Regulating AI-Powered Cyber Operations Under International Law: A Preliminary Inquiry

Yuan Fang *

I. INTRODUCTION

Over the past few years, the international community has seen the rapid emergence of cyber technology as well as the ever-changing landscape of Artificial Intelligence ("AI"). No one should underestimate the significant impacts of AI on cyber technology. To some degree, AI can be seen as a "double-edged sword" in the context of cybersecurity.[1] On the one hand, AI tools can assist us in enhancing our capabilities of detecting and preventing potential cyber threats.[2] But on the other hand, as AI technology continues to advance at a rapid pace, the potential for cyberattacks using AI-based techniques has raised great concerns pertaining to cybersecurity.

---

* This article is based on the presentation given to the Transnational Law & Contemporary Problems Symposium "Artificial Intelligence and International Humanitarian Law" at University of Iowa College of Law on April 4, 2025. The author wishes to extend his heartfelt thanks to the editors of TLCP for the opportunity to present this work at the symposium and get it published afterward.

[1] *E.g.*, Deryck Mitchelson, *The Double-Edged Sword of Artificial Intelligence in Cybersecurity*, WORLD ECON. F. (Oct. 27, 2023), https://www.weforum.org/stories/2023/10/the-double-edged-sword-of-artificial-intelligence-in-cybersecurity [https://perma.cc/6CU2-AALR]; Jithu Joseph, *AI in Cybersecurity – The Double-Edged Sword*, CLOUD SEC. ALL. (Nov. 27, 2024), https://cloudsecurityalliance.org/blog/2024/11/27/ai-in-cybersecurity-the-double-edged-sword [https://perma.cc/EL53-UZSJ]; Sebastian Ganschow, *The Double-Edged Sword of AI in Cybersecurity*, NTT Data (Sep. 16, 2025), https://services.global.ntt/en-us/insights/blog/the-double-edged-sword-of-ai-in-cybersecurity [https://perma.cc/98HY-QQX9].

[2] *See* Scott J. Shackelford & Rachel Dockery, *Governing AI*, 30 CORNELL J.L. & PUB. POL'Y 279, 295 (2020).

Cyber activities involving AI elements present unique challenges due to the complicated nature of AI systems and their increasing integration into various sectors such as healthcare, finance, transportation, and defense.[3] For example, AI tools can automate and accelerate certain phases of a cyberattack or increase attack precision to create new threats to cybersecurity.[4] More specifically, skilled cyber actors are capable of leveraging AI-enabled automation to aid evasion and scalability, proliferation of AI-enabled cyber tools increases access to AI-enabled intrusion capability to an expanded range of state and non-state actors, and the growing incorporation of AI models and systems presents an increased attack surface for adversaries to exploit.[5] In this regard, the governance of cyber operations involving AI has become an increasingly pressing issue in today's interconnected world.[6]

The international community calls for the emergence of novel norms and rules to guide state conduct in AI development and deployment.[7] This Paper, however, aims to explore and address the main challenges in regulating AI-powered cyber operations through revitalizing the existing resources that international law possesses. Section II will discuss the current landscape of the regulatory frameworks of international law governing the issue and unveil the inadequacies there. Section III will then introduce a comprehensive and improved regulatory framework to fill the gaps. Section IV provides an illustration of how this proposed framework will be specifically applied to the

---

[3] *See* MICROSOFT, THE FUTURE COMPUTED: ARTIFICIAL INTELLIGENCE AND ITS ROLE IN SOCIETY 63 (2018), https://news.microsoft.com/cloudforgood/_media/downloads/the-future-computed-english.pdf [https://perma.cc/ZKP6-DGUH].

[4] *See, e.g.*, MixMode Threat Research, *The Rise of AI-Driven Cyberattacks: Accelerated Threats Demand Predictive and Real-Time Defenses*, MIXMODE.AI BLOG (May 1, 2025), https://mixmode.ai/blog/the-rise-of-ai-driven-cyberattacks-accelerated-threats-demand-predictive-and-real-time-defenses [https://perma.cc/3R4M-Q64P]; Juan Hernandez, *How to Combat AI Cybersecurity Threats*, PREY PROJECT (Oct. 30, 2024), http://preyproject.com/blog/battling-ai-enhanced-cyber-attacks [https://perma.cc/YU9J-RP6G]. For a technical explanation of the distinctions between classic and AI-powered cyber-attacks, see Muhammad Mudassar Yamin et al., *Weaponized AI for Cyber Attacks*, 57 J. INFO. SEC. & APPLICATIONS 1, 3–4 (2021); see also MARCUS COMITER, ATTACKING ARTIFICIAL INTELLIGENCE: AI'S SECURITY VULNERABILITY AND WHAT POLICYMAKERS CAN DO ABOUT IT 47 (2019), https://live-hksbelfer.pantheonsite.io/sites/default/files/2019-08/AttackingAI/AttackingAI.pdf [https://perma.cc/ZKW9-AMW8].

[5] *Impact of AI on Cyber Threat from Now to 2027*, NAT'L CYBER SEC. CTR. (May 7, 2025), https://www.ncsc.gov.uk/report/impact-ai-cyber-threat-now-2027 [https://perma.cc/7GHU-UAGB].

