PROTECTING STATE SOVEREIGNTY IN THE AGE OF EMERGING TECHNOLOGIES: ARTIFICIAL INTELLIGENCE AND THE UNWILLING OR UNABLE DOCTRINE

Isabelle Terranova*

Abstract

The United Nations Charter system seeks to strike a careful balance between the fundamental principles of state sovereignty, territorial integrity, and the inherent right of self-defense. This right has been interpreted, albeit controversially, to include the use of force against nonstate actors (NSAs) on the territory of a third state, without the consent of that third state, where the NSA has undertaken an armed attack against the victim state and the third state is unwilling or unable to address the threat. This application of the use of force in self-defense has come to be known as the "unwilling or unable (UoU) doctrine." This Note examines the durability of this doctrine in the age of emerging technologies. This Note uses AI as a case study and concludes that the scope of the UoU doctrine must be redefined to protect the sovereignty of states that may be unable to combat the use of emerging technologies by NSAs within their territory.

Section II begins by providing an overview of the UoU doctrine and surveying state positions on the validity of this doctrine. Section III discusses the weaponization of AI and predicts that NSAs will pursue the use of weaponized AI to carry out armed attacks. Section IV assesses the standing of the UoU doctrine in the age of emerging technologies, ultimately concluding that, without refinement, the UoU doctrine will permit unwarranted violations of state sovereignty under the guise of self-defense. Specifically, this Note predicts that applying the current UoU doctrine in the context of emerging technology will disproportionately infringe upon the sovereign rights of least-developed countries, which are most unlikely to be able to combat the use of weaponized AI by NSAs. Section V sets forth four recommendations to address the consequences of an unrestricted application of the UoU doctrine to combat the use of AI by NSAs. These suggestions include elimination of the unable element,

* Georgetown University Law Center, J.D., 2023; Boston University, B.A., 2020. I would like to extend my sincerest gratitude to Professor David Koplow for his feedback and support on this Note, which was written for his Spring 2022 Issues in Disarmament: Proliferation, Terrorism, and Great Power Rivalry Seminar. Special thanks also to the editors and staff of the Georgetown Journal of International Law for their hard work on this piece.

encouragement of a showing of greater ability, increased regulation of AI, and investment in AI defense.

I. INTRODUCTION

In 1980, the Minister of Foreign Affairs and Information of the Republic of South Africa wrote a letter to the President of the U.N. Security Council justifying "protective action" taken against aggression committed by Southwest Africa People's Organization terrorists acting from Zambian soil.[1] In 1981, the Israeli Ambassador to the United Nations, in addressing attacks against Palestinian Liberation Organization (PLO) terrorists in Lebanon, asserted that "Israel is, in fact, exercising the inherent right of self-defense enjoyed by every sovereign State, a right also preserved under Article 51 of the Charter of the United Nations. Israel's response to PLO terror is what any self-respecting sovereign State would do in similar circumstances."[2] In 1996, the Turkish Foreign Minister, in response to a letter from the Minister of Foreign Affairs of the Republic of Iraq condemning the actions of Turkish armed forces, argued that "Turkey cannot be expected to stand idle until Iraq reassumes its obligations when its territorial integrity and security are incessantly threatened

1. Minister of Foreign Affairs and Information of the Republic of South Africa, Letter dated Apr. 10, 1980, from the Permanent Rep. of South Africa to the United Nations addressed to the President of the Security Council, U.N. DOC. S/13886 (Apr. 10, 1980).

2. U.N. SCOR, 36th Sess., 2292th mtg. at ¶¶ 54-56, U.N. DOC. S/PV.2292 (July 17, 1981).

by the blatant cross-border attacks of a terrorist organization based in and operating from the Iraqi territory profiting from this power vacuum" resulting from Iraq's inability to control portions of the northern territory.[3] In 2011, the United States entered Pakistan and used lethal force against Al Qaeda leader Osama bin Laden, later reiterating that the operation was carried out under the principles the Legal Advisor for the Department of State had outlined in a previous speech.[4] One such principle was the unwilling or unable (UoU) doctrine.[5]

In fact, each of these states, whether implicitly or explicitly, invoked the UoU doctrine. They justified the use of force in self-defense against an NSA on the territory of a third state without the consent of that third state on the grounds that the third state was unwilling or unable to address the threat. However, these are historical examples dating back more than three decades. The global threat environment has evolved drastically in that time, partly in response to unprecedented technological advancements.[6] Now, emerging technologies, like artificial intelligence (AI), are becoming increasingly accessible to the public.[7] As such, it is predicted that this advanced technology "will inevitably enable nonstate actors to conduct more attacks with less manpower, less funding, and less time, while simultaneously still being effective, surgically targeted, and difficult to attribute."[8]

How then will states respond to the threats posed by NSAs employing weaponized AI? More importantly, how will the predicted difficulty in defending against AI-enabled attacks[9] impact the UoU doctrine in the

3. Minister of Foreign Affairs and Deputy Prime Minister of the Republic of Turkey, Letter dated Oct. 22, 1996, from the Permanent Rep. of Turkey to the United Nations addressed to the Security Council, U.N. DOC. A/51/550, S/1996/872 (Oct. 23, 1996).

4. Harold Hongju Koh, *The Lawfulness of the U.S. Operation Against Osama bin Laden,* OP. JURIS (May 19, 2011), http://opiniojuris.org/2011/05/19/the-lawfulness-of-the-us-operation-against-osama-bin-laden/; Harold H. Koh, Legal Adviser, U.S. Dep't of State, Keynote Address at the Annual Meeting of the American Society of International Law (Mar. 25, 2010), https://2009-2017.state.gov/s/l/releases/remarks/139119.htm; *see also* Ariane de Vogue, *Was Killing of Osama bin Laden Legal Under International Law?*, ABC NEWS (May 5, 2011, 3:50 PM), https://abcnews.go.com/Politics/osama-bin-laden-killing-legal-international-law/story?id=13538365.

5. Vogue, *supra* note 4.

6. *See generally* Warren Chin, *Technology, War, and the State: Past, Present, and Future*, 95 INT'L AFF. 765 (2019).

7. Paige Young, *Artificial Intelligence: A Non-State Actor's New Best Friend*, OVER THE HORIZON (May 1, 2019), https://othjournal.com/2019/05/01/artificial-intelligence-a-non-state-actors-new-best-friend/.

8. *Id.*

9. *See generally* MILES BRUNDAGE ET AL., THE MALICIOUS USE OF ARTIFICIAL INTELLIGENCE: FORECASTING, PREVENTION, AND MITIGATION 38 (2018).

age of emerging technologies? This Note predicts that the current UoU doctrine will permit unjustified violations of sovereignty under the guise of self-defense on the basis that territorial states, particularly least-developed countries (LDCs), will be unable to suppress threats posed by NSAs using weaponized AI from within their territory.

While Article 2 of the United Nations Charter (the Charter) reflects universal respect for the principles of sovereignty and non-interference,[10] Article 51 provides for the conflicting right to use force in self-defense.[11] This right is merely an exception to those foundational principles of sovereignty and non-interference; as such, states must not employ the UoU doctrine to extend the right to use force in self-defense beyond the Charter's original intent. Though states should not be foreclosed from defending against AI-enabled attacks by NSAs acting from within the territory of another state, they must not be permitted to violate state sovereignty every time a territorial state is unable to combat that novel threat. Such permission would disproportionately infringe upon the sovereign rights of LDCs, who are most unlikely to be able to combat the use of weaponized AI by NSAs, undercutting the foundational principles of the Charter system. Therefore, the scope of the UoU doctrine must be redefined to protect the sovereignty of states that may be unable to combat the use of emerging technologies, such as weaponized AI, by NSAs within their territory.

This Note begins in Section II by providing an overview of the UoU doctrine. After discussion of the *jus ad bellum* regime and the use of force in self-defense generally, the section explores the origins of the UoU doctrine. Through a case study on the use of force against the Islamic State of Iraq and the Levant (ISIL) in Syria, the Note surveys state positions on the validity of the UoU doctrine.

Section III will discuss the present and future weaponization of AI and the associated implications for global security. Of primary concern for this Note is the likelihood that NSAs will pursue the use of weaponized AI to carry out armed attacks.

The Note will then assess the standing of the UoU doctrine in the age of emerging technologies. Section IV will also describe the offense-defense gap, which may leave states, most likely LDCs, unable to prevent the use of their territory for AI-enabled attacks against other states. Finally, this section will suggest that, without refinement, the UoU doctrine will permit unwarranted violations of state sovereignty and territorial integrity under the guise of self-defense.

10. U.N. Charter art. 2.

11. *Id.* art. 51.

On that basis, Section V will propose that it is necessary to limit the application of the UoU doctrine in the context of AI and other emerging technologies. Namely, the section will set forth four recommendations to address the consequences of an unrestricted application of the UoU doctrine to combat the use of AI by NSAs; these suggestions include the elimination of the "unable" element, encouragement of a showing of greater ability, increased regulation of AI, and investment in AI defense. Ultimately, while each recommendation would play an important role in addressing the challenges associated with the application of the UoU doctrine in the age of emerging technologies, the elimination of the "unable" element strikes the strongest balance between the competing interests of protecting state sovereignty and safeguarding the right to self-defense.

II. Self-Defense and the UoU Doctrine

A. *Use of Force in Self-Defense*

Arising from the devastation of World War II, the modern *jus ad bellum* regime is predicated on the general prohibition on the use of force.[12] Article 2(4) of the Charter requires that states "shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state."[13] While Article 2(4) imposes a general prohibition on the use of force, this restriction is not absolute. A state may use force in another state's territory pursuant to three distinct exceptions:[14] when the territorial state

12. Craig Martin, *Challenging and Refining the "Unwilling or Unable" Doctrine*, 52 Vand. J. Transnat'l L. 387, 395 (2019); s*ee generally What Are Jus ad Bellum and Jus in Bello?*, International Committee of Red Cross (Jan. 22, 2015), https://www.icrc.org/en/document/what-are-jus-ad-bellum-and-jus-bello-0 (contrasting *jus ad bellum*, the body of international law governing "the conditions under which States may resort to war or to the use of armed force in general", with *jus in bello*, the body of international law "regulat[ing] the conduct of parties engaged in an armed conflict.").

