⁾, it has commenced primary examinations into cyber-related crimes and the operation of new technologies in warfare. Despite facing challenges, the ICC's Office of the Prosecutor acknowledges the necessity of conforming its investigative and prosecutorial approaches to effectively attack cyber-enabled offenses by significant limitations in capacity and resources⁽¹¹⁾.

The United Nations has set up multiple groups of governmental experts (GGEs) to formulate guidelines for responsible state conduct in cyberspace and to investigate how international law applies to cyber activities⁽¹²⁾. Although these initiatives have achieved some agreement on fundamental principles, such as the relevance of the UN Charter and international humanitarian law to cyberspace, they remain non-binding and lack effective enforcement tools⁽¹³⁾.

⁽¹⁾ Schmitt, Michael N., "Cyber Operations and the Jus in Bello: Key Issues," *International Law Studies*, Vol. 87, 2011, p. 92. <https://digital-commons.usnwc.edu/ils/vol87/iss1/7/>

⁽²⁾ Lin, Herbert. "Attribution of Malicious Cyber Incidents: From Soup to Nuts." *Journal of International Affairs*, vol. 70, no. 1, 2016, pp. 75–137. JSTOR, <https://www.jstor.org/stable/90012598>

⁽³⁾ Crootof, Rebecca, "The Killer Robots Are Here: Legal and Policy Implications," *Cardozo Law Review*, Vol. 36, 2015, p. 1837. <https://cardozolawreview.com/the-killer-robots-are-here-legal-and-policy-implications/>

⁽⁴⁾ Boulanin, Vincent & Verbruggen, Maaik, "Mapping the Development of Autonomy in Weapon Systems," SIPRI, Stockholm, 2017, p. 45. <https://www.sipri.org/publications/2017/other-publications/mapping-development-autonomy-weapon-systems>

⁽⁵⁾ Simmons, Beth A., and Hyeran Jo. "Measuring Norms and Normative Contestation: The Case of International Criminal Law." *Journal of Global Security Studies*, vol. 4, no. 1, Jan. 2019, pp. 18–36, <https://doi.org/10.1093/jogss/ogy043>

⁽⁶⁾ Rasooli, Sayed Aref. "An Examination of Crimes under the Jurisdiction of the International Criminal Court (ICC)." *Baharestan Scientific Research Quarterly Journal*, Dec. 2024, pp. 133–148. Crossref, <https://doi.org/10.61438/bsrqj.v2i3.124>

⁽⁷⁾ Grigore, Georgiana, et al. "Drama and Discounting in the Relational Dynamics of Corporate Social Responsibility." *Journal of Business Ethics*, vol. 174, no. 1, Aug. 2020, pp. 65–88. Crossref, <https://doi.org/10.1007/s10551-020-04591-5>

⁽⁸⁾ Singer, P.W. & Friedman, Allan, *Cybersecurity and Cyberwar: What Everyone Needs to Know*, Oxford University Press, Oxford, 2014, p. 201. <https://doi.org/10.1093/wentk/9780199918096.001.0001>

⁽⁹⁾ Deibert, Ron. "The Geopolitics of Cyberspace After Snowden." *Current History*, vol. 114, no. 768, Jan. 2015, p.9 <https://doi.org/10.1525/curh.2015.114.768.9>

⁽¹⁰⁾ ICC, "Preliminary Examination: Situation in Ukraine," 2022, <https://www.icc-cpi.int/ukraine>

⁽¹¹⁾ ICC, "Policy Paper on Case Selection and Prioritisation," 2016, https://www.icc-cpi.int/sites/default/files/itemsDocuments/20160915_OTP-Policy_Case-Selection_Eng.pdf

⁽¹²⁾ United Nations, "Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace," 2021 <https://digitallibrary.un.org/record/3934214?ln=en&v=pdf>

⁽¹³⁾ United Nations, "Developments in the Field of Information and Telecommunications in the Context of International Security," A/RES/73/27, 2018, <https://undocs.org/A/RES/73/27>

Regional organizations have also made efforts to tackle new types of criminal activity. The Council of Europe's Convention on Cybercrime (the Budapest Convention) offers a framework for international collaboration in the investigation and prosecution of cybercrime, but its emphasis is on criminal law rather than international criminal law (ICL)⁽¹⁾. The European Union has put forward directives and regulations aimed at boosting cybersecurity and addressing cyber-enabled crime, but these initiatives primarily focus on safeguarding critical infrastructure and personal data⁽²⁾.