[6] For further discussions regarding the significance and challenges of the governance of AI-powered cyber activities, see Blessing Guembe et al., *The Emerging Threat of AI-Driven Cyber Attacks: A Review*, 36 APPLIED A.I. 2376, 2376–78 (2022); Simon Chesterman, *Weapons of Mass Disruption: Artificial Intelligence and International Law*, 10 CAMBRIDGE INT'L L.J. 181, 188–92 (2021); Felipe Chiarello & Lara Rocha Garcia, *Desafios Internacionais da Aplicação da Inteligência Artificial No Direito* [*International Challenges of Applying Artificial Intelligence in Law*], 35 REVISTA JUSTICA DO DIREITO [REV. JUST. DIREITO] 6, 8–23 (2021) (Braz.); Matthijs M. Maas, *International Law Does Not Compute: Artificial Intelligence and the Development, Displacement or Destruction of the Global Legal Order*, 20 MELB. J. INT'L L. 29, 30–34 (2019); Thomas Burri, *International Law and Artificial Intelligence*, 60 GER. Y.B. INT'L L. 91, 95–101 (2017).

[7] *See* Press Release, Security Council, International Community Must Urgently Confront New Reality of Generative, Artificial Intelligence, Speakers Stress as Security Council Debates Risks, Rewards, U.N. Press Release SC/15359 (July 18, 2023).

various AI-powered cyber activities. The concluding Section will summarize the paper with an outlook on the implementation of the innovative framework.

II. THE INADEQUACIES OF THE EXISTING REGULATORY FRAMEWORKS

One of the key challenges in governing AI-powered cyber operations is deciding who (or what) should take the legal responsibility for certain outcomes,[8] given that AI is beginning to increasingly resemble human beings' abilities in memorizing, analyzing, and decision-making.[9] Accordingly, it is crucial to establish explicit rules to navigate these uncertainties and ensure the responsible use of AI technology in cyberspace. So, what do we have in our toolbox right now under international law?

A. *International Hard Law*

First, we have international hard law, which refers to legally binding rules that impose definite obligations on states and other international actors. International hard law mainly consists of treaties and customary international law,[10] and it covers both global and regional regimes. In terms of global regimes, multiple regulatory frameworks are potentially applicable to cyber operations involving AI, *e.g.*, International Criminal Law ("ICL"),[11] International Humanitarian Law ("IHL"),[12] and International Human Rights Law ("IHRL").[13] With regard to regional regimes, one prominent example is the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (hereinafter "Framework Convention").[14] The following discussion examines these regimes, outlining their respective advantages and disadvantages for the governance of AI-powered cyber activities.

We will first look at the application of ICL to AI-powered cyber operations. The core concepts of ICL include genocide, war crimes, crimes against humanity, and crimes of aggression, which are also the four crimes falling within the jurisdiction of the International Criminal Court ("ICC").[15] Since ICL is only

---

[8] JAEMIN LEE, ARTIFICIAL INTELLIGENCE AND INTERNATIONAL LAW 56 (2022).

[9] *Id.* at 63.

[10] Arnold N. Pronto, *Understanding the Hard/Soft Distinction in International Law*, 48 VAND. J. TRANSNAT'L L. 941, 947 (2015).

[11] For discussions about the applicability of ICL to AI-powered cyber operations, see, e.g., Onur Sari & Sener Celik, *Legal Evaluation of the Attacks Caused by Artificial Intelligence-Based Lethal Weapon Systems Within the Context of Rome Statute*, 42 COMPUT. L. & SEC. REV. 1, 1–14 (2021).

[12] For discussions concerning the applicability of IHL to AI-powered cyber operations, see, e.g., Alan Schuller, *At the Crossroads of Control: The Intersection of Artificial Intelligence in Autonomous Weapon Systems with International Humanitarian Law*, 8 HARV. NAT'L SEC. J. 379, 382–425 (2017).

[13] For discussions pertaining to the applicability of IHRL to AI-powered cyber operations, see, e.g., Anna Su, *The Promise and Perils of International Human Rights Law for AI Governance*, 4 L. TECH. & HUMS. 166, 166–77 (2022).

[14] Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, Sep. 5, 2024, C.E.T.S. No. 225.

[15] *About the Court*, INT'L CRIM. CT., https://www.icc-cpi.int/about/the-court [https://perma.cc/KW6G-M2CN] (last visited Apr. 19, 2026, at 20:01 CT).

applicable to the gravest breaches of international law, it sets an extremely high threshold for the breaches to be considered.[16] Nevertheless, it can be extremely difficult for the AI-powered cyber operations to reach that threshold, so a very limited number of such activities might fall within the scope of ICL.[17]

With respect to IHL and IHRL, some scholars have underscored the importance of the distinction between the question of whether the existing rules cover the new situation and the question of whether they are adequate for that situation.[18] Although it is generally agreeable that IHL and IHRL are applicable in the context of AI-powered cyber activities, there will be more uncertainty and suspicion when it comes to the sufficiency of IHL and IHRL to regulate AI-powered cyber operations. There is little doubt that IHL and IHRL are complementary to some extent.[19] For example, IHL applies during armed conflict while IHRL can apply in both peacetime and armed conflict.[20] IHL primarily governs the relationship between states (with the exception of non-international armed conflicts), whereas IHRL governs the conduct of a state towards its people.[21] Hence, IHL and IHRL coming together would potentially cover a much broader range of AI-powered cyber activities as compared with ICL.[22] However, the human rights-centric approach adopted by IHL and IHRL will constrain the scope of AI-powered cyber activities: while human rights protection has an irreplaceable function in modern international law, it only represents one of the dimensions of governing the AI-powered cyber activities under international law.

Apart from the global regimes discussed above, we also have regional regimes governing the issue. The regional efforts to govern AI systems have been fragmented, with various regions adopting different approaches to cybersecurity

---

[16] *See id.*

[17] Notwithstanding the huge potential of AI, at this moment, the most common AI-enabled cyber-attacks primarily contain automated phishing campaigns, AI-enhanced social engineering, AI-generated malware, and deepfake attacks, which are hardly possible to be severe enough to violate ICL. *See* Mili Leitner Cohen, *4 AI-Powered Cyber Threats and Why AI Cybersecurity is the Most Effective Response*, GCORE (Dec. 17, 2024), http://gcore.com/blog/4-ai-powered-cyber-threats [https://perma.cc/8ZTX-C4L8].