13. U.N. Charter art. 2, ¶ 4.

14. *See generally* White House, Report on the Legal and Policy Frameworks Guiding the United States' Use of Military Force and Related National Security Operations (2016) [hereinafter Use of Force Report]. The question of whether there is a right to use force in another state's territory, absent consent or authorization from the Security Council, to prevent an extraordinary humanitarian emergency or protect fundamental human rights is not within the scope of this Note. *See generally* Peter Tzeng, *Humanitarian Intervention at the Margins: An Examination of Recent Incident*s, 50 Vand. J. Transnat'l L. 415 (2017) (examining seven events to suggest that the doctrine of humanitarian intervention is not a norm of international law, but functions to expand the scope of traditional exceptions to the prohibition on the use of force).

has given consent;[15] when the Security Council has authorized the use of force under Chapter VII of the Charter;[16] and when acting in self-defense.[17] The latter exception enables states to respond with force "if an armed attack occurs against a Member of the United Nations."[18]

The Charter's articulation of this right raises several questions about when a state may use force in self-defense. Although the text of the Charter implies that an attack must have already occurred, it is widely recognized that the imminent threat of an armed attack also triggers the right to use force in self-defense.[19] While the scope of imminence is debated, scholars rightfully recognize that "the concept of what constitutes an 'imminent' armed attack will develop to meet new circumstances and new threats."[20] One new threat to which the concept of imminence will have to adapt is that of emerging technologies, including AI. Even more contentious is the definition of an "armed attack."[21] Whatever the true meaning of this term may be under international law is beyond the scope of this Note; henceforth, this Note will use the term "armed attack" to refer to attacks that most states agree would trigger the right to use force in self-defense.[22]

---

15. *See* USE OF FORCE REPORT, *supra* note 14, at 11.

16. U.N. Charter art. 42.

17. *Id.* art. 51.

18. *Id.*

19. *See e.g.,* Derek Bowett, *Reprisals Involving Recourse to Armed Force*, 66 AM. J. INT'L L. 1, 4 (1972) ("It was never the intention of the Charter to prohibit anticipatory self-defense and the traditional right certainly existed in relation to an 'imminent' attack."); Oscar Schachter, *The Right of States to Use Armed Force*, 82 MICH. L. REV. 1620, 1634 (1984) (asserting that it is "not implausible to interpret article 51 as leaving unimpaired the right of self-defense as it existed prior to the Charter").

20. Daniel Bethlehem, *Principles Relevant to the Scope of a State's Right of Self-Defense Against an Imminent or Actual Armed Attack by Nonstate Actors*, 106 AM. J. INT'L L. 769, 772 (2012).

21. *See generally* Erin L. Guruli, *The Terrorism Era: Should the International Community Redefine Its Legal Standards on Use of Force in Self-Defense?*, 12 WILLAMETTE J. INT'L L. & DISP. RESOL. 100 (2004); Molly McNab & Megan Matthews, *Clarifying the Law Relating to Unmanned Drones and the Use of Force: The Relationships Between Human Rights, Self-Defense, Armed Conflict, and International Humanitarian Law*, 39 DENV. J. INT'L L. & POL'Y 661 (2011); Thomas Eaton, *Self-Defense to Cyber Force: Combatting the Notion of "Scale and Effect'*, 36 AM. U. INT'L L. REV. 697 (2021); Laurie R. Blank, *Irreconcilable Differences: The Thresholds for Armed Attack and International Armed Conflict*, 96 NOTRE DAME L. REV. 249 (2020).

22. Some examples of attacks that most agree would trigger the use of force in self defense include the deploying of regular armed forces or irregular militias across borders, bombardment or kinetic attacks having a major effect, or cyber or non-kinetic effects causing significant damage to property, resulting in serious injury to persons, or killing a number of persons. *See* Blank, *supra* note 21, at 255-256.

Some have interpreted the inherent right of self-defense to include the use of force in self-defense against NSAs on the territory of a third state, without the consent of that third state, where the NSA has undertaken an armed attack against the victim state and the third state is unwilling or unable to address the threat.[23] This application of the use of force in self-defense is referred to as the UoU doctrine. The durability of this doctrine in the age of emerging technologies, namely AI, will be the central focus of this Note.

Taking a forward-looking approach, this Note will primarily discuss the "unable" element of the UoU doctrine, as this factor will be impacted most significantly by the emergence of new technologies. Some factors that have been considered in the determination of a state's "ability" include: "fulfillment of due diligence obligations by the host state to prevent the use of its territory for subversive activities by NSAs; a pattern of frequent border conflicts with NSAs from the territory of the host state; response to prior subversive activities of NSAs by the host state . . .; and, the international reputation of the host state in terms of general compliance with international law and UN obligations." [24] Additionally, "inability" may be demonstrated if a host state has "deficient resources to effectively deal with NSAs."[25] This factor is particularly significant in the context of emerging technologies, including weaponized AI, as states will likely find themselves with "deficient

23. Elena Chachko & Ashley S. Deeks, *Which States Support the Unwilling and Unable Test*, LAWFARE (Oct. 10, 2016, 1:55 PM), https://www.lawfareblog.com/which-states-support-unwilling-and-unable-test; *see generally* Ashley S. Deeks, *"Unwilling or Unable": Toward a Normative Framework for Extraterritorial Self-Defense*, 52 VA. J. INT'L. L. 483, 487 (2012); Jutta Brunnée & Stephen J. Toope, *Self-Defence Against Non-State Actors: Are Powerful States Willing but Unable to Change International Law?*, 67 INT'L. & COMP. L. Q. 263, 264 (2018); José Luis Aragón Cardiel et al., *Modern Self-Defense: The Use of Force Against Non-Military Threats*, 49 COLUM. HUM. RTS. L. REV. 99, 119-20 (2018).

24. Yagnesh Sharma & Pranav Agarwal, *Dealing With Non-State Actors In International Law: The "Unwilling And Unable Doctrine"*, THE FLETCHER F. OF WORLD AFF. (May 9, 2020), http://www.fletcherforum.org/the-rostrum/2020/5/9/dealing-with-non-state-actors-in-international-law-the-unwilling-and-unable-doctrine; s*ee also* Irene Couzigou, *The Right to Self-Defence Against Non-State Actors: Criteria of the 'Unwilling or Unable' Test*, 77 HEIDELBERG J. INT'L L. 53, 54 (2017) ("In order to assess whether a State respects its obligation of conduct in addressing armed attacks from the area under its jurisdiction, the victim State should check: whether there has been a continuous pattern of armed attacks; whether the State criminalises the com- mission of armed attacks; whether the State conducts detailed investigations into those attacks; whether the State arrests, prosecutes, or extradites the authors of those attacks; whether the State complies with United Nations (UN) Security Council resolutions, if any, that sanction the authors of those attacks. A careful assessment of all these facts is needed before any determination can be made as to the 'inability' of the territorial State.").

25. Sharma & Agarwal, *supra* note 24.

resources" to combat AI systems, a fact which will be further discussed in *Section IV*. However, any discussion of the future of the UoU doctrine must be informed by the doctrine's history and its current standing in international law.

B. *Development of the UoU Doctrine*

To understand contemporary invocations of the UoU doctrine for the use of force in self-defense, it is first necessary to examine the doctrine's historical roots. Ashley Deeks authored the leading article on the development of the doctrine, which lays out the theoretical and historical origins in great detail.[26] Deeks identifies the law of neutrality, articulated by several 1907 Hague Conventions and customary international law, as the foundation for the UoU doctrine in international law.[27] At its most basic, neutrality law "defines the legal relationship between nations engaged in an armed conflict (belligerents) and nations not taking part in hostilities (neutrals)."[28] This legal relationship imposes the duty on neutral nations to "prevent the use of its territory as a place of sanctuary or a base of operations by belligerent forces of any side."[29] If the neutral nation is unwilling or unable to fulfill this duty, a belligerent is permitted to counter the activities of enemy forces acting from within the neutral nation.[30] Belligerents may also use force in self-defense "when attacked or threatened with attack while *in* neutral territory or when attacked or threatened *from* neutral territory."[31] In sum, neutrality law permits a belligerent state to use force on a neutral state's territory if the latter is *unwilling or unable* to prevent violations of its neutrality.[32]

However, the law of neutrality is limited to international conflict between states; as such, it does not provide a clear legal basis supporting the use of extraterritorial force against NSAs.[33] Nonetheless, the UoU doctrine has repeatedly been used to justify action against NSAs acting

26. Deeks, *supra* note 23.

27. *Id.* at 497.

28. U.S. NAVAL WAR COLL., ANNOTATED SUPPLEMENT TO THE COMMANDER'S HANDBOOK ON THE LAW OF NAVAL OPERATIONS 365 (A.R. Thomas & James C. Duncan eds., 1997), https://permanent.fdlp.gov/gpo3917/Naval-War-College-vol-73.pdf.

29. *Id.* at 370-71.

30. *Id.*

31. *Id.* at 371 (emphasis added).

32. Deeks, *supra* note 23, at 499; *see also* José Luis Aragón Cardiel, et al., *supra* note 23, at 120.

33. *See* Deeks, *supra* note 23, at 502-03; José Luis Aragón Cardiel, et al., *supra* note 23, at 120.

from within the territory of another state.[34] The famous *Caroline* incident of 1837, in which Britain used force within the territory of the United States against Canadian rebels and American supporters, is an early example of the application to NSAs.[35] Roughly five years after the incident, in an exchange of diplomatic notes, Lord Ashburton, the British Foreign Secretary, justified the attack on the grounds of self-defense, arguing that the United States had been unwilling or unable to prevent the rebels from conducting attacks against British Canada:[36]

> Remonstrances, wholly ineffectual were made; so ineffectual indeed that a Militia regiment, stationed on the neighbouring American island, looked on without any attempt at interference, while shots were fired from the American island itself. . . . How long could a Government, having the paramount duty of protecting its own people be reasonably expected to wait for what they had then no reason to expect?[37]

Although the *Caroline* incident predated the drafting of the Charter, Lord Ashburton's reasoning is reminiscent of the Article 51 right to self-defense, which serves as the primary legal authority on which states base the UoU doctrine's application to NSAs.[38] Unsurprisingly, the use

---

34. *See* Martin, *supra* note 12, at 402-03 (noting that the application of the doctrine to non-state actors predates the late twentieth century).

35. *Id.* at 403.

