



Plagiarism Checker X - Report

Originality Assessment

3%



Overall Similarity

Date: Feb 19, 2026 (01:10 PM)

Matches: 234 / 8843 words

Sources: 10

Remarks: Low similarity detected, consider making necessary changes if needed.

Verify Report:

Scan this QR Code



International Law and Artificial Intelligence: A Structural Readiness 1 Assessment. 2 3
Abstract 4 Artificial intelligence (AI) has rapidly become embedded in core domains of
international 5 concern, from autonomous weapons and cyber operations to biometric
border control, digital 6 trade, and financial regulation. While existing debates in
international law tend to focus on 7 discrete questions—such as the legality of lethal
autonomous weapons or the human-rights 8 implications of algorithmic surveillance—much
less attention has been paid to whether the 9 international legal system, as a structure, is
ready to govern AI as a cross-cutting phenomenon. 10 This article offers a structural
readiness assessment of international law for artificial 11 intelligence. It develops a three-
part framework centred on normative coverage (the extent to 12 which existing rules and
principles apply to AI-mediated conduct), institutional capacity (the 13 ability of
international bodies to interpret, monitor, and enforce those norms), and adaptive 14
flexibility (the system’s capacity to adjust to rapid technological change without constant 15
crisis-driven reform). Drawing on doctrinal analysis and case studies relating to
autonomous 16 weapons, AI-enabled surveillance, and cross-border algorithmic regulation,
the article argues 17 that international law is normatively rich but institutionally thin and
procedurally slow in 18 AI-sensitive areas, producing fragmented, reactive, and often ad
hoc responses. It concludes 19 that meaningful readiness for AI will depend less on
drafting entirely new “AI treaties” and 20 more on clarifying responsibility for AI-mediated
harm, strengthening oversight mandates of 21 existing institutions, and developing
interpretive principles tailored to algorithmic opacity, 22 explainability, and systemic risk. 23

1. Introduction 24 The international legal order was not designed with artificial intelligence
in mind. The UN 25 Charter, the Geneva Conventions, core human-rights treaties, and the
multilateral trade regime 26 emerged in an era when decisions of international significance
were taken primarily by human 27 actors, relying on human judgment and responsibility.
Today, however, AI systems participate 28 in or shape decisions across a spectrum of
activities of direct concern to international law. 29 Militaries experiment with autonomous
weapons and AI-assisted targeting; intelligence services 30 and law-enforcement agencies

rely on algorithmic analysis for surveillance, risk-assessment, 31 and predictive policing; border authorities deploy biometric and AI-driven systems to manage 32 migration; and economic regulators and private actors use algorithms in high-frequency 33 trading, credit-scoring, and cross-border digital services. 34

These developments raise familiar doctrinal questions in new guises. Can autonomous weapons 35 comply with the principles of distinction and proportionality in international humanitarian law 36 (IHL)? Are mass algorithmic surveillance programmes compatible with the rights to privacy, 37 freedom of expression, and non-discrimination under international human rights law? How do 38 AI-enabled digital services interact with commitments on data flows, market access, and 39 non-discrimination under trade and investment agreements? And how should responsibility be 40 allocated when AI-mediated conduct causes cross-border harm? A growing body of scholarship 41 and institutional practice addresses these questions within individual regimes. Yet, as with 42 earlier phases of technological disruption, the risk is that international law responds in a 43 piecemeal fashion, treating each issue in isolation and neglecting the structural implications for 44 the system as a whole. 45 Against this background, the present article asks a different, more systemic question: is the 46 structure of public international law ready for artificial intelligence? Instead of focusing 47 exclusively on whether specific AI applications are lawful, it examines whether the combination 48 of norms, institutions, and processes that make up the international legal order is capable of 49 governing AI as a transversal phenomenon. The analysis is guided by a three-part notion of 50 structural readiness: normative coverage, institutional capacity, and adaptive flexibility. 51 The article does not claim that AI renders existing international law obsolete, nor does it 52 assume that new, AI-specific treaties are always necessary. Its central argument is more 53 nuanced. It contends that international law possesses considerable normative resources to 54 regulate AI-mediated activities but that structural weaknesses in institutional capacity and 55 adaptive flexibility threaten to undermine effective governance, particularly where AI

systems 56 are opaque, rapidly evolving, and dominated by private actors. By situating concrete case 57 studies within this broader framework, the article seeks to illuminate not only doctrinal issues 58 but also deeper questions about authority, legitimacy, and accountability in a digitised world. 59 The article is structured as follows. Section 2 introduces the “diaspora” of AI governance across 60 multiple regimes and institutions, tracing the historical evolution and current landscape of 61 international initiatives on AI. Section 3 outlines the research methodology, combining doctrinal 62 and structural analysis with targeted case studies. Section 4 sets out the theoretical framework, 63 defining structural readiness and linking it to debates on regime complexity and technology 64 governance. Section 5 formulates the research questions. Section 6 reviews the literature on AI 65 and international law, highlighting **1 the need for a** structural perspective. Section 7 presents the 66 core analysis of normative coverage, institutional capacity, and adaptive flexibility. Section 8 67 examines three case studies—autonomous weapons, AI-enabled surveillance, and algorithmic 68 regulation in cross-border economic activity—as concrete sites where these structural issues 69 manifest. Section 9 discusses the broader impact of the identified legal challenges on the 70

legitimacy and effectiveness of international law. Section 10 concludes with reflections on the 71 conditions under which international law can achieve meaningful readiness for AI. 72 2. Diaspora and Its Background 73 2.1. The dispersed landscape of AI governance 74 Unlike traditional arms-control treaties or specialised environmental regimes, there is no single, 75 unified “AI convention” that concentrates international legal authority over artificial 76 intelligence. Instead, AI-relevant norms and processes form a dispersed landscape, or diaspora, 77 stretching across different branches of international law and involving a wide range of 78 institutions and actors. This dispersion is partly the product of historical path-dependence: rules 79 dealing with technological issues have accumulated over decades in separate domains such as 80 telecommunications, cybercrime, data protection, trade in services, and human rights. 81 The emergence of AI as a distinct policy

concern has not displaced these pre-existing regimes. 82 Rather, AI has layered itself onto them, accentuating tensions and creating new 83 interdependencies. For example, AI-enabled cyber operations touch on both the law of state 84 responsibility and emerging cyber norms; biometric identification at borders implicates human 85 rights, refugee law, and data-protection principles; and AI in digital trade raises questions about 86 market access, regulatory autonomy, and cross-border data flows under trade agreements. The 87 result is that AI governance **1 at the international level** does not start from a blank slate; it is 88 superimposed on a complex architecture of overlapping and sometimes competing rules. 89 2.2. From early tech governance to AI-specific initiatives 90 International law's engagement with technology predates AI. The early twentieth century saw 91 treaties on telegraphy, radio communications, and aviation; the Cold War era produced nuclear 92 arms-control agreements and regimes governing outer space; the late twentieth century added 93 data-protection instruments such as Council of Europe Convention 108, the Budapest 94 Convention on Cybercrime, and various frameworks on e-commerce and electronic signatures. 95 These instruments established important precedents: they showed that technology-neutral 96 principles could be applied to new tools, but also that specialised regimes might be necessary 97 where risks were acute. 98 AI entered this picture gradually. Initially, many of its legal implications were treated as 99 extensions of existing debates: autonomous weapons **1 in the context of** IHL, AI-driven 100 surveillance in privacy and data-protection law, and algorithmic trading within financial 101 regulation. Over time, however, AI's distinctive features—opacity, autonomy, scalability, and 102 reliance on large data sets—prompted calls for more explicit governance frameworks. This has 103 led to a proliferation of soft-law instruments and emerging treaty processes. 104