The prosecution of foreign combatants, cybercriminals, and private military contractors are examples of more recent atrocities over which national courts have occasionally exercised universal jurisdiction⁽³⁾. However, these efforts are often hindered by political considerations, a lack of international collaboration, and a lack of funding⁽⁴⁾. The principle of complementarity, which enables national jurisdictions to take precedence over international courts, may also present challenges to effective prosecution when states are reluctant or unable to take action⁽⁵⁾.

In order to identify, stop, and respond to atrocities made possible by cyberspace, the private sector particularly technology companies is getting more and more important⁽⁶⁾. Companies like Facebook, Twitter, and Google have established programs and tools to identify and count content that incites violence or facilitates mortal rights violations⁽⁷⁾. Still, the participation of private realities brings up enterprises about responsibility, translucency, and chancing the right balance between public and private authority in administering ICL⁽⁸⁾.

Civil society Associations have also been necessary in establishing new forms of atrocities, championing for legal reforms, and aiding victims⁽⁹⁾. juggernauts like the International Campaign to Stop Killer Robots and the Global Network Initiative have heightened mindfulness of the troubles posed by new technologies and have supported for further robust transnational regulations⁽¹⁰⁾.

Despite these initiatives, there are still considerable deficiencies in how institutions respond to new types of warfare and atrocities. The absence of well-defined legal frameworks, inadequate funding, and the challenges presented by technological and geopolitical factors have obstructed transnational and public institutions in their pursuit of justice and accountability⁽¹¹⁾.

Section 5: Case Studies: Cyber Warfare and Autonomous Weapons

Cyber Warfare

The 2007 cyber incidents targeting Estonia are frequently cited as a landmark event, representing one of the earliest instances of a large-scale, coordinated digital attack directed against a sovereign nation. Over a span of several weeks, the websites belonging to the Estonian government, banking sector, and media were subjected to distributed denial-of-service (DDoS) attacks, severely undermining the nation's digital framework⁽¹²⁾. Although there were no fatalities, the attacks inflicted considerable economic and social turmoil, prompting discussions on whether such actions could be classified as war crimes or crimes against humanity if they led to loss of life or extensive suffering⁽¹³⁾.

(1) Council of Europe, "Convention on Cybercrime," <https://www.coe.int/en/web/cybercrime/the-budapest-convention>. Also, see Halala Slyman Rahman, Mahdi Hamdi Mahdi Mahdi, and Hind Abdulameer Hameed Hameed. "Penal Populism in Criminal Cases in Courts." Zanco Journal of Law and Politics ۱۷۰-۱۵۸ : (۲۰۲۴) ۲۲, ۳۷ گۆڤاری زانکۆ بۆ یاساو رامیاری <https://doi.org/10.21271/zjlp.22.37.8>

(2) European Union, "Directive on Security of Network and Information Systems (NIS Directive)," 2016, <https://eur-lex.europa.eu/eli/dir/2016/1148/oj>

(3) Kagita, Mohan Krishna, et al. A Review on Cyber Crimes on the Internet of Things. Springer Singapore, 2021, pp. 83–98, https://doi.org/10.1007/978-981-16-6186-0_4

(4) See supra note No. 24, pp. 18–36.

(5) Justin Ngambu Wanki, et al. "Putting the Relationship between States and the ICC into Perspective: The Viability of National Courts in Driving Complementarity in Africa." *Obiter*, vol. 41, no. 1, Apr. 2020, pp. 136–153. Crossref, <https://doi.org/10.17159/obiter.v41i1.10554>

(6) See supra note No. 15, pp. 023–034.