[18] *E.g.*, Marco Sassòli, *The Role of Human Rights and International Humanitarian Law in New Types of Armed Conflicts*, *in* INTERNATIONAL HUMANITARIAN LAW AND INTERNATIONAL HUMAN RIGHTS LAW 34, 47 (Orna Ben-Naftali ed., 2011).

[19] *What is the Difference Between IHL and Human Rights Law?*, INT'L COMM. RED CROSS (Jan. 22, 2015) https://www.icrc.org/en/document/what-difference-between-ihl-and-human-rights-law [https://perma.cc/2BBU-GGEK].

[20] Sassòli, *supra* note 18, at 50–51.

[21] *Id.*

[22] For scenarios where IHL is applied to AI-powered cyber operations, see *Artificial Intelligence and Machine Learning in Armed Conflict: A Human-Centred Approach*, INT'L COMM. RED CROSS (June 6, 2019) https://www.icrc.org/en/document/artificial-intelligence-and-machine-learning-armed-conflict-human-centred-approach [https://perma.cc/244S-9CB5]. For scenarios where IHRL is applied to AI-powered cyber operations, see Jootaek Lee, *Artificial Intelligence and Human Rights: Four Realms of Discussion, Research and Annotated Bibliography*, 1 RUTGERS INT'L L. & HUM. RTS. J. 201, 210–12 (2021).

and data protection.[23] With this said, the Framework Convention, which aims to ensure that activities within the lifecycle of AI systems are fully consistent with human rights, democracy, and the rule of law, has become the first-ever international treaty in this field.[24] Opened for signature in September 2024, the Framework Convention has 17 signatories so far.[25] Undeniably, a treaty like this represents a certain degree of integration regarding the issue within a particular region, but it can also pose barriers to the globalization of the regime due to regionalism. We still need to wait and see whether such a novel treaty will gain adequate popularity to eventually become influential on a global scale.

B. *International Soft Law*

In addition to international hard law, we also have international soft law. Sources of international soft law mainly include guidelines, declarations, codes of conduct, etc.[26] Compared with hard law, soft law is usually more favored as it is easier to negotiate.[27] Consequently, AI will be primarily governed by soft law for the immediate future.[28] The latest developments of international soft law regarding AI and cybersecurity include, for instance, the OECD Principles on AI, which serve as the first intergovernmental standard on AI;[29] the G7 AI Principles and Code of Conduct, which aim to promote the safety and trustworthiness of AI systems;[30] the ISO 42001, which is a pivotal standard for AI management systems, etc.[31] Nonetheless, the voluntary nature of soft law acts as both a strength and a weakness in governing AI.[32] Despite the flexibility, international soft law is legally non-binding; therefore, there will be a lack of

---

[23] *See* Shackelford & Dockery, *supra* note 2, at 300–14.

[24] *The Framework Convention on Artificial Intelligence*, COUNCIL EUR., https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence [https://perma.cc/XWT4-YDXV] (last visited Feb. 26, 2026, at 12:17 ET).

[25] *Id.*

[26] Raj Bhala & Cody N. Wood, *Two-Dimensional Hard-Soft Law Theory and the Advancement of Women's and LGBTQ+ Rights through Free Trade Agreements*, 47 GA. J. INT'L & COMPAR. L. 299, 321 (2019) (citing *Soft Law*, BLACK'S LAW DICTIONARY (9th ed. 2009)).

[27] Pronto, *supra* note 10, at 945.

[28] Gary E. Marchant & Carlos Ignacio Gutierrez, *Soft Law 2.0: An Agile and Effective Governance Approach for Artificial Intelligence*, 24 MINN. J.L. SCI. & TECH. 375, 375 (2023).

[29] *See AI Principles*, OECD, https://www.oecd.org/en/topics/sub-issues/ai-principles.html [https://perma.cc/TLA6-UZ5M] (last visited Feb. 26, 2026, at 12:29 ET).

[30] *See* G7 HIROSHIMA SUMMIT, HIROSHIMA PROCESS INTERNATIONAL GUIDING PRINCIPLES FOR ORGANIZATIONS DEVELOPING ADVANCED AI SYSTEM 1–2 (2023), https://www.mofa.go.jp/files/100573471.pdf [https://perma.cc/38PB-XKNY]]; *see also* G7 HIROSHIMA SUMMIT, HIROSHIMA PROCESS INTERNATIONAL CODE OF CONDUCT FOR ORGANIZATIONS DEVELOPING ADVANCED AI SYSTEMS 1–2 (2023), https://www.soumu.go.jp/hiroshimaaiprocess/pdf/document05_en.pdf [https://perma.cc/CM69-K6WR].

[31] *See* Int'l Org. for Standardization & Int'l Electrotech. Comm'n, *Information Technology — Artificial Intelligence — Management System (ISO/IEC 42001:2023)*, ISO ONLINE BROWSING PLATFORM, https://www.iso.org/obp/ui/en/#iso:std:iso-iec:42001:ed-1:v1:en [https://perma.cc/KHL7-8R9R] (last visited Feb. 15, 2026, at 19:32 ET).

[32] Marchant & Gutierrez, *supra* note 28, at 401.

enforceability.[33] Indeed, soft law could be the basis for hard law,[34] but it can take quite some time to turn soft law into hard law (if ever possible). Before that happens, international soft law will remain unenforceable and need the voluntary compliance of the states and other actors.