The OECD's 2019 AI Principles were among the first globally endorsed normative statements on 105 AI, articulating values such as human-centred and trustworthy AI, transparency, robustness, 106 and accountability. UNESCO's 2021 **1 Recommendation on the Ethics of** Artificial Intelligence 107 added a broad, human-rights-oriented framework,

covering issues from non-discrimination to 108 environmental impacts. The Council of Europe has since negotiated a Framework Convention 109 on Artificial Intelligence, Human Rights, Democracy and the Rule of Law, which, once in force, 110 will become the first binding international treaty specifically focused on AI. At the same time, 111 the European Union has elaborated the AI Act, a sophisticated risk-based regulatory model with 112 extraterritorial implications that, while not a treaty, will significantly shape cross-border AI 113 governance. 114 In parallel, UN organs have begun to address AI in various ways. The UN Secretary-General has 115 issued policy briefs on AI and global governance; UN human-rights mechanisms have produced 116 thematic reports on AI and human rights; and debates on autonomous weapons continue 117 under the framework of the Convention ⁹ on Certain Conventional Weapons (CCW). However, 118 these developments remain fragmented: they occur in different fora, with different 119 memberships, mandates, and procedural rules. 120

2.3. Actors and asymmetries in the AI governance diaspora

121 The diaspora of AI governance involves an unusually wide array of actors. States are central, but 122 international and regional organisations (UN, Council of Europe, OECD, UNESCO, EU, African 123 Union, among others), technical standard-setting bodies (ISO, IEC, IEEE), and private 124 corporations all participate in norm-creation. Large technology companies and research labs, in 125 particular, exert de facto regulatory influence through their control of infrastructure, 126 algorithms, and data, as well as through corporate codes of conduct and participation in 127 multi-stakeholder initiatives. 128 This pluralism has both advantages and drawbacks. On the one hand, multiple fora allow 129 experimentation and innovation; different institutions can address different aspects of AI (e.g. 130 ethics, human rights, trade, security). On the other hand, dispersion risks incoherence, 131 duplication, and conflict. It also exacerbates inequalities of participation: states and 132 organisations with greater technical and diplomatic capacity can navigate and shape the 133 emerging landscape more effectively, while others struggle to have their perspectives heard. 134 These asymmetries matter because they influence whose values and interests are embedded in 135 global AI governance. 136 The

dispersed character of AI governance thus forms a crucial background for assessing 137 international law's structural readiness. Any evaluation of normative coverage, institutional 138 capacity, and adaptive flexibility must take into account that AI is regulated not in a single 139 venue but across a constellation of regimes and institutions that interact in complex ways. 140

3. Research Methodology 141 This article employs a qualitative methodology combining doctrinal legal analysis with 142 structural and institutional assessment, supported by targeted case studies. The aim is not to 143 test hypotheses in a statistical sense but to understand and systematise how international law, 144 as a normative and institutional system, engages with AI-mediated activities. 145 First, doctrinal analysis focuses on 4 primary sources of international law relevant to AI. These 146 include the UN Charter (particularly provisions on peace and security), the Geneva Conventions 147 and Additional Protocols, core human-rights instruments (such as the ICCPR and ECHR), 148 multilateral and regional trade agreements, and soft-law instruments such as the OECD AI 149 Principles, the UNESCO Recommendation on AI, and the emerging Council of Europe AI 150 Convention. The analysis also considers decisions and opinions of human-rights courts and 151 treaty bodies, as well as relevant reports and resolutions adopted by UN organs and specialised 152 agencies. The doctrinal method is used to identify applicable norms, interpret their scope and 153 content, and evaluate their suitability for regulating AI-mediated conduct. 154 Second, the study performs a structural and institutional analysis, examining the mandates, 155 procedures, and practices of key international bodies involved in AI-related issues. These 156 include, inter alia, the CCW framework and its Group of Governmental Experts on lethal 157 autonomous weapons systems, UN human-rights mechanisms (treaty bodies, special 158 rapporteurs, and regional courts), economic and technical organisations (such as the WTO, 159 OECD, and ITU where relevant), and emerging AI-specific forums. The analysis assesses their 160 capacity to interpret and enforce norms in AI-sensitive contexts, taking into account 161 jurisdictional limits,

resource constraints, expertise, and political dynamics. 162 Third, the article uses illustrative case studies to ground the structural analysis in concrete 163 practice. The chosen case studies—autonomous weapons and IHL, AI-enabled surveillance and 164 human rights, and algorithmic regulation in cross-border economic activity—were selected 165 based on three criteria: (1) each involves salient AI applications with clear international-law 166 implications; (2) each has generated a significant body of legal and policy debate; and (3) 167 together they span the three broad domains of security, human rights, and economic 168 regulation. The case studies are not intended to be exhaustive; rather, they serve as focal 169 points for exploring how the dimensions of structural readiness play out in practice. 170 The research also draws extensively on secondary sources, including academic literature on AI 171 and international law, reports by international organisations and expert groups, NGO analyses, 172 and policy briefs. These materials provide context, document institutional practice, and 173 articulate critiques and reform proposals that are relevant to the structural assessment. 174

Certain limitations should be acknowledged. The rapid pace of AI development and regulation 175 means that the legal and institutional landscape is in flux; new instruments and initiatives may 176 emerge after this article's completion. The focus on global and European practice inevitably 177 under-represents developments in other regions, although the analysis emphasises the 178 importance of broad participation in AI governance. Lastly, the structural emphasis, while 179 essential for the article's aims, leaves less room for detailed exploration of technical AI design 180 choices, which are themselves crucial for effective regulation. Nonetheless, the chosen 181 methodology offers a robust foundation for evaluating international law's readiness for AI in a 182 systematic and conceptually grounded way. 183