(7) Facebook, "Community Standards," <https://transparency.fb.com/policies/community-standards/>

(8) See supra note No. 28, P. 9.

(9) Human Rights Watch, "Losing Humanity: The Case Against Killer Robots," 2012, p. 12. <https://www.hrw.org/report/2012/11/19/losing-humanity/case-against-killer-robots>

(10) Human Rights Watch, "Losing Humanity: The Case Against Killer Robots," 2012, p. 12. <https://www.hrw.org/report/2012/11/19/losing-humanity/case-against-killer-robots>

(11) See supra note No. 27, p. 201.

(12) See supra note No. 9, p. 5.

(13) See supra note No. 20, p. 92.

The Stuxnet incident targeting Iran's nuclear sites in 2010, reportedly executed by the United States and Israel, marked a novel type of state-sponsored interference⁽¹⁾. The Stuxnet worm was specifically engineered to disrupt and damage centrifuges involved in Iran's uranium enrichment process, delaying the nation's nuclear objectives by several years⁽²⁾. This incident blurred the distinctions between spying, sabotage, and fortified conflict, and underlined the difficulties girding criterion and responsibility in the digital realm⁽³⁾.

The NotPetya malware incident in 2017, linked to Russian military intelligence, inflicted billions in damages on businesses and critical infrastructures globally⁽⁴⁾. This attack illustrated the capacity of cyber operations to produce worldwide, magpie consequences, and raised significant questions regarding the applicability of transnational felonious law (ICL) to acts of cyber aggression⁽⁵⁾.

Although there is increasing awareness of the risks associated with cyber warfare, there have been no legal actions taken regarding cyber-enabled war crimes or crimes against humanity under international criminal law (ICL). The absence of precise legal definitions, mechanisms for attribution, and frameworks for jurisdiction has led to a scenario where offenders can operate with a degree of impunity⁽⁶⁾.

The development and deployment of lethal autonomous weapon systems (LAWS) by major military powers have raised important ethical and legal questions⁽⁷⁾. With the ability to recognize and strike targets without any human intervention, LAWS raise concerns about diminishing human control over the use of force, the risk of unintended escalation, and the potential violation of international humanitarian law⁽⁸⁾.

The use of self-operating drones in battle zones, particularly during the US-led campaign against ISIS, has highlighted the challenges of maintaining responsibility for civilian casualties and violations of wartime regulations⁽⁹⁾. Although drones are usually managed via human operators, the developing reliance on synthetic intelligence and system studying for targeting raises issues about whether cutting-edge criminal structures are adequate⁽¹⁰⁾.

Global attempts to regulate LAWS, including the United Nations Convention on Certain Conventional Weapons (CCW), have faced obstacles due to disagreements regarding definitions, the possibility of a ban, and the priorities of powerful military nations⁽¹¹⁾. Certain countries and civil society groups have advocated for a preemptive prohibition on fully autonomous weapons, asserting that they fundamentally contradict the principles of international criminal law (ICL) and international humanitarian law⁽¹²⁾. Conversely, some have contended that existing legal systems are adequate as long as significant human oversight is preserved in the application of force⁽¹³⁾.

The absence of agreement on LAWS regulation has resulted in a scenario where nations can freely create and implement increasingly autonomous systems, heightening the risk of accountability voids and the emergence of new types of atrocities⁽¹⁴⁾.

Section 6: Pathways for Reform and Future Directions

The difficulties arising from arising types of warfare and atrocities bear a thorough and varied approach from the global community. Above all, the interpretations of fundamental international crimes need to be

⁽¹⁾ See supra note No. 10, pp. 68–84.

⁽²⁾ Ibid.

⁽³⁾ See supra note No. 21, pp. 75–137.