36. Letters between Daniel Webster, U.S. Sec'y State, and Lord Ashburton, U.K. Foreign Sec'y (July, 1842) http://avalon.law.yale.edu/19th_century/br-1842d.asp [hereinafter Letters between Daniel Webster and Lord Ashburton]; *see also* Abraham D. Sofaer, *On the Necessity of Preemption*, 14 EUR. J. INT'L L. 209, 214-17 (2003).

37. Letters between Daniel Webster and Lord Ashburton, *supra* note 36.

38. *See e.g.,* Permanent Rep. of Australia to the U.N., Letter dated Sept. 9, 2015 from the Permanent Rep. of Australia to the United Nations addressed to the President of the Security Council, U.N. Doc. S/2015/693 (Sept. 9, 2015) ("Article 51 of the Charter of the United Nations recognizes the inherent right of States to act in individual or collective self-defence where an armed attack occurs against a Member of the United Nations. States must be able to act in self-defence when the Government of the State where the threat is located is unwilling or unable to prevent attacks originating from its territory."); Chargé d'affaires a.i. of the Permanent Mission of Turkey to the U.N., Letter dated July 24, 2015 from the Chargé d'affaires a.i. of the Permanent Mission of Turkey to the United Nations addressed to the President of the Security Council, U.N. Doc. S/2015/563 (July 24, 2015) ("It is apparent that the regime in Syria is neither capable of nor willing to prevent these threats emanating from its territory, which clearly imperil the security of Turkey and the safety of its nationals. Individual and collective self-defence is our inherent right under international law, as reflected in Article 51 of the Charter of the United Nations."); Chargé d'affaires a.i. of the Permanent Mission of Canada to the U.N., Letter dated Mar. 31, 2015 from the Chargé d'affaires a.i. of the Permanent Mission of Canada to the United Nations addressed to

of the doctrine in this way increased significantly in the years following the 9/11 attacks, as the United States explicitly invoked the doctrine to justify the increased use of force against terrorist organizations on the territory of nonconsenting territorial states.[39] While remaining controversial, the principle has gained prominence through a growing body of scholarship and commentary[40] and through increased incorporation into state practice, which will be explored in subsection C.

C. *Contemporary Applications of the UoU Doctrine*

To accurately assess the role that the UoU doctrine may play in the future, it is first necessary to comprehend its current status. This subsection will provide a broad overview of state positions on the doctrine, officially articulated and implied through practice. Though state opinions vary widely, both proponents and objectors consistently cite the same principles of international law to support their arguments; while advocates invoke the right to self-defense,[41] critics cite the principles of sovereignty, territorial integrity, and political independence as the basis for their opposition.[42]

---

the President of the Security Council, U.N. Doc. S/2015/221 (Mar. 31, 2015) ("In accordance with the inherent rights of individual and collective self-defence reflected in Article 51 of the United Nations Charter, States must be able to act in self-defence when the Government of the State where a threat is located is unwilling or unable to prevent attacks emanating from its territory."); Permanent Rep. of the United States of America to the U.N., Letter dated Sept. 23, 2014 from the Permanent Rep. of the United States to the United Nations addressed to the Secretary-General, U.N. Doc. S/2014/695 (Sept. 23, 2014) [hereinafter Permanent Rep. of the U.S. to the U.N.] ("States must be able to defend themselves, in accordance with the inherent right of individual and collective self-defence, as reflected in Article 51 of the Charter of the United Nations, when, as is the case here, the government of the State where the threat is located is unwilling or unable to prevent the use of its territory for such attacks."); s*ee generally* U.N. Charter art. 51.

39. Martin, *supra* note 12, at 404.

40. *Id.* at 404-406.

41. *See e.g.,* Permanent Rep. of Belgium to the U.N., Letter dated 7 June 2016 from the Permanent Representative of Belgium to the United Nations addressed to the President of the Security Council, U.N. Doc. S/2016/523 (June 7, 2016) [hereinafter Permanent Rep. of Belgium to the U.N.]; Permanent Rep. of the U.S. to the U.N., *supra* note 38.

42. *See e.g.*, U.N. SCOR, 70th Sess., 7504th mtg. at 4, U.N. Doc. S/PV.7504 (Aug. 17, 2015) (statement of Venezuelan Ambassador asserting that "We reiterate our commitment to the sovereignty, territorial integrity and political independence of the Syrian Arab Republic, in line with international law, including the Charter of the United Nations.") [hereinafter Statement of Venezuelan Ambassador]; Press Release, Human Rights Council, Human Rights Council hold urgent debate on Human Rights and humanitarian situation in Syria, U.N. Press Release Human Rights Council (Feb. 28, 2012) [hereinafter Press Release, U.N. Human Rights Council] (reporting that Cuba "rejected any attempt to undermine Syria's sovereignty and territorial

Elena Chachko and Ashley Deeks identified several general categories of state positions: explicit endorsement (states that have specifically invoked the "unwilling or unable" language in their legal justifications for use of force), implicit endorsement (states that have relied on similar justifications but have stopped short of using the "unwilling or unable" language), ambiguous cases (states that have used force against NSAs in third countries without providing a legal justification for their action and states that provided a legal justification that was not, or did not resemble, the UoU doctrine), and objectors (states that have explicitly rejected the UoU doctrine).[43]

A case study of the use of force against ISIL in Syria highlights the justifications that may land states in each one of those categories. This specific example, albeit a controversial application of the UoU doctrine,[44] provides a useful overview of recent articulations of state positions on the UoU doctrine, as coalition actions prompted states to articulate a wide range of opinions on the doctrine's validity.[45] The United States was unsurprisingly the first of several states to assert their support for the doctrine as a legal justification for intervention in Syria; it had previously invoked the UoU doctrine to justify the use of force against NSAs in the territory of a third state in numerous conflicts, becoming particularly strong proponents of the doctrine following the 9/11 attacks.[46] In the context of the coalition operations, the United States justified the use of military action to eliminate the threat posed by ISIL on the basis that Syria was unwilling and unable to do so:

> States must be able to defend themselves, in accordance with the inherent right of individual and collective self-defence, as

independence and demanded full respect for the principles of self-determination and sovereignty of this Arab nation.").

43. Chachko & Deeks, *supra* note 23. The states in the first category of explicit endorsement are the United States, United Kingdom, Germany, The Netherlands, Czech Republic, Canada, Australia, Russia, Turkey, and Israel. The states in the second category of implicit endorsement are Belgium, Iran, and South Africa. States in the third category of ambiguous cases are France, Denmark, Norway, Portugal, Members of the GCC, Egypt, Iraq, Jordan, Lebanon, Colombia, Uganda, Rwanda, Ethiopia, and India.

44. *See* Waseem Ahmad Qureshi, *International Law and the Application of the Unwilling or Unable Test in the Syrian Conflict*, 62 DREXEL L. REV. 61 (2018) (arguing "the theoretical test is inapplicable in the Syrian case, because the prerequisites set by the test itself are not met").

45. *See generally* Madeline Holmqvist Skantz, The Unwilling or Unable Doctrine: The Right to Use Extraterritorial Self-Defense Against Non-State Actors (2017) (Thesis in International Public Law, Stockholm University), http://www.diva-portal.org/smash/get/diva2:1134709/FULLTEXT02.pdf.

46. *See id.* at 47-48, 51; *see also* Chachko & Deeks, *supra* note 23.

> reflected in Article 51 of the Charter of the United Nations, when, as is the case here, the government of the State where the threat is located is *unwilling or unable* to prevent the use of its territory for such attacks. The Syrian regime has shown that it cannot and will not confront these safe havens effectively itself. Accordingly, the United States has initiated necessary and proportionate military actions in Syria in order to eliminate the ongoing ISIL threat to Iraq.[47]

Some states, including the United Kingdom, Germany, the Netherlands, the Czech Republic, Canada, and Australia, followed suit and explicitly invoked the doctrine in support of their actions in Syria.[48] On the other hand, Belgium, who similarly used force against ISIL in Syria, implicitly invoked the UoU doctrine to justify its actions:

> ISIL has occupied a certain part of Syrian territory *over which the Government of the Syrian Arab Republic does not, at this time, exercise effective control*. In the light of this exceptional situation, States that have been subjected to armed attack by ISIL originating in that part of the Syrian territory are therefore justified under Article 51 of the Charter to take necessary measures of self-defence.[49]

Other states were more ambiguous in their positions.[50] France, Denmark, and Norway all justified their actions pursuant to Security Council Resolutions condemning the terrorist acts of ISIL.[51] In particular, states relied on Resolution 2249, which "calle[ed] upon Member States that have the capacity to do so to take all necessary measures, in compliance with international law, in particular with the United

47. Permanent Rep. of the U.S. to the U.N., *supra* note 38.

48. Skantz, *supra* note 45, at 55; *see* Chachko & Deeks, *supra* note 23.

49. Permanent Rep. of Belgium to the U.N., *supra* note 41.

50. *See* Skantz, *supra* note 45, at 58–59.

51. *See* Permanent Rep. of France to the U.N., Identical letters dated Sept. 8,2015 from the Permanent Rep. of France to the United Nations addressed to the Secretary-General and the President of the Security Council, U.N. Doc. S/2015/745 (Sept. 8, 2015); Permanent Rep. of Denmark to the U.N., Letter dated Jan. 11, 2016 from the Permanent Rep. of Denmark to the United Nations addressed to the President of the Security Council, U.N. Doc. S/2016/34 (Jan. 13, 2016); Permanent Rep. of Norway to the U.N. Letter dated June 3, 2016 from the Permanent Rep. of Norway to the United Nations addressed to the President of the Security Council, U.N. Doc. S/2016/513 (June 3, 2016).