4. Theoretical Framework 184

The theoretical framework of this article is built around the concept of structural readiness. 185 Rather than evaluating individual AI applications solely in terms of compliance with specific 186 rules, structural readiness assesses whether the overall configuration of norms,

institutions, 187 and processes in international law is capable of governing AI in a coherent and legitimate 188 manner. 189 The framework comprises three interrelated components: normative coverage, institutional 190 capacity, and adaptive flexibility. 191 Normative coverage refers to the extent to which existing rules and principles of international 192 law apply to AI-mediated activities, and whether they can do so effectively. Many fundamental 193 norms are drafted in technology-neutral terms. The prohibition of the threat or use of force, 194 **1 the principles of distinction, proportionality, and** precaution in IHL, and human-rights 195 guarantees of privacy, non-discrimination, and procedural fairness do not depend on the 196 specific tools used. Likewise, trade and investment rules often speak broadly of services, 197 measures, and treatment without differentiating between AI-enabled and traditional activities. 198 From this perspective, AI does not create a legal vacuum. However, AI's distinctive features— 199 such as opacity of decision-making, the speed and scale of automated actions, reliance on large 200 and sometimes biased datasets, and the centrality of private developers and platforms—place 201 stress on existing norms. Questions arise about how to apply due diligence standards to 202 AI-mediated risk, how to assess foreseeability and control when systems learn and adapt, and 203 how to ensure meaningful accountability when harms are distributed across complex 204 socio-technical systems. Normative coverage thus concerns not only whether rules formally 205 apply, but whether they are substantively adequate to address AI's challenges. 206 Institutional capacity concerns the ability of international institutions to interpret, monitor, and 207 enforce the norms relevant to AI. This includes formal attributes such as jurisdiction, 208 competence, and enforcement powers, as well as practical factors like expertise, resources, and 209

access to information. For example, the CCW framework has taken up **3 the issue of** **lethal** 210 autonomous weapons systems but remains divided on whether to prohibit, regulate, or merely 211 monitor their development. Human-rights courts and treaty bodies have begun to address 212 AI-related surveillance and profiling, but face difficulties in

obtaining evidence about 213 proprietary systems and in crafting general standards. Economic and technical organisations 214 grapple with AI ¹ in the context of digital trade and standards, yet often lack explicit 215 human-rights mandates. Institutional capacity also involves the ability to coordinate across 216 regimes and to engage with non-state actors who control much of the relevant technology. 217 Weak or fragmented institutional capacity can leave even well-formulated norms 218 under-enforced. 219 Adaptive flexibility captures the system's capacity to respond to rapidly evolving technologies 220 without requiring constant formal treaty amendment. In practice, much adaptation occurs 221 through interpretive evolution, soft-law instruments, expert guidelines, and multi-stakeholder 222 processes. Soft law has been particularly prominent in AI governance, as seen in the OECD AI 223 Principles, the UNESCO Recommendation, and various policy frameworks issued by 224 international organisations and regional bodies. These instruments can be adopted relatively 225 quickly and updated as practice develops, but they lack the binding force and institutionalised 226 enforcement mechanisms of treaties. Adaptive flexibility thus involves a trade-off between 227 speed and legal solidity. A system with high adaptive flexibility will generate timely, coherent 228 guidance that shapes behaviour and can be integrated into formal law over time; a system with 229 low flexibility will respond slowly and inconsistently, leaving gaps and uncertainties that actors 230 may exploit. 231 This framework is informed by debates on regime complexity and fragmentation, which 232 describe how international governance often takes place in regime complexes—sets of partially 233 overlapping and non-hierarchical regimes. AI governance exemplifies this phenomenon: 234 security, human-rights, trade, data-protection, and technical-standardisation regimes all claim 235 some jurisdiction over AI-related issues. This can lead to both innovation and conflict. The 236 notion of structural readiness is therefore relational; it is concerned with how these regimes 237 interact and whether, taken together, they can provide coherent and legitimate governance. 238 Finally, the framework engages with scholarship on emerging technology governance, which 239 emphasises anticipatory regulation, precaution, and polycentric governance structures. AI

240 challenges traditional assumptions about agency, foreseeability, and control—elements that 241 underpin legal concepts such as fault, intent, and due diligence. Ideas like “meaningful human 242 control” over autonomous systems, “human-rights impact assessments” for AI deployments, 243 and requirements of transparency and explainability can be seen as early attempts by law and 244 policy to internalise AI-specific concerns. By analysing how and where such concepts are 245

emerging, the article assesses whether international law is evolving towards a more AI-sensitive 246 mode of operation. 247 In the sections that follow, this theoretical framework underpins both the statement of 248 research questions and the analysis of law and practice in the selected case studies. 249

5. Research Questions 250

The present study is structured around a primary research question and three interrelated 251 sub-questions, each corresponding to a component of the structural readiness framework 252 developed above. Together, they seek to move beyond isolated doctrinal debates and to 253 produce a more integrated assessment of international law’s capacity to govern artificial 254 intelligence. 255 The core research question that guides the analysis 4 is: To what extent is the current structure of 256 public international law—its norms, institutions, and adaptive processes—capable of governing 257 AI-mediated activities across security, human rights, and economic domains in a coherent, 258 effective, and legitimate manner? This question is deliberately systemic. It does not ask 259 whether international law is “for” or “against” AI, nor whether a particular application is lawful. 260 Rather, it interrogates the underlying architecture 4 of international law in an era where 261 algorithmic decision-making increasingly shapes decisions of international concern. 262 From this core inquiry, three sub-questions emerge. The first concerns normative 263 coverage: How far do existing rules and general principles of international law already extend to 264 the design, deployment, and effects of AI-driven systems in key domains such as armed conflict, 265 surveillance and border control, and cross-border economic regulation, and where do significant 266 normative gaps or ambiguities arise? This sub-question examines whether

technology-neutral 267 norms—such as due diligence, proportionality, non-discrimination, and procedural fairness— 268 are sufficient, or whether AI’s distinct features demand further specification or novel legal 269 concepts. 270 The second sub-question relates to institutional capacity: Are existing international 271 institutions—security and disarmament fora, human rights courts and treaty bodies, economic 272 and technical organisations, and emerging AI-specific initiatives—equipped, in terms of 273 mandate, expertise, procedure, and enforcement powers, to interpret and implement 274 international norms in relation to AI-mediated activities? Here the focus is not only on formal 275 jurisdiction but also on practical ability: access to technical knowledge, capacity to compel 276 cooperation, and willingness to confront powerful state and non-state actors. 277 The third sub-question addresses adaptive flexibility: Through which mechanisms, and with 278 what degree of agility and coherence, does international law adapt to the rapid evolution of AI 279

technologies, and what structural factors facilitate or impede such adaptation? This inquiry 280 looks at interpretive developments, soft-law instruments, multi-stakeholder processes, and 281 cross-regime coordination as expressions of the system’s ability to respond to AI-related 282 challenges without constant formal treaty revision. 283 These questions are not posed in the abstract. They are operationalised through detailed 284 examination of legal texts, institutional practice, and case studies in subsequent sections. By 285 answering them, the article seeks to illuminate whether international law is merely coping with 286 AI on an ad hoc basis or whether it possess, or can develop, the structural readiness required 287 for long-term governance. 288 6. Literature Review 289