⁽⁴⁾ Greenberg, Andy, *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*, Doubleday, New York, 2019, p. 156. <https://dokumen.pub/sandworm-a-new-era-of-cyberwar-and-the-hunt-for-the-kremlins-most-dangerous-hackers-978-0385544405.html>

⁽⁵⁾ See supra note No. 8, p. 34.

⁽⁶⁾ See supra note No. 19, p. 156. Also, See Hamad, Hamad Kareem. "Impunity in International Criminal Justice." QALAAI ZANIST SCIENTIFIC JOURNAL 10.4 (2025): 1287-1310. <https://doi.org/10.25212/lfu.qzj.10.4.50>

⁽⁷⁾ See supra note No. 11, pp. 273–282.

⁽⁸⁾ See supra note No. 23, p. 45.

⁽⁹⁾ Crootof, Rebecca, "The Killer Robots Are Here: Legal and Policy Implications," *Cardozo Law Review*, Vol. 36, 2015, p. 1837. <https://cardozolawreview.com/the-killer-robots-are-here-legal-and-policy-implications/>

⁽¹⁰⁾ See supra note No. 27, p. 201.

⁽¹¹⁾ United Nations, "Group of Governmental Experts on Lethal Autonomous Weapons Systems (LAWS)," <https://meetings.unoda.org/ccw/convention-on-certain-conventional-weapons-group-of-governmental-experts-on-lethal-autonomous-weapons-systems-2025>

⁽¹²⁾ Human Rights Watch, "Losing Humanity: The Case Against Killer Robots," 2012, p. 12. <https://www.hrw.org/report/2012/11/19/losing-humanity/case-against-killer-robots>

⁽¹³⁾ See supra note No. 8, p. 34.

⁽¹⁴⁾ See supra note No. 23, p. 45.

revised to include newer forms of detriment, analogous as cyber- attacks, algorithmic targeting, and the deployment of independent weapons⁽¹⁾. This could mean creating new international agreements that specifically address these challenges or revising the Rome Statute⁽²⁾.

Enhancing attribution methods also requires the establishment of specialized cyber units in international tribunals, improved international cooperation, and technical standards for digital evidence⁽³⁾. We can address the issues of identifying offenders and by using cutting-edge forensic techniques, working with foreign colleagues, and getting help from professionals in the commercial sector. understanding their objectives in complicated cyber activities⁽⁴⁾.

Additionally, the jurisdiction of international courts should be broadened to include crimes perpetrated by non-state actors and those occurring in cyberspace⁽⁵⁾. This could mean the introduction of new protocols, the formation of hybrid tribunals that combine both national and international components, or employing universal jurisdiction by national courts⁽⁶⁾.

Furthermore, enhancing collaboration with the private sector and civil society is crucial for identifying, preventing, and responding to new types of atrocities⁽⁷⁾. Collaborations between public and private entities can improve information sharing, facilitate the identification of harmful content and actions, and help establish ethical guidelines for the deployment of new technologies in conflict⁽⁸⁾.

In addition, the global community needs to focus on capacity-building, education, and the formation of ethical and legal frameworks for the application of new technologies in warfare⁽⁹⁾. This encompasses training for investigators, prosecutors, and judges regarding the technical elements of cyber warfare and autonomous systems, alongside the creation of guidelines for the responsible use of artificial intelligence and other innovative technologies⁽¹⁰⁾.

Finally, to address the threats posed by new forms of war and atrocities, there is an immediate need for greater political will and international cooperation. We must build new legal structures, make our current systems stronger, and encourage taking responsibility in international criminal law to keep it relevant and working well.⁽¹¹⁾. every person who commits crimes with an international scope.

Conclusion

The future of International Criminal Law relies on its capability to acclimatize to the fleetly changing geography of atrocities and warfare. The emergence of cyber warfare, autonomous weapons, mongrel conflicts, and the adding involvement of non-state actors has exposed major sins in being legal fabrics. While public governments and transnational associations have begun to attack these issues, there remains a significant quantum of work ahead. ICL refines legal definitions, enhances attribution mechanisms, broadens jurisdiction, fosters collaboration with the private sector and civil society, and invests in education and skill-building. It could remain an essential resource for justice and accountability in the 21st century.