Nations Charter, as well as international human rights, refugee and humanitarian law, on the territory under the control of ISIL."[52]

Russia rescinded previous support for the doctrine in the face of coalition operations in Syria. Previously, in 2002, Russia referenced the UoU doctrine in justifying the use of force against Chechen rebels in the Pankisi Gorge in Georgia;[53] then-Prime Minister Vladimir Putin stated, in a letter to the U.N. Security Council, that "the continued existence... of territorial enclaves outside the control of national governments, which ... are unable or unwilling to counteract the terrorist threat is one of the reasons that complicate efforts to combat terrorism effectively. One such place ... is the Pankisi Gorge."[54] This statement of support appears to be based on the same self-defense justifications highlighted in the U.S. government's statement on the use of force against ISIL in Syria. Nonetheless, just over one decade later, in 2014, Russia condemned the coalition's invocation of the UoU doctrine:

> [A]ny action aimed at combating the threat of ISIL and groups like it must be carried out in accordance with the principles of the Charter of the United Nations and the standards of international law, based on existing anti-terrorism instruments of the United Nations, and in close cooperation with the Governments of the region. An international anti-terrorist operation should be conducted either with the consent of the sovereign Governments or sanctioned by the Security Council. We consider other options to be unlawful and detrimental to international and regional stability.[55]

Finally, some states outright objected to these actions and justifications.[56] Unsurprisingly, Syria itself, in a letter to the U.N. Secretary General and the Security Council, opposed the actions; it asserted that the military actions taken in Syria belonged "outside the scope of international law, absent full cooperation and prior coordination with the

52. S.C. Res. 2249, ¶ 5 (Nov. 20, 2015).

53. *See* Russian Federation President V. V. Putin, Annex to the letter dated Sept. 11, 2002 from the Permanent Rep. of the Russian Federation to the United Nations addressed to the Secretary-General, U.N. Doc. S/2002/1012 (Sept. 11, 2002); Permanent Rep. of Russian Federation to U.N., Statement by the Russian Federation Ministry of Foreign Affairs, U.N. Doc. A/57/269-S/2002/854 (July 31, 2002).

54. Annex to the letter dated Sept. 11, 2002 from the Permanent Rep. of the Russian Federation to the United Nations addressed to the Secretary-General, *supra* note 53, at 2.

55. U.N. SCOR, 69th Sess., 7271st mtg. at 19, U.N. Doc. S/PV.7271 (Sept. 19, 2014).

56. *See* Chachko & Deeks, *supra* note 23.

Syrian State and its legitimate institutions as is the case with the Syrian and Russian Governments."[57] Venezuela, Ecuador, and Cuba spoke out in support of Syria's position, asserting the belief that the use of force by the United States against ISIL in Syria violated international law.[58] For example, a Cuban representative made the following statement before the U.N. Human Rights Council:

> Taking into account recent cases in which we have seen a manipulation of the U.N. Charter as well as the double standard of the United States and other NATO members, we reject any attempt to undermine the sovereignty, independence, and territorial integrity of Syria.[59]

This survey of state positions on the legitimacy of the UoU doctrine to justify the use of force against ISIL in Syria demonstrates the test's contentious nature. One should recognize that any state's public assessment of the legitimacy of the UoU doctrine may be influenced by other factors, such as a desire to maintain relationships with allies. Regardless of the true motivation for opposition, many states currently express their resistance to the doctrine in terms of respect for sovereignty, territorial integrity, and political independence,[60] principles of paramount importance in the Charter system.[61] As such, objectors take issue with the ability of victim states to make their own determinations regarding the ability and willingness of a territorial state to suppress a threat

57. Permanent Rep. of the Syrian Arab Republic to the U.N., Identical letters dated Dec. 29, 2015 from the Permanent Rep. of the Syrian Arab Republic to the United Nations addressed to the Secretary-General and the President of the Security Council, ¶ 4, U.N. Doc. A/70/673–S/2015/1048 (Dec. 29, 2105) ("[A]ny attempt to invoke Article 51 of the Charter to justify military action on Syrian territory without coordination with the Syrian Government manipulates, distorts and misinterprets the provisions of that Article. The international community recognizes that the exercise of legitimate defence is subject to conditions that were put in place in order to uphold international law and the principles of sovereignty and non-interference, and to prevent the threat or use of force. Among the conditions required by Article 51 are that there should be an ongoing and effective act of aggression on the part of an armed force against a Member State, that the response should be temporary, and that it should respect the authority and responsibility of the Security Council. The military actions taken by Britain and other States in Syria do not meet those conditions. As a result, they belong outside the scope of international law, absent full cooperation and prior coordination with the Syrian State and its legitimate institutions as is the case with the Syrian and Russian Governments.")

58. Skantz, *supra* note 45, at 60-61; *see also* Chachko & Deeks, *supra* note 23.

59. Chachko & Deeks, *supra* note 23.

60. *See e.g.*, Statement of Venezuelan Ambassador, *supra* note 42; Press Release, U.N. Human Rights Council, *supra* note 42.

61. *See* U.N. Charter art. 2, ¶¶ 1, 4.

within its territory.[62] The fact that a victim state is empowered under the UoU doctrine to use force based on an independent evaluation of when another state is "unwilling" or "unable" to address a threat may violate these norms. Nonetheless, the doctrine does not impose any requirement of outside verification as to the level of willingness or ability.[63] To further understand why some states may be likely to oppose the application of the doctrine in the context of emerging technology, including to combat malicious uses of AI by NSAs, one must first understand what AI is, how it can be weaponized by NSAs, and why states may be unable to suppress threats posed by this weaponization.

III. Use of Force and Artificial Intelligence

From Star Wars to Star Trek, The Terminator to Wall-E, Hollywood has been fascinated by AI technology for decades, bringing anthropomorphized machines to life on the big screen.[64] While C-3PO levels of humanoid automation have yet to be achieved, AI is no longer a prisoner to the genre of science fiction. Anyone with a smartphone utilizes AI technology countless times each day, maybe without even realizing it.[65] Today, commonplace technologies such as "automatic speech recognition, machine translation, spam filters, and search engines,"[66] all rely on the use of AI. Despite the reality that AI makes life easier for some, not all potential uses of AI are quite so benevolent.

The Critical Emerging Technologies (CETs) List, which identifies CETs, a subset of advanced technologies that are potentially significant to U.S. national security, names AI as one of these critical and emerging technologies.[67] AI, like other emerging technologies, is unique in the

62. *See* Martin, *supra* note 12, at 436.

63. *See id.* at 439-40; *but see* Deeks, *supra* note 23, at 495-96 (In accordance with Article 51 of the Charter, the unwilling or unable determination lies with the victim state when the threat posed by a nonstate actor requires the victim state to act urgently before the Security Council can intervene. However, if the victim state unwilling or unable, assessment lies with the Security Council. Even so, the victim state most often must make the determination as a practical matter).

64. *See* Michael Hogan & Greg Whitmore, *The Top 20 Artificial-Intelligence Films – in Pictures*, Guardian (Jan. 8, 2015), https://www.theguardian.com/culture/gallery/2015/jan/08/the-top-20-artificial-intelligence-films-in-pictures.

65. *See* Ralf Llanasas, *How AI and Machine Learning are Transforming Mobile Technology*, Greenbook (Oct. 15, 2020, 7:10 AM), https://www.greenbook.org/mr/market-research-technology/how-ai-is-transforming-mobile-technology/.

66. Brundage et al., *supra* note 9, at 9.

67. Fast Track Action Subcomm. on Critical and Emerging Techs., Nat'l Sci. & Tech. Council, Critical and Emerging Technologies List Update 2, 4 (Feb.2, 2022), https://www.whitehouse.gov/wp-content/uploads/2022/02/02-2022-Critical-and-Emerging-Technologies-List-Update.pdf. The full list of CETs includes: Advanced Computing, Advanced Engineering

challenges that it poses to the application of the UoU doctrine; as such, this Note urges that the application of the UoU doctrine should be limited to protect state sovereignty in the age of emerging technologies by using AI as an illustrative case study. The rapid growth of and increased interest in weaponized AI renders it particularly demonstrative of the need to redefine the UoU doctrine. One commentator's remarks highlight the global interest and accompanying legal significance in the weaponization of AI—"[i]n the competition to lead the emerging technology race and the futuristic warfare battleground, artificial intelligence (AI) is rapidly becoming the center of the global power play."[68]

This section seeks to outline the security implications of the proliferation of AI, particularly the proliferation of weaponized AI, and caution that NSAs will likely pursue the use of AI to carry out armed attacks. Sections IV and V will subsequently discuss the legal implications emanating from this prospect and suggestions for how to mitigate them.

A. *Weaponization of Artificial Intelligence*

Understanding the implications of the weaponization of AI requires defining the term. AI is "a field of computer science dedicated to the theory and development of computer systems that are able to perform tasks normally requiring human intelligence, such as visual perception, speech recognition, translation between languages, decision-making, and problem-solving."[69] This broad definition encompasses many different subfields, including machine learning and deep learning.[70] Despite its futuristic reputation, AI is quite prevalent in the everyday

Materials, Advanced Gas Turbine Engine Technologies, Advanced Manufacturing, Advanced and Networked Sensing and Signature Management, Advanced Nuclear Energy Technologies, Artificial Intelligence, Autonomous Systems and Robotics, Biotechnologies, Communication and Networking Technologies, Directed Energy, Financial Technologies, Human-Machine Interfaces, Hypersonics, Networked Sensors and Sensing, Quantum Information Technologies, Renewable Energy Generation and Storage, Semiconductors and Microelectronics, Space Technologies and Systems. Although these technologies are outside the scope of this Note, it can be understood that significant advances in any of these areas would similarly complicate the application of unwilling or unable doctrine.

68. Jayshree Pandya, *The Weaponization of Artificial Intelligence,* FORBES (Jan. 14, 2019, 12:51 AM), https://www.forbes.com/sites/cognitiveworld/2019/01/14/the-weaponization-of-artificial-intelligence/?sh=4d2b9ae63686.

69. U.N. INTERREGIONAL CRIME AND JUST. RSCH. INST. & U.N. COUNTER-TERRORISM CTR., ALGORITHMS AND TERRORISM: MALICIOUS USE OF ARTIFICIAL INTELLIGENCE FOR TERRORIST PURPOSES 13 (2021) [hereinafter UNICRI & UNCCT Joint Report].