Scholarship on **1 artificial intelligence and international law** is still relatively young, but it has 290 expanded rapidly in recent years. For analytical purposes, it can be divided into several 291 overlapping strands: work on autonomous weapons and the law of armed conflict; analyses of 292 AI-mediated surveillance and human rights; studies of AI, digital trade, and economic 293 regulation; and examinations of global AI governance initiatives

and soft law. While each strand 294 is rich in its own right, they tend to proceed in parallel, leaving the structural questions that 295 motivate this article only partially addressed. 296 A first major strand concerns autonomous weapons and IHL. Since the early 2010s, discussions 297 under ³ the Convention on Certain Conventional Weapons (CCW) have focused on whether lethal 298 autonomous weapons systems (LAWS) should be prohibited or regulated, and what 299 “meaningful human control” over targeting decisions should entail. International and regional 300 organisations, including the ICRC and various UN special rapporteurs, have produced influential 301 reports warning that fully autonomous weapons could challenge compliance with the principles 302 of distinction, proportionality, and precaution, as well as undermine meaningful accountability. 303 Academic writers mirror these concerns, debating whether existing IHL is sufficient or whether 304 specific treaty-based bans are necessary. This literature offers valuable insights into how AI 305 might disrupt core security norms but generally stops short of assessing broader institutional 306 and adaptive capacities. 307 A second corpus addresses AI-enabled surveillance, profiling, and human rights. UN 308 human-rights mechanisms and the Council of Europe have warned that AI-driven facial 309 recognition, predictive policing, and biometric border systems risk entrenching discrimination, 310 enabling pervasive surveillance, and eroding due-process guarantees. Reports by the UN High 311 Commissioner for Human Rights have called for moratoria or strict regulation of certain uses of 312 AI that are incompatible with privacy and equality rights, while regional courts have begun to 313 consider cases involving digital surveillance and algorithmic decision-making. Scholars analyse 314

these developments through the lenses of privacy, non-discrimination, freedom of expression, 315 and access to remedies, often drawing analogies with earlier jurisprudence on mass 316 surveillance and data-retention. Yet, here too, attention tends to remain within the 317 human-rights silo, with less emphasis on how these issues intersect with trade, security, or 318 technical standard-setting. 319 A growing third strand

explores AI, digital trade, and economic regulation. WTO-related 320 literature has examined how rules on services, data flows, and non-discrimination apply to 321 AI-enabled platforms, algorithmic services, and cross-border data-intensive business models. 322 Regional trade agreements, particularly those involving digital chapters, increasingly address 323 issues such as source-code disclosure, data localisation, and algorithmic regulation, raising 324 questions about regulatory autonomy and the ability of states to impose transparency or 325 human-rights-oriented requirements on AI-driven services. Scholarship in this area 326 demonstrates that AI does not fit neatly within existing trade categories, but it rarely connects 327 these concerns with parallel debates in security and human-rights regimes. 328 A fourth body of work deals with global AI governance and soft-law instruments. Analyses of 329 the OECD AI Principles, UNESCO's Recommendation, the EU's AI Act, and the Council of 330 Europe's AI convention process highlight emergent consensus around certain values—such as 331 transparency, accountability, and human-centric design—as well as persistent tensions 332 between innovation, regulation, and geopolitical competition. This literature emphasises the 333 role of multi-stakeholder processes, private governance by big technology companies, and the 334 increasing weight of technical standards bodies. It also raises concerns about fragmentation, 335 duplication, and possible “forum-shopping” by states seeking favourable regulatory 336 environments. 337 Finally, there is an emerging but still thin strand that explicitly contemplates AI and the 338 structure of international law. Some authors discuss AI in relation to general principles such as 339 state responsibility and due diligence, or in connection with the concept of jus cogens and 340 peremptory norms, especially 1 in the context of lethal autonomous weapons and systemic 341 surveillance. Others allude to regime complexity and the risk of “siloeed” governance, but few 342 attempt a systematic evaluation of normative coverage, institutional capacity, and adaptive 343 flexibility across multiple regimes. 344 In sum, existing literature offers rich doctrinal and policy analysis of AI within specific legal 345 fields but tends to overlook the cross-cutting structural questions that this article seeks to 346 address. There is a clear need for a study that

synthesises insights across these strands and 347 evaluates international law's readiness for AI as a systemic issue, rather than as a series of 348 isolated challenges. 349

7. Analysis 350 This section applies the structural readiness framework to three key dimensions of 351 international law's engagement with AI: normative coverage, institutional capacity, and 352 adaptive flexibility. It draws on doctrinal material, institutional practice, and the case studies 353 developed in the next section to provide an integrated assessment. 354 7.1. Normative coverage: technology-neutral rules and AI-specific pressures 355 At first glance, international law appears well-equipped to address AI-mediated activities. Core 356 norms are formulated in broad, technology-neutral terms and apply irrespective of the tools 357 used. The prohibition of the threat or use of force, the principles of distinction and 358 proportionality in IHL, human-rights guarantees of privacy, non-discrimination, and fair trial, 359 and trade rules on services and non-discrimination all cover conduct carried out through AI 360 systems as much as through traditional means. States remain responsible under existing 361 doctrines when they deploy AI in ways that breach these obligations, just as they would be for 362 violations committed with conventional tools. 363 However, the appearance of sufficiency masks deeper tensions. AI systems introduce new 364 modalities of risk and harm that strain traditional concepts. Opacity, often described as the 365 "black box" problem, can make it difficult to ascertain how an AI system arrived at a particular 366 output, complicating assessments of intent, foreseeability, and negligence. Machine-learning 367 models may evolve in deployment, creating a moving target for regulation. When AI systems 368 interact in complex digital environments, chains of causation become diffuse: harms may 369 emerge from a combination of design choices, training data, deployment contexts, and user 370 behaviour. Existing doctrines of state responsibility and due diligence must therefore operate in 371 a context where attribution of specific decisions to individual human agents is less 372 straightforward, and where control is shared between states and private developers or 373 platforms. 374 In the security domain, debates [2 on lethal autonomous](#)