III. THE PROPOSAL OF A MULTILAYERED SYSTEM FOR GAP-FILLING

The pitfalls of the existing legal frameworks governing AI-powered cyber operations call for a specifically tailored framework to bridge these gaps. This new framework needs to meet all of the following requirements simultaneously: first, it should be able to govern less serious violations of international law; second, it must cover non-human rights breaches of international law; third, it is supposed to have global applicability; finally, it must be legally binding and enforceable under international law. These requirements remind us to explore the sections of international law that are outside of the previously mentioned analytical models, particularly at those established principles that are significantly relevant here but have been neglected.[35] As a result, the principle of the prohibition of the use of force, the principle of non-intervention, and the principle of sovereignty can jointly serve as the three primary pillars for regulating AI-driven cyber operations. This Section aims to provide a threefold introduction to this newly proposed multilayered system, respectively focusing on the structure, components, and operation of the system.

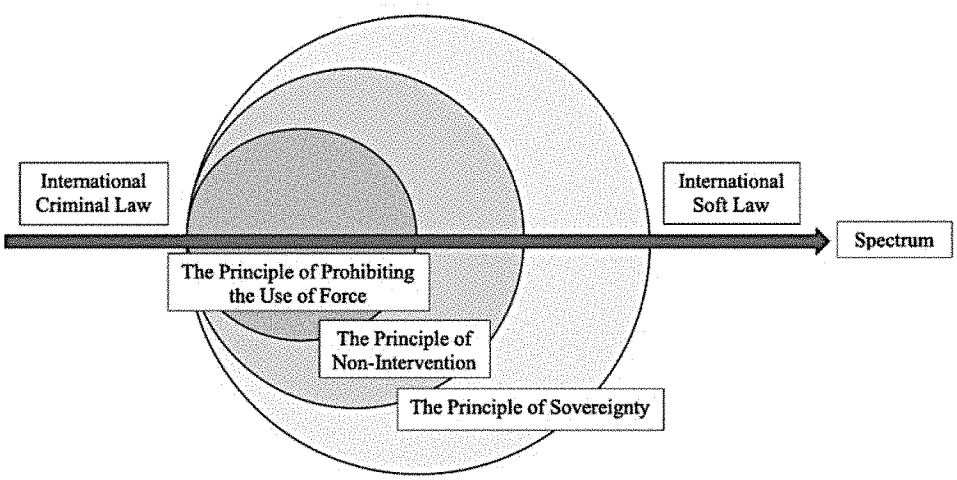
A. *Structure of the System*

---

[33] *See* Andrew T. Guzman & Timothy L. Meyer, *International Soft Law*, 2 J. LEGAL ANALYSIS 171, 176 (2010).

[34] *See* Gregory C. Shaffer & Mark A. Pollack, *Hard Versus Soft Law in International Security*, 52 B.C. L. REV. 1147, 1165 (2011) (citing Kenneth Abbott & Duncan Snidal, *Pathways to International Cooperation*, *in* THE IMPACT OF INTERNATIONAL LAW ON INTERNATIONAL COOPERATION 50, 59–60 (Eyal Benvenisti & Moshe Hirsch eds., 2004)); *see also* Susan Block-Lieb, *Soft and Hard Strategies: The Role of Business in the Crafting of International Commercial Law*, 40 MICH. J. INT'L L. 433, 434 (2019) (citing Charles Lipson, *Why Are Some International Agreements Informal?*, 45 INT'L ORG. 495, 508–13 (1991)).

[35] Some former discussions have been either skeptical about the significance of the existing international norms in governing AI-driven cyber operations or have more or less omitted the established principles of international law while applying the current international law to the AI-related cyber sphere. *See, e.g.*, Maas, *supra* note 6, at 38–43; Burri, *supra* note 6, at 101–07; LEE, *supra* note 8, at 84–90.



This diagram illustrates the proposal of a comprehensive system for the regulation of AI-enabled cyber operations under international law. Within the given spectrum, the use of weaponized AI for cyberattacks amounting to the gravest breaches of international law will be at one extreme, falling within the sphere of ICL. The AI-based cyber activities governed by legally non-binding rules will be at the other extreme, falling within the area of international soft law. The majority of AI-powered cyber operations, however, are more likely to fall in between, where the principle of prohibiting the use of force, the principle of non-intervention, and the principle of sovereignty will be able to play their roles.[36]

The principle of prohibiting the use of force and the principle of non-intervention both derive from and are attached to the principle of sovereignty, but they are also separated from each other.[37] As shown in the diagram, the application scope of the principle of prohibiting the use of force is narrower than the principle of non-intervention,[38] and the application scope of the principle of

---

[36] The boundary between ICL and the three principles is essentially the border of crime of aggression and the principle of non-use of force. *See* OPPENHEIM'S INTERNATIONAL LAW 429 (Robert Jennings & Arthur Watts eds., 9th ed. 2008) ("If the use of armed force is of sufficient gravity, it may also constitute aggression."). The 2010 Kampala Review Conference reached a consensus that an act of aggression is the prohibited use of force that constitutes a "manifest violation" of the U.N. Charter in contrast to the less serious illegal use of force. *See* Jennifer Trahan, *A Meaningful Definition of the Crime of Aggression: A Response to Michael Glennon*, 33 U. PA. J. INT'L L. 907, 936 (2012). The Rome Statute of the International Criminal Court Article 8 *bis* further enumerates seven acts that qualify as an act of aggression. Rome Statute of the International Criminal Court, art. 8 *bis*, July 17, 1998, 2187 U.N.T.S. 90.