Results

1. The existing ICL frameworks are insufficient to handle new types of atrocities and warfare, especially when it comes to cyberspace and autonomous weapons.
2. It is necessary to update legal definitions of basic crimes to include injuries caused by algorithms and digital devices.
3. Issues with jurisdiction and attribution make it difficult to prosecute emerging types of crime effectively.
4. There are still a lot of gaps in the adaptation to these issues that international institutions have made.
5. Investment in technical know-how and cooperation with the commercial sector are necessary for future efficacy.

⁽¹⁾ See supra note No. 18, p. 234.

⁽²⁾ See supra note No. 19, p. 156.

⁽³⁾ See supra note No. 26, pp. 65–88.

⁽⁴⁾ See supra note No. 27, p. 201.

⁽⁵⁾ See supra note No. 35, p. 321.

⁽⁶⁾ Adanan, Amina. "Reflecting on the Genocide Convention in Its Eighth Decade." *Journal of International Criminal Justice*, vol. 19, no. 5, Nov. 2021, pp. 1039–1065. Crossref, <https://doi.org/10.1093/jicj/mqab070>

⁽⁷⁾ See supra note No. 15, pp. 023–034.

⁽⁸⁾ See supra note No. 28, P.9.

⁽⁹⁾ See supra note No. 27, p. 201.

⁽¹⁰⁾ See supra note No. 18, p. 234.

⁽¹¹⁾ See supra note No. 3, p. 12.

Recommendations:

1. Amend the Rome Statute and affiliated covenants to explicitly include cyber- attacks, algorithmic targeting, and independent munitions as prosecutable crimes.
2. Establish specialized cyber and technology units within International Criminal Tribunals to enhance investigative and prosecutorial capacity.
3. Develop transnational norms for digital evidence and criterion, supported by specialized cooperation among countries and the private sector.
4. Expand the governance of transnational courts to cover crimes committed by non-state actors and in cyberspace, including through the use of hybrid courts and universal governance.
5. Encourage collaboration between the public and private sectors, invest in education and capacity-building, and establish ethical frameworks for the responsible application of new technologies in conflict situations.