weapons highlight these concerns. While 375 IHL principles remain applicable, serious doubts exist about whether autonomous systems can 376 reliably distinguish combatants from civilians, assess proportionality, or react appropriately to 377 dynamic battlefield conditions without human judgment. The very notion of “meaningful 378 human control” is contested, and existing treaty language does not specify the degree or 379 quality of human involvement required. In human-rights law, AI-driven surveillance and 380 profiling raise questions about what constitutes “arbitrary” or “unlawful” interference with 381 privacy when data collection and analysis become ubiquitous and continuous. 382 Non-discrimination norms must grapple with algorithmic bias embedded in training data and 383

model design, often in ways that evade traditional categories of direct or indirect 384 discrimination. 385 In economic law, AI-enabled services complicate the application of definitions and 386 commitments negotiated before such technologies existed. The classification of AI-driven 387 platforms and services for purposes of market-access commitments, the treatment of 388 algorithmic transparency requirements as potential trade barriers, and the interaction between 389 data-localisation rules and AI’s data needs all expose grey areas in trade and investment law. 390 Overall, normative coverage is substantial but incomplete. International law has the conceptual 391 tools to address AI in many areas, yet the specificity and clarity of those tools may be 392 insufficient for consistent application. Emerging soft-law instruments and interpretive efforts 393 can be seen as attempts to fill this gap, signalling an evolving, but still uneven, normative 394 landscape. 395 7.2. Institutional capacity: mandates, expertise, and enforcement 396 Even where norms exist, the capacity of institutions to apply and enforce them in AI-related 397 contexts is uneven. The CCW’s **2 Group of Governmental Experts on lethal autonomous weapons** 398 has, over several years, produced guiding principles and ongoing discussions but has not yet 399 agreed on a legally binding outcome, reflecting deep divisions among states about the 400 desirability and feasibility of a prohibition or strict

regulation. Its mandate, the need for 401 consensus, and the complexity of technical issues limit its ability to move from general 402 principles to concrete, enforceable rules. 403 Human-rights institutions have been more active in addressing AI. UN special rapporteurs and 404 the Office of the High Commissioner for Human Rights have issued detailed reports on AI and 405 human rights, calling for moratoria on certain uses and for robust safeguards in others. 406 Regional courts and treaty bodies have begun to interpret existing rights in light of digital 407 surveillance and algorithmic decision-making, sometimes grounding their reasoning in broader 408 principles of the rule of law and democratic oversight. Nonetheless, they often face evidentiary 409 challenges when dealing with proprietary AI systems, lack direct access to technical expertise, 410 and rely heavily on submissions from states and civil society for information about system 411 design and impact. Their decisions may have strong persuasive authority but limited direct 412 enforcement power, especially beyond their regional scope. 413 Economic and technical organisations occupy a more ambiguous position. Bodies involved in 414 trade, standards, and telecommunications have significant influence over the conditions under 415 which AI systems are designed and deployed, but their mandates frequently emphasise 416 efficiency, interoperability, and trade facilitation rather than human-rights or security concerns. 417 Coordination between these institutions and human-rights or security bodies is limited and 418

often informal. Emerging AI-specific forums and initiatives—whether under the OECD, UNESCO, 419 or ad hoc multi-stakeholder platforms—can develop sophisticated guidance but lack the 420 authority to impose binding obligations. 421 Institutional capacity is thus characterised by fragmentation and asymmetry. Some institutions 422 are norm-rich but enforcement-poor; others have technical influence but weak human-rights 423 mandates. Few possess a combination of strong jurisdiction, robust enforcement mechanisms, 424 and deep technical expertise oriented explicitly toward AI governance. This structural weakness 425 risks leaving AI-mediated harms inadequately addressed, particularly where

powerful states or 426 corporations are involved. 427 7.3. Adaptive flexibility: soft law, experimentation, and inertia 428 With respect to adaptive flexibility, the picture is mixed. On the one hand, international law has 429 seen a proliferation of soft-law instruments, guidelines, and principles that address AI more 430 rapidly than formal treaties could. The OECD AI Principles, the UNESCO Recommendation, and 431 numerous policy frameworks at regional level demonstrate a willingness to engage with AI in a 432 forward-looking manner. These instruments can be updated over time, serve as references for 433 domestic legislation, and influence corporate practices, especially where they are backed by 434 major economies and institutions. 435 **5** On the other hand, the reliance on soft law and interpretive evolution creates risks of 436 fragmentation and variable implementation. Without binding force or strong monitoring 437 mechanisms, adherence to AI principles can be uneven, and their integration into hard law is 438 neither automatic nor guaranteed. Moreover, formal treaty-making on AI—such as the Council 439 of Europe’s AI convention—proceeds slowly and may be limited in geographic reach. 440 Security-related processes, such as those concerning autonomous weapons, struggle to keep 441 pace with technological developments, leading to a sense that “law always arrives late” in the 442 face of emerging capabilities. 443 Institutional inertia, geopolitical rivalry, and **1** the complexity of AI itself all constrain adaptive 444 flexibility. States may be reluctant to agree to stringent international standards that they fear 445 could limit their strategic or economic advantages. Multi-stakeholder processes can include 446 diverse perspectives but sometimes lack clear decision-making authority. Technical expertise, 447 while increasingly integrated into governance discussions, remains unevenly distributed and is 448 often concentrated in the private sector. 449 Taken together, these factors suggest that international law’s adaptive flexibility in relation to 450 AI is present but fragile. The system can generate soft-law responses and interpretive 451 developments, but structural obstacles may prevent these from coalescing into a coherent and 452 sufficiently robust governance framework. The following case studies illustrate how these 453

dynamics play out in practice, and how legal challenges in specific domains reflect the broader 454 structural issues identified in this section. 455 8. Case Studies 456 This section examines three illustrative case studies that bring into focus the dynamics of 457 normative coverage, institutional capacity, and adaptive flexibility discussed above. They are not 458 exhaustive of all AI-related challenges in international law, but they represent key domains— 459 security, human rights, and economic regulation—where structural tensions are particularly 460 visible. 461 8.1. 2 Autonomous weapons and the law of armed conflict 462 Debates on lethal autonomous weapons systems (LAWS) have become one of the most 463 prominent intersections between AI and international law. LAWS are generally understood as 464 weapons systems that, once activated, can 6 select and engage targets without further human 465 intervention. The prospect of delegating 1 life-and-death decisions to machines has triggered 466 intense legal, ethical, and political controversy. 467 From a normative coverage perspective, IHL applies fully to the use of LAWS. Parties to armed 468 conflict remain bound by the principles of distinction, proportionality, and precaution, as well as 469 by customary rules governing weapons that are indiscriminate or cause unnecessary suffering. 470 States deploying LAWS would be responsible for ensuring that such systems can comply with 471 these obligations in practice. Article 36 of Additional Protocol I requires legal reviews of new 472 weapons to determine their compatibility with international law, a provision that applies 473 equally to AI-enabled systems. 474 Nevertheless, the application of these norms is contested. Critics argue that current or 475 foreseeable AI technology cannot reliably distinguish combatants from civilians in complex 476 environments, particularly where civilians and fighters intermingle or where contextual 477 judgment is required. They question whether autonomous systems can make proportionality 478 assessments that require qualitative evaluation of expected military advantage versus collateral 479 harm, or adequately interpret dynamic battlefield signals indicating surrender or incapacitation. 480 Proponents contend that, in some contexts, autonomous systems might be more precise than 481 humans, reducing error and emotional bias. The lack of explicit AI-specific rules in IHL