70. *Id.*

lives of many people today.[71] AI systems are used for a wide range of tasks, such as: data analytics (e.g., medical diagnoses), controlling autonomous systems (e.g., self-driving cars); predicting future trends or behavior; object classification and recognition; detecting anomalous activity (e.g., financial transactions); optimizing systems to achieve a goal; and performing simple automated tasks at scale.[72]

However, not all applications of AI are so benevolent. Many AI systems are dual-use, meaning that the technology itself, and the knowledge of how to design and develop it, can be utilized in both civilian and military contexts.[73] Partially autonomous and intelligent systems have been used in warfare since World War II.[74] However, it would be erroneous to base a prediction on the future of weaponizable AI on the most primitive iterations; recent breakthroughs in AI and machine learning signify a turning point in the automation of warfare.[75] The utilization of weaponized AI already includes "navigating and utilizing unmanned naval, aerial, and terrain vehicles, producing collateral-damage estimations, deploying "fire-and-forget" missile systems and … automat[ing] everything from personnel systems and equipment maintenance to the deployment of surveillance drones, robots and more."[76]

Autonomous weapons are of particular interest and concern. These systems are believed to achieve greater speed, accuracy, persistence, precision, reach, and coordination on the CGS[77] battlefield at lower operating costs;[78] as a result, many states, including China, Israel, Russia, South Korea, the United Kingdom, the United States, Australia,

71. *See* U.N. INST. FOR DISARMAMENT RSCH., THE WEAPONIZATION OF INCREASINGLY AUTONOMOUS TECHNOLOGIES: ARTIFICIAL INTELLIGENCE, OBSERVATION REPORT NO. 8 8 (2018); *see also* J.D. Biersdorfer, *Use that Everyday A.I. in Your Pocket*, N.Y. TIMES (Jun. 29, 2022), https://www.nytimes.com/2022/06/29/technology/personaltech/use-that-everyday-ai-in-your-pocket.html.

72. U.N. INST. FOR DISARMAMENT RSCH., *supra* note 71 at 8.

73. BRUNDAGE ET AL., *supra* note 9, at 16.

74. GREG ALLEN & TANIEL CHAN, HARVARD U.'S BELFER CTR. FOR SCI. & INT'L AFF., ARTIFICIAL INTELLIGENCE AND NATIONAL SECURITY 13 (2017), https://www.belfercenter.org/sites/default/files/files/publication/AI%20NatSec%20-%20final.pdf; *see also* ROBERT O. WORK, CTR. FOR NEW AM. SEC., A SHORT HISTORY OF WEAPON SYSTEMS WITH AUTONOMOUS FUNCTIONALITIES (2021), https://www.jstor.org/stable/pdf/resrep32146.4.pdf (discussing the evolution of partially autonomous weapons, including–the 1943 Mk-24 "Fido", an "air-dropped, passive acoustic homing torpedo"; semi-round environment (SAGE), "designed to direct and control U.S. continental air defense"; fire-and-forget guided munitions; and static search weapons).

75. ALLEN & CHAN, *supra* note 74.

76. Pandya, *supra* note 68.

77. CGS stands for Cyberspace, geospace, space. *Id.*

78. *Id.*

and Turkey, are investing in their development.[79] In fact, there is evidence suggesting that Israel, Russia, South Korea, and Turkey have already used weapons with fully autonomous capabilities;[80] for example, open source analysis suggests that Russia may have deployed a weapon, the Kalashnikov ZALA Aero KUB-BLA loitering munition, that was capable of autonomously recognizing and striking targets in Ukraine in March 2022[81] and a U.N. report alleges that Turkey deployed lethal autonomous systems, including the STM Kargu-2, to "hunt[] down and remotely engag[e]" Libyan logistics convoys and retreating ground forces in March 2020.[82] Despite the interest and existing capability demonstrated by these states, a growing number of legislators, policymakers, companies, and international and domestic organizations have called for a complete ban on autonomous weapons.[83] Between 2013 and 2020, 30 countries supported such a ban[84] and even more states have called for an international agreement to prescribe prohibitions and regulations on autonomous weapons.[85] The Convention on Conventional Weapons has held meetings on lethal autonomous

79. Brian Stauffer, *Stopping Killer Robots: Country Positions on Banning Fully Autonomous Weapons and Retaining Human Control*, HUMAN RIGHTS WATCH 3 (Aug. 10, 2020), https://www.hrw.org/sites/default/files/media_2021/04/arms0820_web_1.pdf.

80. Robert F. Trager & Laura M. Luca, *Killer Robots Are Here–and We Need to Regulate Them*, FOREIGN POL'Y (May 11, 2022, 1:46 PM), https://foreignpolicy.com/2022/05/11/killer-robots-lethal-autonomous-weapons-systems-ukraine-libya-regulation/.

81. Zachary Kallenborn, *Russia May Have Used a Killer Robot in Ukraine. Now What?*, BULL.OF THE ATOMIC SCIENTISTS (Mar. 15, 2022), https://thebulletin.org/2022/03/russia-may-have-used-a-killer-robot-in-ukraine-now-what/?utm_source=Newsletter&utm_medium=Email&utm_campaign=ThursdayNewsletter03172022&utm_content=DisruptiveTechnologies_KillerRobotInUkraine_03152022; Trager & Luca, *supra* note 80.

82. Letter Dated 8 March 2021 from the Panel of Experts on Libya Established pursuant to resolution 1973 (2011) Addressed to the President of the Security Council, U.N. Doc. S/2021/229 (Mar. 8, 2021); *see also* Trager & Luca, *supra* note 81; Kallenborn, *supra* note 81;

83. Trager & Luca, *supra* note 80.

84. *Id.* at 9.

85. *See, e.g.,* Bolivarian Republic of Venezuela on behalf of the Non-Aligned Movement (NAM) and Other States Parties to the Convention on Certain Conventional Weapons (CCW), Group of Governmental Experts of the High Contracting Parties to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects, U.N. Doc. CCW/GGE.1/2018/WP.1 (Mar. 28, 2018) ("a general sense has developed among High Contracting Parties that all weapons, including those with autonomous functions, must remain under the direct control and supervision of humans at all times, and must comply with international law including International Humanitarian Law and International Human Rights Law. These core elements must be an integral part of the legally binding instrument on LAWS. In this regard, pending the conclusion of a legally binding instrument, NAM calls upon all States to declare moratoria on the further development and use of LAWS.").

weapons since 2014; however, these talks, which were formalized in 2016, have failed to yield a meaningful multilateral agreement.[86] As the group operates by consensus,[87] it is unlikely that a universal, comprehensive ban on lethal autonomous weapons will be achieved any time soon. Therefore, the proliferation of weaponized AI is sure to continue despite the widespread concern about the resulting global security threats. As such, the implications for the UoU doctrine cannot be ignored.

The report, *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation*, written by twenty-six authors from academia, civil society, and industry, asserts that "absent the development of adequate defenses, progress in AI will: [e]xpand existing threats, [i]ntroduce new threats, [and] [a]lter the typical character of threats."[88] The experts predict that AI will expand existing threats by increasing the set of actors who are capable of carrying out an attack, the rate at which these actors can carry it out, the set of plausible targets, and the willingness of actors to carry out certain attacks.[89] They also suggest that AI will introduce new threats by completing tasks more successfully than any human could.[90] Finally, they expect that AI will alter the typical character of threats by resulting in a greater frequency of attacks that are more effective, larger in scale, finely targeted, difficult to attribute, and exploitative of vulnerabilities in AI systems.[91]

The report further identifies three areas in which these threats could fall: "digital security (e.g., through criminals training machines to hack or socially engineer victims at human or superhuman levels of performance), physical security (e.g., NSAs weaponizing consumer drones), and political security (e.g., through privacy-eliminating surveillance, profiling, and repression, or through automated and targeted disinformation campaigns)."[92] While digital security and political security are equally important, this Note will primarily focus on the threats that AI poses to physical security, as kinetic attacks fit most squarely in the analysis of self-defense and the UoU doctrine.[93]

---

86. Stauffer, *supra* note 79.

87. *Id.*

88. BRUNDAGE ET AL., *supra* note 9, at 18.

89. *Id.*

90. *Id.*

91. *Id.*

92. *Id.* at 10.

93. In theory, a cyberattack can reach the threshold of an "armed attack" for the purpose of self-defense. *See* TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 339-48 (Michael N. Schmitt & Liis Vihul eds., 2017). However, in practice, "few if any

Many non-autonomous robotic systems can be readily customized and equipped with dangerous payloads to carry out precise physical attacks from a great distance, not unlike those carried out through the use of cruise missiles.[94] While the report admits that "this threat exists independent of AI," citing non-automated drone attacks carried out by NSAs, it states that increased autonomy in robotic systems, aided by the commercialization and democratization of AI, will enable smaller groups of actors to inflict greater degrees of physical damage.[95] Of course, advocates of AI would argue that AI can be used to defeat and reduce each of the aforementioned threats; while autonomous systems can help attackers identify vulnerabilities and plan attacks, they also supply defenders with "better situational awareness to monitor movements of attackers and plan ambushes."[96] Several factors, including the nature of application, reliability in the face of interference, affordability, and effects on the cost of war influence whether autonomy will favor offense or defense.[97] Regardless of which side wins in the end, the extensive capabilities in both arenas reasonably raise the concern that NSAs will soon turn to AI technology.

B. *Artificial Intelligence and the NSA*

As a general rule, "terrorist organizations tend to be risk averse with their repertoire."[98] As such, they typically favor firearms and bombs over more advanced weaponry.[99] However, it would be misguided to infer future resistance to innovation from this historical preference. After all, even if some NSAs shy away from the relatively untested realm of weaponized AI, others will be attracted to the benefits. Terrorist organizations have shown a willingness and ability to adapt, with the nature of attacks changing in response to technological developments. [100] Some examples of the use of technology in attacks include: the use of

of the known cyberattacks appear to meet the threshold for a 'use of force,' let alone for an 'armed attack.'" Lorraine Finlay & Christian Payne, *The Attribution Problem and Cyber Armed Attacks*, 113 AM. J. INT'L L. UNBOUND 202, 202 (2019). Regardless, these issues are beyond the scope of this Note.

94. BRUNDAGE ET AL., *supra* note 9, at 39-40.

95. *Id.* at 38-40.

96. Zachary Kallenborn, *Swords and Shields: Autonomy, AI, and the Offense-Defense Balance,* GEO. J. INT'L AFF. (Nov. 22, 2021), https://gjia.georgetown.edu/2021/11/22/swords-and-shields-autonomy-ai-and-the-offense-defense-balance/.

97. *Id.*

98. UNICRI & UNCCT Joint Report, *supra* note 69, at 17.

99. *See* U.N. Off. on Drugs & Crime, *Conventional Terrorist Weapons*, https://www.unodc.org/images/odccp/terrorism_weapons_conventional.html (last visited May 13, 2022).