[37] Russell Buchan & Nicholas Tsagourias, *The Crisis in Crimea and the Principle of Non-Intervention*, 19 INT'L CMTY. L. REV. 165, 173 (2017).

[38] *See* OPPENHEIM'S INTERNATIONAL LAW, *supra* note 36, at 428 ("Where intervention involves the use of armed force it is likely additionally, to violate Article 2(4) of the Charter of the United Nations.").

non-intervention is narrower than the principle of sovereignty.[39] Concerning severity, the acts governed by the principle of prohibiting the use of force are usually graver than those governed by the non-intervention principle,[40] and the acts governed by the principle of non-intervention are graver than the acts in violation of the principle of sovereignty.[41]

B. *Components of the System*

Before diving into the intersections of the three principles, each should be addressed individually. Concerning the prohibition of the use of force, this principle is mainly embodied in Article 2(4) of the U.N. Charter.[42] Meanwhile, the principle of the prohibited use of force is also a norm of customary international law as both the *opinio juris* ("opinion of law") and the state practices indicate the customary law nature of the principle.[43] The key elements of the principle of prohibited use of force are: first, there is the use of armed force (or in other words, armed attack);[44] second, this armed attack must have direct physical effects;[45] and third, such an armed attack can be attributed to a state.[46]

With regard to the principle of non-intervention, Article 2(7) of the U.N. Charter is an embodiment of this principle, and Article 41 of the Vienna Convention on Diplomatic Relations reaffirms this principle.[47] This principle is an international custom as well.[48] Generally, the non-intervention principle has three key elements. The first element is the existence of an "intervention," which certainly includes acts amounting to force, but may also include acts in other

---

[39] *See* Harriet Moynihan, *The Application of International Law to Cyberspace: Sovereignty and Non-Intervention*, JUST SEC. (Dec. 13, 2019), https://www.justsecurity.org/67723/the-application-of-international-law-to-cyberspace-sovereignty-and-non-intervention [https://perma.cc/S5RN-28YF] ("The sovereignty principle is closely linked to the prohibition on non-intervention, but without the requirement of coercion.").

[40] *See* OPPENHEIM'S INTERNATIONAL LAW, *supra* note 36.

[41] *See* Moynihan, *supra* note 39.

[42] Article 2(4) of the U.N. Charter requires the U.N. Members to refrain from "the threat or use of force against the territorial integrity or political independence of any State." U.N. Charter art. 2, ¶ 4.

[43] *See* Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUM. J. TRANSNAT'L L. 885, 920 (1999).

[44] Yuan Fang, *Is the Current International Law a Good Fit for Cybersecurity? A U.N. Charter-Based Analysis*, 20 WASH. U. GLOB. STUD. L. REV. 549, 552 (2021) (citing G.A. Res. 3314 (XXIX), Definition of Aggression (Dec. 14, 1974)).

[45] Schmitt, *supra* note 43, at 929.

[46] Fang, *supra* note 44, at 555–58.

[47] Article 2(7) of the U.N. Charter prohibits the acts to "intervene in matters which are essentially within the domestic jurisdiction of any state." U.N. Charter art. 2, ¶ 7. Article 41(1) of the Vienna Convention on Diplomatic Relations stipulates that all persons enjoying privileges and immunities shall "respect the laws and regulations of the receiving State" and "not . . . interfere in the internal affairs of that State." Vienna Convention on Diplomatic Relations, art. 41, ¶ 1, Apr. 18, 1961, 500 U.N.T.S. 95.

[48] *See* G.A. Res. 37/10 (Nov. 15, 1982); G.A. Res. 2625 (XXV) (Oct. 24, 1970).

forms.[49] The second element is that the purpose of the intervention is to interfere with the internal or external affairs of the state.[50] Internal affairs comprise the matters in principle not regulated by international law,[51] concerning the relations between a state and its citizens or national territory;[52] external affairs refer to the relations that a state has with other states and international organizations.[53] The third and last element of the principle of non-intervention is, the act of intervention can be attributed to a state.[54]

In terms of the principle of sovereignty, it is a "fundamental principle of international law and is considered a 'basic constitutional doctrine of the law of nations'".[55] This principle is primarily reflected in Article 2(1) and Article 78 of the U.N. Charter,[56] and it is also a part of international customs.[57] In addition, to be considered a violation of sovereignty, an act must be: first, against the territorial integrity or political independence of the state; and second, attributable to a state.[58]

C. *Operation of the System*

Furthermore, the determination of the principle or principles that are breached depends on how to precisely identify the differences between these overlapping principles. As shown above, the elements of all three principles are composed of the nature of the act, the effects of the act, and implicitly the linkage between the act and its effects. Attribution is another pivotal component in

---

[49] *See* Maziar Jamnejad & Michael Wood, *The Principle of Non-Intervention*, 22 LEIDEN J. INT'L L. 345, 348 (2009) (citing G.A. Res. 2625 (XXV) (Oct. 24, 1970)).

[50] Marcelo Kohen, *The Principle of Non-Intervention 25 Years After the Nicaragua Judgment*, 25 LEIDEN J. INT'L L. 157, 158–59 (2012).

[51] Nationality Decrees Issued in Tunis and Morocco (French Zone), Advisory Opinion, 1923 P.C.I.J. (ser. B) No. 4, at 24 (Nov. 8).

[52] MARCO ROSCINI, INTERNATIONAL LAW AND THE PRINCIPLE OF NON-INTERVENTION: HISTORY, THEORY, AND INTERACTIONS WITH OTHER PRINCIPLES 162 (2024).

[53] *Id.*

[54] Jamnejad & Wood, *supra* note 49, at 371.