leaves 482 considerable discretion to states in interpreting their obligations. 483 As to institutional capacity, the CCW framework and its 3 Group of Governmental Experts (GGE) 484 have become the primary forum for multilateral discussion. The GGE has agreed on guiding 485 principles, including that IHL continues to 2 apply to all weapons systems and that humans remain 486 responsible for decisions on the use of force. However, 7 it has not reached consensus on a legally 487

binding instrument prohibiting or strictly regulating LAWS. A number of states and civil-society 488 coalitions advocate for a pre-emptive ban, while others favour continued monitoring, arguing 489 that existing law suffices. The CCW's consensus-based decision-making and its limited 490 enforcement mechanisms constrain its ability to produce strong, binding outcomes. The ICRC 491 and UN officials have urged states to adopt clear constraints on 7 autonomy in weapons systems, 492 but these recommendations lack direct legal effect. 493 Regarding adaptive flexibility, the LAWS debate demonstrates both innovation and inertia. On 494 the one hand, the very existence 2 of the GGE and the rapid development of normative concepts 495 such as “meaningful human control” show that states and institutions can respond proactively 496 to emerging technologies. 5 On the other hand, the slow progress toward binding rules, despite 497 years of discussion and accelerating technological development, exemplifies the problem of law 498 lagging behind technological change. The absence of clear global standards risks a scenario in 499 which some states unilaterally develop and deploy increasingly autonomous weapons, creating 500 pressure on others to follow and making future regulation harder. 501 Overall, the LAWS case reveals substantial normative coverage but contested interpretation, 502 limited institutional capacity to translate debates into binding rules, and only partial adaptive 503 flexibility 5 in the face of rapid technological advancement. 504 8.2. AI-enabled surveillance and international human rights law 505 The second case study concerns AI-driven surveillance, profiling, and decision-making in areas 506 such as law enforcement, border control, and social-media monitoring. States and private actors 507

increasingly deploy facial-recognition systems, predictive policing tools, and algorithmic analysis 508 of online content. These practices raise core human-rights issues, particularly regarding privacy, 509 non-discrimination, 1 freedom of expression, and access to effective remedies. 510 In terms of normative coverage, international human-rights treaties already provide robust 511 protection against arbitrary or unlawful interference with privacy, discriminatory treatment, and 512 unjustified restrictions on expression and movement. The ICCPR, for example, protects the right 513 to privacy and family life and prohibits discrimination on various grounds. Regional instruments, 514 8 such as the European Convention on Human Rights, contain analogous protections and have 515 generated extensive jurisprudence on surveillance, data retention, and secret-service activities. 516 These norms apply irrespective of whether surveillance is conducted through human agents or 517 AI-enabled systems. 518 However, AI-enabled surveillance introduces new forms of risk. Large-scale facial-recognition 519 systems can track individuals across multiple contexts and datasets, creating pervasive, 520 continuous monitoring. Predictive policing tools 10 trained on historical crime data may reproduce 521 and reinforce existing biases, disproportionately targeting certain communities. Algorithmic 522

content moderation and recommender systems can shape access to information and public 523 discourse in opaque ways. Traditional human-rights tests—such as whether an interference is 524 lawful, pursues a legitimate aim, and is necessary and proportionate—must now be applied to 525 complex socio-technical systems whose functioning is not easily understandable. 526 With respect to institutional capacity, human-rights mechanisms have begun to respond. UN 527 special rapporteurs have issued reports expressing concern about AI-driven surveillance, 528 recommending moratoria on certain uses, and calling for strict safeguards and human-rights 529 impact assessments. Regional courts have extended existing surveillance jurisprudence to 530 digital contexts, emphasising the need for clear legal bases, independent oversight, and 531 effective

remedies. Yet, many of these bodies face practical limitations: they depend on 532 information provided by states and civil-society organisations, may lack in-house technical 533 expertise, and cannot directly compel disclosure of proprietary algorithms or training data. 534 Remedies are often individual and retroactive, whereas AI-enabled surveillance is systemic and 535 ongoing. 536 The adaptive flexibility of human-rights law in this area is both promising and incomplete. On 537 the one hand, interpretive developments—such as recognition of the chilling effect of mass 538 surveillance on expression and association, and acknowledgment of algorithmic bias as a form 539 of discrimination—show that human-rights bodies can adapt existing norms to new 540 technologies. 5 On the other hand, the absence of binding, AI-specific human-rights instruments 541 and the reliance on case-by-case adjudication may lead to uneven standards and enforcement. 542 Some states embrace robust safeguards; others use AI tools in ways that evade scrutiny or rely 543 on opaque security justifications. 544 Thus, while human-rights law offers strong normative foundations, institutional capacity and 545 adaptive mechanisms are still catching up with the scale and complexity of AI-enabled 546 surveillance. 547 8.3. AI, algorithms, and cross-border economic regulation 548 The third case study explores AI's role in cross-border economic activity, particularly digital 549 trade, algorithmic decision-making in services, and data-driven business models. AI is now 550 integral to e-commerce platforms, cloud-based services, algorithmic trading, and personalised 551 advertising, all of which operate across borders and fall within the ambit of trade and 552 investment rules. 553 From a normative coverage standpoint, WTO agreements and regional trade treaties regulate 554 trade in goods and services, intellectual property, and related aspects of digital commerce. 555 However, most of these instruments were negotiated before AI became central to digital 556 services. Commitments on services often refer to modes of supply without distinguishing 557

between human-provided and algorithmically delivered services. Provisions on 558 non-discrimination, market access, and domestic regulation apply, but their interaction with 559