100. UNICRI & UNCCT Joint Report, *supra* note 69, at 19.

GPS, mobile phone, and internet by perpetrators of the Mumbai attacks in 2008,[101] the use of crowdfunding, mobile banking, and cryptocurrencies, such as Bitcoin, to raise or move funds,[102] and the use of the dark web to source materials, weapons and fake documents.[103] These instances suggest that as emerging technologies, including AI, become increasingly accessible to the general public, NSAs are likely to utilize them in advancing their interests and carrying out attacks. One commentator distinguished AI from nuclear weapons, which NSAs have failed to harness despite widespread concerns—"Unlike nuclear weapons which are expensive and require hard to obtain components, many AI applications will be cheap to mass produce or make commercially available. The wider accessibility and affordability of AI makes it only a matter of time until AI technologies appear on the black market for nefarious use."[104]

A group of experts from government, industry, academia, and international and regional organizations were assembled to assess the risk posed by the terrorist use of AI.[105] When asked about the perceived likelihood of malicious use of AI for terrorist purposes, 44% felt that it was "very likely," 56% felt it was "somewhat likely", and none felt that it was "unlikely."[106] In making this assessment, participants identified four factors that contributed to their concerns: democratization, scalability,

101. Jeremy Kahn, *Mumbai Terrorists Relied on New Technology for Attacks*, N.Y. TIMES (Dec. 8, 2008), https://www.nytimes.com/2008/12/09/world/asia/09mumbai.html; s*ee also* UNICRI & UNCCT joint report, *supra* note 69, at 20.

102. *See generally* CYNTHIA DION-SCHWARZ ET AL., RAND CORP., TERRORIST USE OF CRYPTOCURRENCIES: TECHNICAL AND ORGANIZATIONAL BARRIERS AND FUTURE THREATS (2019).

103. *See generally* Abeer ElBahrawy et al., *Collective Dynamics of Dark Web Marketplaces*, 10 SCI. REPS. 1, 1 (2020).

104. Young, *supra* note 7.

105. UNICRI & UNCCT Joint Report, *supra* note 69, at 7. Participants in the Expert Group Meeting included representatives from the Austrian Institute of Technology; AWO; Chemonics; the Council of Europe; the European Commission - Directorate-General for Migration and Home Affairs (DG HOME); the European Union Agency for Law Enforcement Cooperation (Europol); the Foreign Ministry of the Russian Federation; Chatham House; the Geneva Centre for Security Policy; the Organization for Security and Cooperation in Europe (OSCE); Link11 Cyber Resilience; MalwareBytes; the North Atlantic Treaty Organization (NATO); Trend Micro; the United Kingdom Re- search and Innovation (UKRI) Trustworthy Autonomous Systems (TAS) Hub; the United Nations Counter-Terrorism Committee Executive Directorate (CTED); the United Nations University; and the Universities of College London, Bristol, Cambridge and Southampton.

106. *Id.* at 11.

inherent asymmetry in terrorism and counterterrorism, and growing societal dependency on data and technology.[107]

The threat posed by AI has been described as "a combination of intention and capability."[108] According to "lethal empowerment theory," for a weapon to be desirable to violent NSAs, it must be "accessible, cheap, simple to use, transportable, concealable, and effective."[109] It follows that AI, as a technology that would require significant time, money, and effort to successfully weaponize,[110] may not be desirable to NSAs for these reasons. On the other hand, AI is appealing to NSAs because it can be utilized in a wide range of contexts.[111] Notwithstanding these seemingly conflicting assessments, the intent of NSAs to use AI cannot be underestimated.

The second requirement, capability, is similarly debated. While AI technologies have become commercially available, the capacity to leverage these tools is less established.[112] Some experts have concluded that terrorist groups "lack the necessary capabilities or funding or are simply not sufficiently organized to do so."[113] However, it has been suggested that NSAs could outsource their attacks to black-market hackers or other criminal groups, removing the requirement that the groups have the AI capability themselves.[114] Additionally, capabilities of the groups themselves will improve as they adopt and learn from the successes of early adopters.

Irrespective of the theoretical evaluations of intent and capability, there is evidence that NSAs have continued to pursue emerging technologies. For example, ISIL created a "United Cyber Caliphate" dedicated to building a cyber army capable of carrying out asymmetrical attacks.[115] Despite the absence of evidence of a direct use of AI by NSAs, there is considerable proof that these groups have used AI-related and semi-autonomous technologies in attacks. One prominent

---

107. *Id.*

108. *See id.* at 49-52.

109. INST. FOR ECON. & PEACE, GLOBAL TERRORISM INDEX 2022: MEASURING THE IMPACT OF TERRORISM 72 (2022), https://www.economicsandpeace.org/wp-content/uploads/2022/03/GTI-2022-web-09062022.pdf.

110. UNICRI & UNCCT Joint Report, *supra* note 69, at 50.

111. INST. FOR ECON. & PEACE, *supra* note 109, at 75; UNICRI & UNCCT Joint Report, *supra* note 69, at 50.

112. *See* UNICRI & UNCCT Joint Report, *supra* note 69, at 50-51.

113. *Id.*

114. *See id.* at 51.

115. *See* Christina Schori Liang, *Unveiling the "United Cyber Caliphate" and the Birth of the E-Terrorist*, 18 GEO. J. INT'L AFF. 11, 11 (2017).

example is the proliferation of drones; in fact, terrorists have been experimenting with the use of drones for decades.[116] More recently, ISIL, Iran and militia proxies, a Syrian rebel group, and others have used drones to carry out their own attacks.[117] One open source report identified 440 instances in which NSAs used weaponized drones in attacks, 99% of which occurred between August 2016 and March 2020.[118] Although NSAs have historically only used semi-autonomous drones,[119] these drone attacks are demonstrative of intent to pursue other technologies.[120] It may be argued that the use of drones, given their increased commercial availability and relative technological simplicity, is not proof of high-tech capability or intention and therefore an inadequate predictor for the nonstate weaponization of AI. However, this argument overlooks the reality that AI is rapidly mainstreaming.[121] It follows that AI will soon find its way into the arsenals of NSAs if it has not already.[122]

IV. UoU, Artificial Intelligence, and State Sovereignty

The potential weaponization of AI by NSAs prompts the question of what this may mean for the state of international law. Relevant here

116. In the early 1990s, Aum Shinkrikyo, the Japanese cult behind the Tokyo subway sarin attack in 1995, purchased two remote control drones as part of an unused plot. Amy E. Smithson, Ataxia: The Chemical and Biological Terrorism Threat and the US Response 80 (Amy E. Smithson & Leslie-Anne Levy eds., 2000), https://www.stimson.org/wp-content/files/file-attachments/atxchapter3_1.pdf.

117. In 2016, ISIL used drones to kill two Peshmerga warriors in northern Iraq. In January 2018, an unidentified Syrian rebel group deployed a swarm of 13 homemade drones to attack Russian bases. In August 2018, an unknown group used exploding drones in an assassination attempt against Venezuela's Nicolas Maduro. In September 2019, Iran and its militia proxies used drone-carried explosives in an attack on Saudi oil facilities. Jacob Ware, *Terrorist Groups, Artificial Intelligence, and Killer Drones*, War on the Rocks (Sept. 24, 2019), https://warontherocks.com/2019/09/terrorist-groups-artificial-intelligence-and-killer-drones/.

118. Sarah Kreps, Brookings Inst., Democratizing Harm: Artificial Intelligence in the Hands of Non-State Actors 7 (Nov. 2021), https://www.brookings.edu/wp-content/uploads/2021/11/FP_20211122_ai_nonstate_actors_kreps.pdf.

119. *Id.* at 8.

120. *See* UNICRI & UNCCT Joint Report, *supra* note 69, at 50.

121. *See* Brundage et al., *supra* note 9, at 9 ("Artificial intelligence (AI) and machine learning (ML) have progressed rapidly in recent years, and their development has enabled a wide range of beneficial applications"); s*ee also* James Vincent, *ChatGPT Proves AI is Finally Mainstream and Things Are only Going to Get Weirder*, The Verge (Dec. 8, 2022, 10:31 AM), https://www.theverge.com/2022/12/8/23499728/ai-capability-accessibility-chatgpt-stable-diffusion-commercialization.

122. *See* Kreps, *supra* note 118, at 6 (stating that "the demonstrated appeal of, and rising investment in these technologies means that the increased use of both drones and AI-enabled autonomous capabilities by nonstate actors is almost inevitable").

is the standing of the UoU doctrine in the age of emerging technologies. The concern that AI can be "used by groups and individuals to enhance the intensity of terrorist attacks or to amplify the potential of these groups or individuals to disseminate extremist propaganda and incite violence"[123] suggests that repelling such attacks will be increasingly difficult. There is significant evidence that "regulation and technical research on defense have been slow to catch up with the global proliferation of weaponizable [AI systems]."[124] Effective physical defenses include "detection via radar, lidar, acoustic signature, or image recognition software; interception through various means; and passive defense through physical hardening or nets."[125] While the hardware and software necessary to carry-out AI attacks are increasingly available to the public,[126] the disparity between the development of offensive and defensive AI capabilities is predicted to grow because these defenses are capital-intensive, requiring extensive funds and human labor.[127]

Furthermore, AI "is leading us toward a new algorithmic warfare battlefield that has no boundaries or borders, may or may not have humans involved, and will be impossible to understand and perhaps control across the human ecosystem in cyberspace, geospace, and space (CGS)."[128] As such, physical attacks could take place anywhere in the world, from anywhere in the world, including in many regions with "insufficient resources to deploy large-scale physical defenses."[129] Thus, even if the capability gap does not increase as expected[130] and the offense-defense race neutralizes overall, some states would likely lag behind. As a general rule, the economic and social benefits of technological advancement are geographically concentrated in developed countries.[131] On the other hand, the least-developed countries (LDCs) tend to remain far behind as "a result of the serious and manifold development challenges these countries continue to face, experiencing delays in their efforts to eradicate poverty, achieve sustainable development and participate fully in an increasingly competitive global

123. *See* UNICRI & UNCCT Joint Report, *supra* note 69, at 10.

124. BRUNDAGE ET AL., *supra* note 9, at 38.

125. *Id.* at 43.

126. *Id.* at 38.

127. *Id.* at 42.

128. Pandya, *supra* note 68.

129. BRUNDAGE ET AL., *supra* note 9, at 38.

130. *See id.*

131. Fekitamoeloa 'Utoikamanu, *Closing the Technology Gap in Least Developed Countries,* U.N. CHRON. (Dec. 2018), https://www.un.org/en/chronicle/article/closing-technology-gap-least-developed-countries.

market."[132] As many LDCs struggle to make broadband internet access available and affordable to all,[133] one can assume that they would also face great difficulties in deploying widespread and effective defenses against AI weaponization.