References

Books & Journal Articles

- Aanonsen, Claudia Emilie. "Stuxnet, Revisited (Again): Producing the Strategic Relevance of Cyber Operations." *Journal of Cyber Policy*, vol. 10, no. 1, Jan. 2025, Crossref, <https://doi.org/10.1080/23738871.2025.2492570>
- Adanan, Amina. "Reflecting on the Genocide Convention in Its Eighth Decade." *Journal of International Criminal Justice*, vol. 19, no. 5, Nov. 2021, Crossref, <https://doi.org/10.1093/jicj/mqab070>
- Bassiouni, M. Cherif, *Introduction to International Criminal Law*, 2nd ed., Brill, Leiden, 2012, <https://doi.org/10.1163/9789004231696>
- Boulanin, Vincent & Verbruggen, Maaïke, "Mapping the Development of Autonomy in Weapon Systems," SIPRI, Stockholm, 2017, <https://www.sipri.org/publications/2017/other-publications/mapping-development-autonomy-weapon-systems>
- Cassese, Antonio, *International Criminal Law*, 3rd ed., Oxford University Press, Oxford, 2013, p. 45. <https://doi.org/10.1093/he/9780199694921.001.0001>
- Crotoft, Rebecca, "The Killer Robots Are Here: Legal and Policy Implications," *Cardozo Law Review*, Vol. 36, 2015, <https://cardozolawreview.com/the-killer-robots-are-here-legal-and-policy-implications/>
- Cryer, Robert et al., *An Introduction to International Criminal Law and Procedure*, 4th ed., Cambridge University Press, Cambridge, 2019, <https://doi.org/10.1017/9781108680455>
- Deibert, Ron. "The Geopolitics of Cyberspace After Snowden." *Current History*, vol. 114, no. 768, Jan. 2015, <https://doi.org/10.1525/curh.2015.114.768.9>
- Dinniss, Heather Harrison, *Cyber Warfare and the Laws of War*, Cambridge University Press, Cambridge, 2012, <https://doi.org/10.1017/CBO9780511894527>
- Greenberg, Andy, *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*, Doubleday, New York, 2019, <https://dokumen.pub/sandworm-a-new-era-of-cyberwar-and-the-hunt-for-the-kremlins-most-dangerous-hackers-978-0385544405.html>
- Grigore, Georgiana, et al. "Drama and Discounting in the Relational Dynamics of Corporate Social Responsibility." *Journal of Business Ethics*, vol. 174, no. 1, Aug. 2020, Crossref, <https://doi.org/10.1007/s10551-020-04591-5>.
- Halala Slyeman Rahman, Mahdi Hamdi Mahdi Mahdi, and Hind Abdulameer Hameed Hameed. "Penal Populism in Criminal Cases in Courts." *Zanco Journal of Law and Politics* ٢٢، ٣٧ (٢٠٢٤): ٢٢، ٣٧. <https://doi.org/10.21271/zjlp.22.37.8>
- Hamad, Hamad Kareem. "Impunity in International Criminal Justice." *QALAAI ZANIST SCIENTIFIC JOURNAL* 10.4 (2025). <https://doi.org/10.25212/lfu.qzj.10.4.50>
- Hamad, Hamad Kareem. "Sovereign Immunity and Its Development in International Law." *Qalaa Zanist Scientific Journal* 3.1 (2018). <https://doi.org/10.25212/lfu.qzj.3.1.46>
- Human Rights Watch, "Losing Humanity: The Case Against Killer Robots," 2012, <https://www.hrw.org/report/2012/11/19/losing-humanity/case-against-killer-robots>
- ICC, "Policy Paper on Case Selection and Prioritisation," 2016, https://www.icc-cpi.int/sites/default/files/itemsDocuments/20160915_OTP-Policy_Case-Selection_Eng.pdf
- ICC, "Preliminary Examination: Situation in Ukraine," 2022, <https://www.icc-cpi.int/ukraine>