AI-specific measures is not always clear. For example, requirements that firms disclose information about their algorithms, ensure explainability, or maintain certain data within national borders may be characterised as barriers to trade or investment, even when motivated by human-rights or security concerns. In terms of institutional capacity, economic tribunals and dispute-settlement bodies have not yet developed a substantial body of case law on AI-specific measures. Nonetheless, emerging disputes over data localisation, access to source code, and cross-border digital services suggest that such cases are likely. Technical standard-setting bodies (such as ISO and IEC) and economic organisations (like the OECD and WTO) influence the conditions under which AI systems operate through standards, guidelines, and trade rules, yet their mandates typically prioritise trade facilitation and interoperability over human-rights or security considerations. Coordination with human-rights or security bodies is limited, raising the risk that AI-relevant trade rules may conflict with other international obligations or hinder domestic regulation aimed at ensuring trustworthy AI. Regarding adaptive flexibility, digital trade negotiations and plurilateral initiatives on e-commerce have begun to include provisions on source-code and algorithmic disclosure, data flows, and localisation. Some of these proposals seek to restrict states' ability to demand access to algorithms or to impose data-localisation requirements, reflecting concern about protectionism but potentially constraining regulatory space for AI oversight. Soft-law frameworks on trustworthy AI from economic organisations can encourage good practices but lack binding force. **2 The absence of a clear,** integrated approach to AI in trade and investment law underscores the structural challenge: economic rules are adapting to digitalisation, but not always in ways that account for the broader governance needs of AI. This case study thus illustrates how AI interacts with economic regimes that were not designed with such technologies in mind, raising questions about normative coherence, institutional role allocation, and the balance between trade facilitation and regulatory autonomy. 9. Impact of Legal Challenges The legal challenges identified in the preceding analysis and case studies

have significant 587 implications for the legitimacy, effectiveness, and coherence 4 of

international law in the age of 588 AI. They also affect how states, individuals, and private actors perceive and engage with the 589 international legal order. 590 9.1. Legitimacy and trust in international institutions 591

Structural shortcomings in normative clarity, institutional capacity, and adaptive flexibility can 592 erode the perceived legitimacy of international law. When autonomous weapons debates stall 593 despite widespread ethical concern, when AI-enabled surveillance appears to outpace 594 human-rights oversight, or when trade rules seem to constrain legitimate regulation of AI, 595 affected communities may question whether international institutions are capable of protecting 596 fundamental values in a digitised world. 597 This legitimacy deficit can have self-reinforcing effects. States may become less willing to accept 598 international scrutiny or to invest in strengthening institutions they perceive as ineffective. 599 Individuals and civil-society organisations may turn to domestic courts or political advocacy 600 rather than international mechanisms. Private actors, particularly large technology companies, 601 may fill governance gaps through self-regulation, further privatising normative choices that 602 ought to be subject to public oversight. 603 9.2. Accountability gaps and unequal protection 604 AI's deployment in security, surveillance, and economic systems can exacerbate existing 605 accountability gaps. If international law struggles to attribute responsibility for AI-mediated 606 harm—because of diffuse causal chains, shared control between states and private entities, or 607 limited access to technical evidence—victims may find it difficult to obtain remedies at national 608 or international levels. 609 Moreover, structural inequalities in participation and capacity mean that not all states are 610 equally able to shape AI governance or to protect their populations from harmful uses. 611 Wealthier states and corporations often lead in AI development and standard-setting, while 612 many developing countries must accept imported technologies and governance frameworks 613 with limited influence over their design. This can entrench imbalances in power and protection, 614 with residents of some

regions more likely to be subjected to unregulated surveillance, 615 experimental systems, or exploitative economic models. 616 If left unaddressed, these accountability and equity concerns risk undermining the universality 617 and fairness that international law claims as core attributes. 618 9.3. Fragmentation, forum-shopping, and regulatory arbitrage 619 The dispersed nature of AI governance and the uneven development of norms and institutions 620 create opportunities for fragmentation and strategic behaviour. States and private actors may 621 engage in forum-shopping, selecting the most favourable venue or regime for advancing their 622 interests—whether in trade negotiations, technical standard-setting, or security forums. 623

Regulatory arbitrage becomes easier when 4 there is no clear, coherent framework for AI across 624 regimes. Companies may locate data or operations in jurisdictions with weaker oversight, while 625 still benefiting from cross-border markets. States may invoke security or trade justifications 626 selectively to resist human-rights-oriented constraints. Such behaviour can further erode 627 coherence and undercut efforts by more ambitious regulators to enforce higher standards. 628 9.4. Prospects for structural reform 629 6 At the same time, the challenges highlighted in this article create pressure for structural reform. 630 Calls for clearer allocation of responsibility in AI-related harms, stronger human-rights mandates 631 for technical and economic bodies, more robust oversight mechanisms for AI deployment in 632 security and surveillance, and better coordination across regimes reflect a growing awareness 633 that fragmented governance is inadequate. 634 Efforts such as the Council of Europe's AI convention, ongoing debates under the CCW, and the 635 integration of AI considerations into human-rights and trade bodies illustrate attempts to move 636 toward more coherent frameworks. Whether these initiatives will coalesce into a genuinely 637 structural response depends on political will, the willingness of states to accept constraints on 638 strategic and commercial interests, and the capacity of international institutions to integrate 639 technical expertise and diverse perspectives. 640 10. Conclusion 641 Artificial intelligence does not confront

international law with an entirely new universe; rather, 642 it amplifies and accelerates existing tensions about authority, accountability, and the 643 relationship between technology and human dignity. This article has offered a structural 644 readiness assessment of international law for AI, focusing on three dimensions: normative 645 coverage, institutional capacity, and adaptive flexibility. 646 The analysis suggests that international law is normatively rich: core principles in IHL, 647 human-rights law, and economic law already apply to many AI-mediated activities and provide 648 meaningful constraints in theory. However, AI's distinctive characteristics—opacity, complexity, 649 speed, and reliance on private actors—strain the application of these norms and expose areas 650 where greater specificity or new interpretive tools are needed. 651 Institutional capacity is more uneven and fragile. Security fora, human-rights bodies, economic 652 organisations, and technical standard-setters all play roles in AI governance but often operate 653 with limited mandates, incomplete expertise, and modest enforcement powers. Coordination 654 across regimes remains ad hoc. As a result, even where norms exist, their implementation and 655 enforcement in AI-related contexts can be inconsistent and incomplete. 656

Adaptive flexibility, finally, is present but constrained. Soft-law instruments, expert guidelines, 657 and interpretive developments show that international law can respond to AI more quickly than 658 formal treaty-making would allow. Yet, structural obstacles—including consensus-based 659 procedures, geopolitical competition, and institutional inertia—limit the speed and coherence 660 of this adaptation. 661 The case studies on autonomous weapons, AI-enabled surveillance, and cross-border economic 662 regulation illustrate these dynamics in concrete settings. They reveal persistent accountability 663 gaps, legitimacy concerns, and risks of fragmentation, but also sites of innovation where new 664 concepts and processes are emerging. 665 The article therefore concludes that international law is neither obsolete 5 in the face of AI nor 666 fully prepared. Its structural readiness is a moving target. To improve it, states and international