It follows that some states, if not all, may find themselves unable to prevent the use of their territory for AI-enabled attacks against other states. It may be equally unlikely that the victim state would be able to defend against the effective, finely targeted, difficult-to-attribute AI-enabled attacks, as they would be subject to the same gap between attack capabilities and defense capabilities. However, there is no requirement of greater ability under the existing UoU doctrine. Given this reality, victim states will likely be granted wide latitude to use force against territorial states under the current formulation of the UoU doctrine. The incorporation of a limiting principle would serve the doctrine well, as will be discussed in the next section.

Without refinement, the UoU doctrine, with all its ambiguity, will permit unwarranted violations of state sovereignty under the guise of self-defense. While Article 2 of the Charter reflects universal respect for the principles of sovereignty and non-interference, Article 51 expresses the conflicting concern for self-defense. However, the right to use force in self-defense is an exception to those underlying presumptions of sovereignty and non-interference; consequently, states must be careful not to extend the right to use force in self-defense too far beyond what was originally intended by the drafters of the Charter. While it would be unreasonable to leave states defenseless against AI-enabled attacks by NSAs acting from within the territory of another state, it would be even more unfair to permit a violation of state sovereignty every time the territorial state is unable to combat that novel threat. These core principles risk deterioration if states are permitted to use force against NSAs in the territory of a third state to repel an AI-enabled attack that the territorial state will, in all likelihood, be unable to prevent itself. For these reasons, it is necessary to limit the application of the UoU doctrine in the context of AI and other emerging technologies.

V. Recommendations

A. *Eliminate the "Unable" Element*

Out of respect for state sovereignty and the right to self-defense, application of the doctrine should be limited to instances in which the

132. *Id.*
133. *Id.*

territorial state is unwilling to address the threat independently or accept assistance.[134] In other words, a victim state could no longer use the UoU doctrine to justify the use of force against an NSA within the territory of a state that is simply lacking the means necessary to combat a threat but is willing to accept assistance from the victim state in doing so. This formulation would protect a territorial state's sovereignty by permitting it to grant limited consent in terms of technological or military assistance while also preserving a victim state's right to self-defense if a territorial state refuses to address the threat or accept help.

However, this proposal prompts several challenging debates regarding what level of assistance is required and who is authorized to make that determination. For instance, one may ask whether a territorial state must accept all the assistance that the victim state may want to provide or, alternatively, may the territorial state specify that it will accept technical assistance but will not allow the victim state to put boots on the ground.[135] While questions such as this are important to address, it is unwise to establish bright-line rules regarding the threshold for adequate assistance. This is particularly true in the context of emerging technologies including AI, as it is difficult to anticipate what new threats may look like and thus what new defenses will require. As such, it is best to require only that the territorial state be willing to accept a level of assistance that could reasonably combat the threat posed by the NSA. If, after collaborating with the territorial state to carry out a coordinated response to the threat, the victim state determines that the level

134. Martin, *supra* note 12, at 451 ("[M]ere inability to deal with the threat posed by an NSA should not be grounds for a use of force against a state. The onus is on the target state to approach the unable territorial state for consent to take action. It is only when the state that is unable to deal with the threat posed by an NSA also refuses its consent to allow the target state to do so that it becomes 'unwilling,' such that that the use of force may be justified against the NSA and the territorial state in which it is operating as an exercise of self-defense.").

135. The concept of limited consent is well settled in other contexts. Article 20 of the Articles on the Responsibility of States for Internationally Wrongful Acts provides that "[v]alid consent by a State to the commission of a given act by another State precludes the wrongfulness of that act in relation to the former State to the extent that the act remains within the limits of that consent." G.A. Res. 56/83, Articles on the Responsibility of States for Internationally Wrongful Acts (Dec. 12, 2001). The 2001 commentary of the International Law Commission elaborates on this principle, stating "where consent is relied on to preclude wrongfulness, it will be necessary to show that the conduct fell within the limits of the consent. Consent to overflight by commercial aircraft of another State would not preclude the wrongfulness of overflight by aircraft transporting troops and military equipment. Consent to the stationing of foreign troops for a specific period would not preclude the wrongfulness of the stationing of such troops beyond that period." Report of the International Law Commission to the General Assembly, U.N. GAOR Supp. No. 10, at 78-79, U.N. Doc. A/56/10 (2001), reprinted in [2001] 2 Y.B. INT'L L. COMM'N 1, U.N. Doc. A/CN.4/SER.A/2001/Add.1 (Part 2).

of assistance approved by the territorial state is not sufficient to combat the threat, the victim state may take further action, even if the territorial state does not approve. Just as the doctrine's current formulation operates in a sphere of ambiguity,[136] some amount of flexibility is necessary to facilitate the longevity of a doctrine governing the use of force to combat threats posed by emerging technology.

A benefit of this approach in the age of emerging technologies is that LDCs, who would likely face difficulties in deploying widespread and effective defenses against AI weaponization, will not be at a greater risk of having their sovereignty violated than more developed countries. Imagine a scenario in which a terrorist organization deploys a large swarm of semi-autonomous unmanned aerial vehicles programmed to target large crowds of civilians in a victim state. If the terrorist group is operating from within one of the world's LDCs, that country, possibly struggling to provide broadband internet access, is unlikely to possess the technology to defeat an NSA that has access to AI-enabled systems. However, if the victim state is a highly developed and technologically advanced country, it is likely to possess more advanced weapons systems that may be capable of locating, targeting, and suppressing the threat posed by the terrorist organization. Rather than taking unilateral action based on an independent determination that the territorial state is incapable of defending against a technologically advanced actor, the victim state should aid the territorial state. If the territorial state is unwilling to accept a level of assistance that is reasonably likely to counter the threat, the victim state may then, and only after making all reasonable efforts to collaborate with the territorial state, take independent action. The same UoU formulation would apply if the territorial state were not an LDC but was simply unable to independently suppress the threat posed by an AI-capable NSA. Even the most technologically advanced territorial states may be subject to independent intervention by a victim state if they are unable to accept assistance. Thus, by eliminating the "unable" element, the doctrine levels the playing field between LDCs and developed countries, with all states being at risk of having their sovereignty violated under the doctrine only if they refuse to accept aid.

The elimination of the "unable" element could be limited to circumstances involving emerging technologies or AI. This would result in a bifurcated UoU regime, under which different standards would control depending on the nature of the threat posed by the NSA. This division,

136. *See* Deeks, *supra* note 23, at 546-47 (proposing a set of substantive and procedural factors to address the "current, vague incarnation of the test").

while certainly novel, would likely cause further confusion about an already nebulous doctrine. It would be more efficacious to eliminate the "unable" doctrine altogether. Doing so would not only modernize the doctrine by controlling for the uneven distribution of emerging technologies among states of varying degrees of development but would also address many of the criticisms of the traditional application. For example, concerns over sovereignty, territorial integrity, and political independence[137] would be mitigated by requiring a victim state to aid the territorial state before resorting to a unilateral use of force within that state's territory. At the same time, interests of self-defense, often cited by state proponents of the current doctrine,[138] would be preserved, allowing the victim state to invoke the doctrine when the territorial state refuses to address the threat or accept assistance.

While this approach to the UoU doctrine provides a strong balance between state sovereignty and self-defense, it may be opposed by states that benefit from the ambiguity and leniency of the current formulation. As the UoU doctrine is not currently codified as a matter of international law, enacting this change could pose significant challenges. What the mechanism of change should be is beyond the scope of this Note. All this recommendation aims to assert is that the UoU doctrine should, preferably in all circumstances but surely in the context of emerging technologies, be limited to instances in which the territorial state is unwilling to address the threat independently or is unwilling to accept assistance in doing so.

B. *Encourage a Showing of Greater Ability*

If the UoU doctrine is not limited to cases in which the territorial state is unwilling to address the threat independently or is unwilling to accept assistance in doing so, the doctrine should be bolstered by encouraging transparency and accountability in invocation. To do so, victim states should make a showing of greater ability when invoking the UoU doctrine. In this context, a showing of "greater ability" should consist of a fact-based analysis grounded in the factors discussed in *Section II*; namely, the showing should address each state's response to prior threats posed by NSAs and whether each state has sufficient resources to combat the threat posed by the NSA.[139] This empirical

137. *See* Statement of Venezuelan Ambassador, *supra* note 42; Press Release, U.N. Human Rights Council, *supra* note 42.

138. *See, e.g.*, Permanent Rep. of Belgium to the U.N., *supra* note 41; Permanent Rep. of the U.S. to the U.N., *supra* note 38.

139. Sharma & Agarwal, *supra* note 24.

showing of greater ability should be made by states whenever they seek to invoke the UoU doctrine; for example, a victim state should provide a factual basis for greater ability when invoking the UoU doctrine to justify the use of force in self-defense in an Article 51 letter.

While this suggestion could be limited to the narrow context of weaponized AI, it would be more desirable to require a showing of greater ability in all contexts; this would ensure that the UoU doctrine maintains credibility in the age of emerging technologies and ever-changing threats. Of course, this recommendation is grounded in this Note's conclusion that the proliferation of weaponized AI by NSAs will leave some states, particularly LDCs, unable to address that threat, thereby leaving them vulnerable to violation of state sovereignty by more capable victim states. However, as noted from the outset, AI is used in this Note as an illustrative case study for the challenges posed to the UoU doctrine by emerging technologies more generally. Therefore, states should be encouraged to make a showing of greater ability in all future invocations of the doctrine.

By encouraging victim states to make a showing of greater ability, rather than solely a claim of inability of the territorial state, application of the doctrine would result in fewer unjustifiable violations of sovereignty. If the modern UoU doctrine is based in the right of self-defense, it would be illogical to allow a victim state to use force on the territory of another state when doing so would be futile. Encouraging victim states to make a showing of greater ability to suppress the threat posed to them by an NSA, supported by a factual record, would incorporate an element of accountability. A norm of states making a showing of greater ability may result in increased political pressure on a state that neglects to make a showing or attempts to make a showing that is contrary to the factual situation as understood by other entities. Such political pressures, although not necessarily determinative of the ultimate resort to force, may reduce the frequency with which the UoU doctrine is used to justify an unwarranted violation of state sovereignty.