- International Campaign to Stop Killer Robots, <https://www.stopkillerrobots.org/>
- Jin young Hwang. "Sovereignty and Non-State Actors: The Rise of Transnational Influence." Open Access Research Journal of Science and Technology, vol. 9, no. 2, Apr. 2025, Crossref, <https://doi.org/10.53022/oarjms.2025.9.2.0025>
- Justin Ngambu Wanki, et al. "Putting the Relationship between States and the ICC into Perspective: The Viability of National Courts in Driving Complementarity in Africa." Obiter, vol. 41, no. 1, Apr. 2020, Crossref, <https://doi.org/10.17159/obiter.v41i1.10554>
- Kagita, Mohan Krishna, et al. A Review on Cyber Crimes on the Internet of Things. Springer Singapore, 2021, https://doi.org/10.1007/978-981-16-6186-0_4
- Kucyi, Aaron, et al. "Spontaneous Cognitive Processes and the Behavioral Validation of Time-Varying Brain Connectivity." Network Neuroscience, vol. 2, no. 4, Oct. 2018, https://doi.org/10.1162/netn_a_00037.
- Land, Molly K., and Jay D. Aronson. "Human Rights and Technology: New Challenges for Justice and Accountability." Annual Review of Law and Social Science, vol. 16, no. 1, July 2020, <https://doi.org/10.1146/annurev-lawsocsci-060220-081955>
- Lin, Herbert. "Attribution of Malicious Cyber Incidents: From Soup to Nuts." Journal of International Affairs, vol. 70, no. 1, 2016, JSTOR, <https://www.jstor.org/stable/90012598>.
- Melzer, Nils, *International Humanitarian Law: A Comprehensive Introduction*, ICRC, Geneva, 2016, <https://eprints.gla.ac.uk/145960/>
- Ottis, Rain, "Analysis of the 2007 Cyber- attacks Against Estonia," NATO CCD COE Publications, Tallinn, 2008, p. 5. https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf
- Rahman, Halala Sleyman. "Criminalizing Forced Marriage in Iraqi Law and International Law." QALAAI ZANIST SCIENTIFIC JOURNAL 10.4 (2025). <https://doi.org/10.25212/lfu.qzj.10.4.51>
- Rasooli, Sayed Aref. "An Examination of Crimes under the Jurisdiction of the International Criminal Court (ICC)." Baharestan Scientific Research Quarterly Journal, Dec. 2024, Crossref, <https://doi.org/10.61438/bsrqj.v2i3.124>
- Sassòli, Marco, *International Humanitarian Law: Rules, Controversies, and Solutions to Problems Arising in Warfare*, Edward Elgar, Cheltenham, 2019, <https://doi.org/10.4337/9781786438553>
- Schabas, William A., *An Introduction to the International Criminal Court*, 5th ed., Cambridge University Press, Cambridge, 2017, <https://doi.org/10.1017/9781316459997>
- Schmitt, Michael N., "Cyber Operations and the Jus in Bello: Key Issues," *International Law Studies*, Vol. 87, 2011, <https://digital-commons.usnwc.edu/ils/vol87/iss1/7/>
- Schmitt, Michael N., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, Cambridge, 2017, <https://doi.org/10.1017/9781316822524>
- Simmons, Beth A., and Hyeran Jo. "Measuring Norms and Normative Contestation: The Case of International Criminal Law." Journal of Global Security Studies, vol. 4, no. 1, Jan. 2019, <https://doi.org/10.1093/jogss/ogy043>
- Singer, P.W. & Friedman, Allan, *Cybersecurity and Cyberwar: What Everyone Needs to Know*, Oxford University Press, Oxford, 2014, <https://doi.org/10.1093/wentk/9780199918096.001.0001>
- Suresh, Veena. "The Victims' Court? An Analysis of the Participation of Victims of Sexual Violence in International Criminal Proceedings." Groningen Journal of International Law, vol. 8, no. 2, Feb. 2021, <https://doi.org/10.21827/groijl.8.2.244-269>
- Umbrello, Steven, et al. "The Future of War: Could Lethal Autonomous Weapons Make Conflict More Ethical?" AI & SOCIETY, vol. 35, no. 1, Feb. 2019, <https://doi.org/10.1007/s00146-019-00879-x>

International Instruments

- Council of Europe, "Convention on Cybercrime," <https://www.coe.int/en/web/cybercrime/the-budapest-convention>
- European Union, "Directive on Security of Network and Information Systems (NIS Directive)," 2016, <https://eur-lex.europa.eu/eli/dir/2016/1148/oj>

- Facebook, "Community Standards," <https://transparency.fb.com/policies/community-standards/>
- Geneva Conventions of 1949 and Additional Protocols, ICRC, <https://digitallibrary.un.org/record/3934214?ln=en&v=pdf>
<https://www.icrc.org/en/law-and-policy/geneva-conventions-and-their-commentaries>
- Rome Statute of the International Criminal Court, 1998, <https://www.icc-cpi.int/resource-library/documents/rs-eng.pdf>
- United Nations, "Developments in the Field of Information and Telecommunications in the Context of International Security," A/RES/73/27, 2018, <https://undocs.org/A/RES/73/27>
- United Nations, "Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace," 2021
- United Nations, "Group of Governmental Experts on Lethal Autonomous Weapons Systems (LAWS)," <https://meetings.unoda.org/ccw/convention-on-certain-conventional-weapons-group-of-governmental-experts-on-lethal-autonomous-weapons-systems-2025>
- United Nations, "Report of the Independent International Fact-Finding Mission on Myanmar," A/HRC/39/64, 2018, https://www.ohchr.org/sites/default/files/Documents/HRBodies/HRCouncil/FFM-Myanmar/A_HRC_39_64.pdf