667 institutions should prioritise: 668 □ Clarifying responsibility for AI-mediated harm, including the duties of states to regulate 669 private developers and platforms. 670 □ Strengthening the mandates, resources, and technical expertise of existing bodies that 671 oversee AI-relevant norms, particularly in human-rights and security contexts. 672 □ Developing cross-cutting interpretive principles—such as transparency, explainability, 673 human-rights impact assessment, and meaningful human control—that can be 674 integrated into multiple regimes. 675 □ Enhancing coordination between security, human-rights, trade, and technical-standards 676 bodies to reduce fragmentation and regulatory arbitrage. 677 Ultimately, whether international law becomes genuinely ready for artificial intelligence will 678 depend on political choices. AI can either reinforce an international order marked by inequality, 679 opacity, and contestation, or it can act as a catalyst for renewing commitments to human rights, 680 the rule of law, and shared responsibility in a technologically complex world. 681 11. References 682 1. OECD. (2019). OECD Principles on Artificial Intelligence. OECD 683 Publishing. <https://www.oecd.org/sti/artificial-intelligence/policies/oecd-principles-on684-artificial-intelligence.htm> 685 2. UNESCO. (2021). **1 Recommendation on the Ethics of** Artificial Intelligence. 686 UNESCO. <https://unesdoc.unesco.org/ark:/48223/pf0000380455> 687

3. Council of Europe. (2024). Framework Convention on Artificial Intelligence, Human 688 Rights, Democracy and the Rule of Law. Council of Europe Treaty Series No. 689 235. <https://www.coe.int/en/web/artificial-intelligence/cai-convention> 690 4. Office **3 of the United Nations** High Commissioner for Human Rights (OHCHR). (2021). The 691 Right to Privacy in the Digital Age: Report of the Special Rapporteur on the Right to 692 Privacy. A/HRC/48/31. <https://www.ohchr.org/en/documents/thematic693-reports/ahrc4831-report-special-rapporteur-right-privacy-right-privacy-digital-age> 694 5. **3 International Committee of the Red Cross (ICRC)**. (2018). Autonomous Weapon Systems: 695 Implications of Increasing Autonomy in the Critical Functions of Weapons. ICRC 696 Report. <https://www.icrc.org/en/document/autonomous-weapon-systems-implications697>

increasing-autonomy-critical-functions-weapons 698 6. United Nations. ⁴ (1969). Vienna Convention on the Law of Treaties. United Nations Treaty 699 Series, vol. 1155, p. 700 331. https://legal.un.org/ilc/texts/instruments/english/conventions/1_1_1969.pdf 701 7. International Committee of the Red Cross (ICRC). (2005). Measures to Implement Article 702 36 of Additional Protocol I of 1977. ICRC Expert Meeting Report. https://international703review.icrc.org/sites/default/files/irrc_864_11.pdf 704 8. Cortright, D., & Lopez, G. A. (2000). The Sanctions Decade: Assessing UN Strategies in the 705 1990s. Lynne Rienner Publishers. 706 9. Farrall, J. M. (2007). United Nations Sanctions and the Rule of Law. Cambridge University 707 Press. 708 10. Hovell, D. (2016). The Power of Process: The Value of Due Process in Security Council 709 Sanctions Decision-Making. Oxford University Press. 710 11. Reinisch, A. (2001). "Securing the Effects of Security Council Sanctions: The Need for a 711 Full Judicial Review." *European Journal of International Law*, 12(4), 795–819. 712 12. Scharre, P. (2018). *Army of None: Autonomous Weapons and the Future of War*. W.W. 713 Norton & Company. 714 13. Yeung, K., & Lodge, M. (2019). "Algorithmic Regulation: A Critical 715 Interrogation." *Regulation & Governance*, 12(4), 505–523. 716 14. United Nations Secretary-General. (2021). *Our Common Agenda: Report of the 717 Secretary-General*. A/75/982. <https://www.un.org/en/content/common-agenda-report/> 718 15. ³ International Committee of the Red Cross (ICRC). (2017). *Autonomous Weapon Systems: 719 Technical, Military, Legal and Humanitarian Aspects*. ICRC Expert Meeting 720 Report. <https://www.icrc.org/en/document/autonomous-weapon-systems-technical721military-legal-and-humanitarian-aspects> 722 16. European Court of Human Rights. (2020). *Big Brother Watch and Others v. United 723 Kingdom* (Application nos. 58170/13, 62322/14 and 24960/15). Judgment. 724 17. ² United Nations General Assembly. (2023). *Resolution on Human Rights and Artificial 725 Intelligence*. A/RES/78/XXX (forthcoming or related resolutions). 726

18. World Trade Organization. (2021). *Digital Trade Developments*. WTO 727 Report.

https://www.wto.org/english/res_e/booksp_e/digital_trade_2021_e.pdf 728 19. Alter, K. J., & Raustiala, K. (2018). "The Rise of International Regime 729 Complexes." *American Journal of International Law*, 112(3), 417–464. 730 20. Drezner, D. W. (2011). "Sanctions Sometimes Smart: Targeted Sanctions in Theory and 731 Practice." *International Studies Review*, 13(1), 96–108. 732 733

Sources

1	https://bhattandjoshiassociates.com/artificial-intelligence-and-international-law-ethical-and-legal-implications/ INTERNET 1%
2	https://carnegieendowment.org/research/2024/08/understanding-the-global-debate-on-lethal-autonomous-weapons-systems-an-indian-perspective INTERNET <1%
3	https://www.unoda.org/en/our-work/conventional-arms/convention-certain-conventional-weapons INTERNET <1%
4	https://www.academia.edu/7637590/Sources_of_International_Law_A_brief_analysis INTERNET <1%
5	https://www.theaiforum.org/the-ai-forum/yacoubi-ai-transparency-black-box-paradox INTERNET <1%
6	https://fsi.stanford.edu/sipr/content/lethal-autonomous-weapons-next-frontier-international-security-and-arms-control INTERNET <1%
7	https://www.lawfaremedia.org/article/considering-a-legally-binding-instrument-on-autonomous-weapons INTERNET <1%
8	https://bromundlaw.com/human-rights/regional-human-rights-instruments-vs-global-human-rights-instruments INTERNET <1%
9	https://www.odu.edu/sites/default/files/documents/ib-6th-updating-the-cccw.pdf INTERNET <1%
10	https://www.researchgate.net/profile/Harrison-Blake-2/publication/387382131_AI_in_Criminal_Justice_Addressing_Concerns_About_Bias_Fairness_and_Accountability_in_Predictive_Policing_and_Sentencing_Algorithms/links/676b7309fb9aff6eaaebae7c/AI-in-Criminal-Justice-Addressing-Concerns-About-Bias-Fairness-and-Accountability-in-Predictive-Policing-and-Sentencing-Algorithms.pdf INTERNET <1%

EXCLUDE CUSTOM MATCHES ON

EXCLUDE QUOTES OFF

EXCLUDE BIBLIOGRAPHY OFF