[55] Gary P. Corn & Robert Taylor, *Sovereignty in the Age of Cyber*, 111 AJIL UNBOUND 207, 209 (2017).

[56] Article 2(1) of the U.N. Charter states that the U.N "is based on the principle of the sovereign equality of all its Members." U.N. Charter art. 2, ¶ 1. Article 78 of the U.N. Charter restates that relationship among U.N. Members "shall be based on respect for the principle of sovereign equality." U.N. Charter art. 78.

[57] Some doubt the assertion that the principle of sovereignty operates as an independent rule of customary international law. *Contra* Corn & Taylor, *supra* note 55, at 208; *but see* Michael Schmitt, *US Transparency Regarding International Law in Cyberspace*, JUST SEC. (Nov. 15, 2016), https://www.justsecurity.org/34465/transparency-international-law-cyberspace [https://perma.cc/KYG6-78ZJ] (assuming the principle of sovereignty is still a rule of international law that can be violated).

[58] *See* Corn & Taylor, *supra* note 55, at 209–10.

addition to these elements. Despite the importance of the attribution issue,[59] this Section will concentrate on the act itself, specifically, prohibited use of force, illegal intervention, and violation of sovereignty.[60] To be more specific, the Paper will dive deep into the nature of these acts.

First, how can we distinguish between prohibited use of force and illegal intervention? To answer this, we have to first know about their similarities. Coercion is a common element of prohibited use of force and illegal intervention.[61] The notion of "coercion" can be formulated in the following way: 1) A wants B to do something and wants to be certain that this will happen; 2) A then takes some action to get B to do that something, either by uttering a coercive threat, using coercive force, or engaging in coercive manipulation; 3) due to A's actions, B does that something.[62] Putting it shortly, coercion means "the application of various kinds of pressure including but not limited to threats, intimidation, and the use of force to compel one State to think or act in a certain way."[63] The main distinction between these two acts, however, is the level of coercion involved. [64] Prohibited use of force solely encompasses military coercion, [65] whereas illegal intervention could contain both military and nonmilitary coercion.[66] Second, how do we differentiate illegal intervention from

---

[59] For discussions in relation to attribution, see generally Kristen E. Eichensehr, *The Law and Politics of Cyberattack Attribution*, 67 UCLA L. REV. 520 (2020) (arguing that when cyberattacks are publicly attributed to states, such attributions should be governed by legal standards); Delbert Tran, *The Law of Attribution: Rules for Attributing the Source of a Cyber-Attack*, 20 YALE J.L. & TECH 376 (2018) (suggesting that a legal approach, rather than a technological one, can solve the attribution problem); Herbert Lin, *Attribution of Malicious Cyber Incidents: From Soup to Nuts*, 70 COLUM. J. INT'L AFFS. 75 (2016) (emphasizing the distinction between attribution of malicious cyber activity to a machine, to a specific perpetrator initiating that activity, and to an adversary that is deemed ultimately responsible for that activity).

[60] The reason for using "prohibited" use of force in lieu of "use of force" here is that there are at least two types of use of force that are not prohibited. The first type is the right of self-defense formulated in Article 51 of the U.N. Charter. The second type is the use of force authorized by the U.N. Security Council in accordance with the U.N. Charter. *See* Matthew C. Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, 36 YALE J. INT'L L. 421, 422 (2011). Similarly, the reason for using "illegal" intervention instead of simply "intervention" is that the ICJ Court in *Nicaragua* states that "[i]ntervention is wrongful when it uses methods of coercion…", which implies that an intervention might be legitimized if it does not use "methods of coercion." That is to say, consent-based intervention (*e.g.*, intervention by invitation) is generally lawful under international law. *See* Military and Paramilitary Activities In and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶ 205 (June 27) [hereinafter Nicaragua case].

[61] Arlen Printz, *Election Hacking: A Trifecta of Sovereignty, Intervention, and Use of Force Violations in International Law*, 42 LOY. L.A. INT'L & COMPAR. L. REV. 291, 310 (2019).

[62] *See* Steven Wheatley, *Foreign Interference in Elections Under the Non-Intervention Principle: We Need to Talk About "Coercion"*, 31 DUKE J. COMPAR. & INT'L L. 161, 182 (2020).

[63] Printz, *supra* note 61, at 306.

[64] Sean Watts, *Low-Intensity Cyber Operations and the Principle of Non-Intervention*, 14 BALTIC Y.B. INT'L L. 137, 149 (2014).

[65] *See* Duncan B. Hollis, *Why States Need an International Law for Information Operations*, 11 LEWIS & CLARK L. REV. 1023, 1041 (2007).

[66] *See* Watts, *supra* note 64, at 147–48 ("Acts amounting to direct threats or uses of force, particularly armed force…constitute the clearest examples of coercion sufficient to establish illegal intervention." "To qualify as coercion for purposes of the principle of non-intervention, the acts of a State need not involve physical coercion or force.")

a violation of sovereignty? There are two main components of the concept of intervention: coercion and sovereignty.[67] Coercion is a premise of illegal intervention,[68] but is not required for a violation of sovereignty.[69]

This clarification gives us a better understanding of why prohibited use of force is narrower and graver than illegal intervention and illegal intervention is narrower and graver than violation of sovereignty, because they interact with the notion of coercion in different ways. The combination of the three principles will assist in filling the gaps between international criminal law and international soft law with regard to the governance of AI-powered cyber operations.

IV. THE APPLICATION OF THE MULTILAYERED SYSTEM

The normative and doctrinal analyses of how these established principles might be applied to AI-enabled cyber operations will now be integrated with a series of scenario simulations reflecting the demands of real-world practice. The three scenarios provided below cover a broad array of subjects, including the AI-involved autonomous weapon systems, the AI-enabled cyber interference with elections, and the AI-assisted cyber espionage.

A. *AI–Involved Autonomous Weapon Attack*

State A has deployed Lethal Autonomous Weapon Systems ("LAWS"), which are also known as "killer robots," to locate, identify, and attack the militants of State B.[70] Unlike the drones that are usually controlled individually by remote operators, the drones used by State A consist of coordinated systems of potentially thousands of drones that can perform missions autonomously with minimal human oversight.[71] These combat drone swarms are single networked entities flying themselves and using AI to navigate obstacles like GPS jamming, radio signal interference, and adverse environmental conditions.[72]

The first question to ask while applying the multilayer system to this given scenario is, does the use of combat drone swarms probably constitute a prohibited use of force? Some might be more skeptical, arguing that autonomous

---

[67] Buchan & Tsagourias, *supra* note 37, at 171.

[68] *See* Nicaragua case, *supra* note 60 ("The element of coercion . . . defines, and indeed forms the very essence of, prohibited intervention.").

[69] *See* Moynihan, *supra* note 39.

[70] David Hambling, *Israel Used World's First AI-Guided Combat Drone Swarm in Gaza Attacks*, NEW SCIENTIST (June 30, 2021), https://www.newscientist.com/article/2282656-israel-used-worlds-first-ai-guided-combat-drone-swarm-in-gaza-attacks [https://perma.cc/JQ68-3EF7].

[71] Aja Melville, *Drone Wars: Developments in Drone Swarm Technology*, DEF. & SEC. MONITOR (Jan. 21, 2025), https://dsm.forecastinternational.com/2025/01/21/drone-wars-developments-in-drone-swarm-technology [https://perma.cc/H62L-X3GQ].

[72] *Id.*

weapons may help minimize civilian harm.[73] However, this will not alter the essential nature of the use of weaponized AI systems as military coercion, since any automated process, even if measurably better than human performance, cannot guarantee that the use of force is not arbitrary without human control.[74] In this sense, the use of weapon systems assisted by AI could be considered a prohibited use of force by its nature.

If the weaponization of AI systems is likely to be seen as a prohibited use of force, the follow-up question will be, is it possibly an illegal intervention? Recalling the structure of the proposed system, prohibited use of force normally sets a stricter threshold than illegal intervention in terms of the nature of the act. This suggests that an act of prohibited use of force is inherently an act of illegal intervention. In this regard, the use of AI-assisted combat drones is supposed to be an illegal intervention.

If the act of State A in this scenario is considered an illegal intervention, then is it a violation of sovereignty? Similarly, an act of illegal intervention should be inherently considered as an act of violation of sovereignty, given that the bar of illegal intervention is higher than violation of sovereignty concerning the nature of act. In summary, regardless of other factors, the use of weaponized AI is likely to be simultaneously an act of prohibited use of force, illegal intervention, and a violation of sovereignty.

B. *AI–Enabled Cyber Interference with Elections*

State A leverages AI-enabled influence operations to interfere with the elections of State B. Specifically, State A utilizes AI-generated videos, images, and audio of political candidates to make false or controversial statements, triggering State B users' uncertainty about the authenticity of the content and eroding their trust in the integrity of online sources.[75] State A also uses social bots to spread conspiracy theories and disinformation on campaign issues, security incidents, and baseless claims of election fraud, preventing specific political candidates of State B from garnering meaningful voter engagement.[76]

Does the AI-enabled influence operation impacting elections amount to a prohibited use of force? Generally, these actions are not likely to be classified as a prohibited use of force because they lack the required gravity of an armed attack. AI-powered election intervention, as shown in the scenario description

---

[73] *See, e.g.*, Michael N. Schmitt, *Autonomous Cyber Capabilities and the International Law of Sovereignty and Intervention*, 96 INT'L L. STUD. 549, 550 (2020) (citing Michael Schmitt & Jeffrey Thurner, *"Out of the Loop": Autonomous Weapon Systems and the Law of Armed Conflict*, 4 HARV. NAT'L SEC. J. 231, 233 (2013)).

[74] *See* Peter Asaro, *On Banning Autonomous Weapon Systems: Human Rights, Automation, and the Dehumanization of Lethal Decision-Making*, 94 INT'L REV. RED CROSS 687, 708 (2012); *see also* Nicholas W. Mull, *The Roboticization of Warfare with Lethal Autonomous Weapon Systems (LAWS): Mandate of Humanity or Threat to It?*, 40 HOU. J. INT'L L. 461, 529 (2018).

[75] SAM STOCKWELL ET AL., CTR. FOR EMERGING TECH. & SEC., AI-ENABLED INFLUENCE OPERATIONS: SAFEGUARDING FUTURE ELECTIONS 20–21 (2024), https://cetas.turing.ac.uk/sites/default/files/2024-11/cetas_research_report_-_ai-enabled_influence_operations_-_safeguarding_future_elections.pdf [https://perma.cc/8JBA-Z5SU].

[76] *Id.* at 24–25.

above, typically does not contain anything amounting to a military coercion, and accordingly will not be understood as an act of prohibited use of force.

Now that AI-enabled election interference is unlikely to be a prohibited use of force, is it likely to be an illegal intervention? Illegal intervention could encompass both military coercion and political/economic coercion,[77] and the key to determining whether a certain act amounts to a coercion is to look at whether it engages in coercive threat, force, or manipulation.[78] Even though State A neither threatens to use nor actually uses force, it does attempt to manipulate the public opinions of State B, which will have an impact on the election results. As a consequence, the election interference generated by AI could be political coercion, and accordingly an act of wrongful intervention.

If State A's actions in the given scenario are construed as illegal intervention, then these actions will be inherently considered as acts in violation of sovereignty as well, because a violation of sovereignty does not require the given act to have a coercive nature, whereas an illegal intervention does. As a summary, the AI-enabled election interference is not a prohibited use of force but can be an illegal intervention and a violation of sovereignty.

C. *AI–Assisted Cyber Espionage*

The hackers of State A have used AI technologies to conduct cyber espionage targeting State B. They use OpenAI's large language models to automate phishing campaigns and identify targets more efficiently, making it harder for State B to counter their cyber operations.[79] They also employ AI to analyze massive datasets to identify network vulnerabilities more effectively, enabling them to breach systems undetected and steal sensitive data.[80] By these means, State A has completed a theft of three billion dollars' worth of cryptocurrency from State B.[81]

Is the AI-enabled cyber espionage a prohibited use of force? The answer is apparently not. Instead of using armed force, State A uses much more peaceful and invisible means to reach its aim. Is the act of State A an illegal intervention? On the surface, cyber espionage aims to gain economic benefits, which is very similar to the purpose of economic coercion. Nevertheless, economic coercion requires the actions taken to be coercive, and espionage cannot meet this requirement. In this case, State A deploys AI technology to steal money from State B, so the act of theft is non-coercive. As a result, it should not be considered as an economic coercion, and therefore not an illegal intervention. Despite this,

---

[77] *See* Jamnejad & Wood, *supra* note 49.

[78] *See* Wheatley, *supra* note 62.

[79] *See* Louise Lipsker, *Artificial Intelligence and State-Sponsored Cyber Espionage: The Growing Threat of AI-Enhanced Hacking and Global Security Implications*, N.Y.U. L. J. INTELL. PROP. & ENT. L.: BLOG (Feb. 25, 2025), https://jipel.law.nyu.edu/artificial-intelligence-and-state-sponsored-cyber-espionage [https://perma.cc/XV2S-NR3T].

[80] *Id.*

[81] *Id.*

the AI-enabled cyber espionage could be an act in violation of sovereignty, since violation of sovereignty has nothing to do with coercion.

V. CONCLUDING REMARKS

The ever-changing landscape of AI has posed significant impacts on cybersecurity. The primary frameworks of international law governing the issue, including but not limited to ICL, IHL, IHRL, and international soft law, are generally ineffective at responding to the rapid evolution of AI-powered cyber operations. These frameworks have excessively stringent thresholds, an overly narrow focus on a particular issue, and difficulties enforcing the rules. To bridge these regulatory gaps, a comprehensive and multilayered system has been proposed. This novel approach proposes a combination of the principle of prohibiting the use of force, the principle of non-intervention, and the principle of sovereignty to address the challenges that stem from AI-generated cyber activities. Applying the proposed system to real-world scenarios, an AI-involved autonomous weapon attack could be construed as a prohibited use of force, an AI-enabled cyber interference with the election is possibly understood as an illegal intervention, and an AI-assisted cyber espionage might constitute a violation of sovereignty.

Looking forward, the implementation of the proposed system could be uncertain and problematic. Conventionally, the violations of the three principles may all fall within the jurisdiction of the International Court of Justice ("ICJ").[82] Although the ICJ ruling is legally binding, given that the ICJ itself lacks enforcement mechanisms, what if the state just doesn't comply with the court's judgment?[83] Theoretically, the U.N. Security Council ("UNSC") may then make recommendations or decide on the measures to be taken to enforce the judgment.[84] However, its ability to do this is limited by the veto power of the P5 (the five permanent members of the UNSC).[85] Indeed, we live in a world where international law is somehow shaped by international politics and international

---

[82] Article 36(1) of the Statute of the International Court of Justice stipulates: "The jurisdiction of the Court comprises all cases which the parties refer to it and all matters specially provided for in the Charter of the United Nations or in treaties and conventions in force." Statute of the International Court of Justice art. 36, ¶ 1.

[83] *See* Irène Couzigou, *Enforcement of UN Security Council Resolutions and of ICJ Judgments: The Unreliability of Political Enforcement Mechanisms*, *in* THE ENFORCEMENT OF EU LAW AND VALUES: ENSURING MEMBER STATES' COMPLIANCE 363, 363–64 (András Jakab & Dimitry Kochenov eds., 2017).

[84] Article 94(2) of the U.N. Charter formulates that the UNSC can do so with two prerequisites: (1) any party to a case fails to perform the obligations under an ICJ judgment; and (2) the other party has recourse to the UNSC. U.N. Charter art. 94, ¶ 2.

[85] *See* Michael J. Kelly, *United Nations Security Council Permanent Membership and the Veto Problem*, 52 CASE W. RSRV. J. INT'L L. 101, 106 (2020) ("[T]he P5's power to positively or negatively affect not only the creation of international law but also its implementation is enormous."); *but see* Aziz Tuffi Saliba, *Is the Security Council Legibus Solutus? An Analysis of the Legal Restraints of the UNSC*, 20 MICH. STATE INT'L L. REV. 401, 419 (2012) (arguing that the UNSC is subject to legal limitations deriving from the U.N. Charter, *jus cogens*, and other pertinent treaties).

relations.[86] In this context, it is necessary and important to think beyond international law as we pave the path forward for the global governance of AI-powered cyber operations and other pressing issues facing the international community in the contemporary era.

[86] For an elaborated discussion regarding the underlying rationale, namely "structural realism" and "rationalist institutionalism," see Anthony Clark Arend, *Do Legal Rules Matter? International Law and International Politics*, 38 VA. J. INT'L L. 107, 110–25 (1998).