One should acknowledge that an unambiguous showing of greater ability may not always be feasible. It might not always be crystal clear which state has superior capabilities; different states possess varying degrees of experience, knowledge, and defense infrastructure, making them better suited to address different types of threats. Determining the adequacy of defensive capabilities is particularly challenging in the context of weaponized AI, as AI "is leading us toward a new algorithmic warfare battlefield that has no boundaries or borders, may or may not have humans involved, and will be impossible to understand and

perhaps control."[140] Therefore, this showing will likely become increasingly challenging in the age of emerging technologies.

Consequently, this suggestion should not be understood to imply that a victim state should be left without recourse if it is unable to make a clear showing of greater ability. Rather, it is urged that states go through the process of investigating the abilities of both parties and providing a transparent, factually backed summary of their position. If the ultimate showing results in a degree of uncertainty or suggests that the victim state is in fact less capable of addressing the threat than the territorial state, the victim state should reconsider all other options, including a resolution by the Security Council or consent of the territorial state, before acting unilaterally to combat the threat. While the invocation of the UoU doctrine should be discouraged absent a clear showing, the decision is ultimately that of the victim state. Although imperfect, such a formulation would increase transparency and accountability while promoting autonomy and security.

C. *Increase Regulation of AI*

By increasing the regulation of AI, states could, to some extent, prevent NSAs from obtaining weaponizable AI systems in the first place. A complete ban on AI would be both undesirable and unattainable.[141] AI technology has the potential to address some of the world's biggest challenges, "from hunger and disease, to climate change and disaster relief."[142] Social good should not be stifled to reduce the possibility that the AI technology they rely on could be weaponized by a relatively small subset of the population. Of course, strong regulation would likely be opposed by those who benefit economically from the sale and distribution of AI. Even more limited bans, such as the proposed ban on autonomous weapons, would not necessarily prevent the use of weaponized AI by NSAs; in fact, "these proposed bans would only apply to states, which would increase the asymmetrical advantage of nonstate actors because of

140. Pandya, *supra* note 68.

141. *See* Sarah Kreps & Richard Li, *Cascading Chaos: Nonstate Actors and AI on the Battlefield*, BROOKINGS INST. (Feb. 1, 2022), https://www.brookings.edu/blog/order-from-chaos/2022/02/01/cascading-chaos-nonstate-actors-and-ai-on-the-battlefield/ ("As the sections above suggest, AI-enabled technologies are evolving quickly in ways accessible to nonstate actors because of their commercial availability and affordability. The same commercial use that makes these technologies available also makes them difficult to regulate.").

142. MICHAEL CHUI ET AL., MCKINSEY GLOB. INST., NOTES FROM THE AI FRONTIER: APPLYING AI FOR SOCIAL GOOD 1 (2018), https://www.mckinsey.com/~/media/mckinsey/featured%20insights/artificial%20intelligence/applying%20artificial%20intelligence%20for%20social%20good/mgi-applying-ai-for-social-good-discussion-paper-dec-2018.ashx.

their exclusion from organized bans and the participation of state actors."[143] Even if desirable, a complete ban would be impossible to achieve, as knowledge is proliferation in and of itself. Just as some believe that a nuclear weapon global zero cannot be achieved since "[n]either the knowledge or the nuclear materials will disappear,"[144] the same is true for AI; AI is a genie that simply cannot be put back in the bottle.

Rather than pursuing a ban, states should restrict and monitor the sale and use of AI technology, namely weaponizable AI hardware and software, by establishing a multilateral export control regime. Multilateral export control arrangements are "informal groups of like-minded supplier countries which seek to contribute to the non-proliferation of [weapons of mass destruction] and delivery systems through national implementation of Guidelines and control lists for exports."[145] The guidelines established and enforced by these groups, although voluntarily implemented, "limit the ability of proliferators to 'shop' items and technology in countries that do not have export control systems in place."[146] Existing multilateral export control arrangements consist of the Australia Group,[147] the Missile Technology Control Regime,[148] the Nuclear Suppliers Group,[149] and the Wassenaar Arrangement.[150]

---

143. Kreps & Li, *supra* note 141.

144. Michael E. O'Hanlon, *Is a World Without Nuclear Weapons Really Possible?*, BROOKINGS INST. (May 4, 2010), https://www.brookings.edu/opinions/is-a-world-without-nuclear-weapons-really-possible/.

145. DEPT. OF ENERGY, NAT'L NUCLEAR SEC. ADMIN., OVERVIEW OF THE MULTILATERAL EXPORT CONTROL SUPPLIER ARRANGEMENTS: NSG, MTCR, AG, AND WAASENAR 3, https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/attachments/150625_LodenPresentation.pdf.

146. *Id.*

147. *See Objectives of the Group*, AUSTL. GRP., https://www.dfat.gov.au/publications/minisite/theaustraliagroupnet/site/en/objectives.html (last visited May 14, 2022) ("The principal objective of the Australia Group participants' is to use licensing measures to ensure that exports of certain chemicals, biological agents, and dual-use chemical and biological manufacturing facilities and equipment, do not contribute to the spread of [chemical and biological weapons].").

148. *See Our Mission*, MISSILE TECH. CONTROL REGIME, https://mtcr.info (last visited May 14, 2022) ("Our mission is to coordinate national export licensing efforts aimed at preventing proliferation of unmanned delivery systems capable of delivering weapons of mass destruction.").

149. *See About the NSG*, NUCLEAR SUPPLIERS GRP., https://www.nuclearsuppliersgroup.org/en/about-nsg, (last visited May 14, 2022) ("The Nuclear Suppliers Group (NSG) is a group of nuclear supplier countries that seeks to contribute to the non-proliferation of nuclear weapons through the implementation of two sets of Guidelines for nuclear exports and nuclear-related exports.").

150. *See Introduction*, WASSENAAR ARRANGEMENT, https://www.wassenaar.org (last visited May 14, 2022) ("The Wassenaar Arrangement has been established in order to contribute to regional and international security and stability, by promoting transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies, thus preventing destabilising accumulations.").

While AI regulations could be incorporated into one of these existing regimes, it would likely be more productive to establish a completely independent AI export control arrangement. Existing regimes would be strained by an attempt to prescribe regulatory measures for emerging technologies; for example, efforts to put controls on intrusion software under the Wassenaar Arrangement caused confusion and discontentment among government agencies and private actors in cybersecurity.[151] Eventually, members agreed to make changes to the intrusion software controls, but the changes may have caused more confusion and less conformity among states' export control policies in this area.[152] The integration of export controls on AI would surely cause further division and disorientation. Thus, the best way forward is to create a multilateral export control arrangement dedicated to AI and other emerging technologies. States would enter the arrangement with the shared understanding that the regulated technologies are constantly evolving; this would ensure that member states are relatively like-minded and willing to adjust as necessary.

However, in recommending a similar arrangement controlling the export of AI, the challenges associated with such regimes must be addressed. First and foremost, membership in any of these groups is optional; as such, some of the most important players, like Russia and China, may not join, meaning that they could continue to act as suppliers to malicious actors. Furthermore, these groups are frustrated by "an informal structure that allows some member governments to flout the norms, consensus rules that slow efforts to reform, discretionary implementation, and members with increasingly divergent interests."[153] Despite the downfalls, supporters maintain that these arrangements "play a key role in preventing terrorist attacks employing [weapons of mass destruction]."[154]

Therefore, states should form a multilateral export control regime for the export of hardware and software necessary to carry out AI attacks. Any arrangement of this sort must consider the dual-use capabilities of AI and the interests of states and independent parties in acquiring AI for peaceful uses. As such, transfers of AI technology should only be denied if government judges, after careful consideration of all available

151. *See* Garrett Hinck, *Wassenaar Export Controls on Surveillance Tools: New Exemptions for Vulnerability Research*, LAWFARE (Jan. 5, 2018, 9:30 AM), https://www.lawfareblog.com/wassenaar-export-controls-surveillance-tools-new-exemptions-vulnerability-research.

152. *See id.*

153. Michael D. Beck & Scott A. Jones, *The Once and Future Multilateral Export Control Regimes: Innovate or Die*, 5 STRATEGIC TRADE REV. 55, 73 (2019).

154. DEPT. OF ENERGY, NAT'L NUCLEAR SEC. ADMIN., *supra* note 145, at 17.

information, determine that the AI technology or related items are intended for malicious use, or there is a significant risk of diversion.[155] In making this determination, judges should consider relevant factors, including but not limited to the effectiveness of export control in recipient and intermediate states; the capabilities and objectives of the recipient state; past actions of the end-user, such as whether they have previously used, or intended to use, AI maliciously or whether they have previously diverted a transfer for unauthorized purposes.[156] An alternative to this self-judging model could be the formation of a board of independent arbiters tasked with approving export licenses. However, this is not the model that current regimes have adopted, likely because states would not be willing to join a group with this level of bureaucracy and external control. Instead, to ensure that each government complies with established controls, the arrangement should impose national reporting requirements and establish yearly meetings of state participants.[157]

A multilateral export control arrangement may be able to frustrate the efforts of NSAs to acquire weaponized AI. However, regulation on its own, while a step in the right direction, cannot entirely prevent AI-enabled armed attacks from occurring. Consequently, regulation cannot eliminate the possibility that a victim state will violate the sovereignty of a territorial state unable to prevent the use of its territory to carry out such an attack. Therefore, further measures, such as those previously discussed, must be taken in conjunction with creating a multilateral export control regime.

D. *Invest in AI Defense*

The regulation of AI could be supplemented by investing in defenses against weaponized AI. As AI development is expected to expand and alter the threat landscape,[158] states could take a wide range of approaches to this suggestion. One option is to invest in physical defenses, such as "radar, lidar, acoustic signature, or image recognition software" and "passive defense through physical hardening or nets."[159]

---

155. *See Guidelines for Transfers of Sensitive Chemical or Biological Items*, AUSTL. GRP. (June 2015), http://www.australiagroup.net/en/guidelines.html.

156. *Id.*

157. *See* WASSENAAR ARRANGEMENT SECRETARIAT, WA-DOC (19) PUB 007, WASSENAAR ARRANGEMENT ON EXPORT CONTROLS FOR CONVENTIONAL ARMS AND DUAL-USE GOODS AND TECHNOLOGIES 8 (Dec. 2019), https://www.wassenaar.org/app/uploads/2021/12/Public-Docs-Vol-I-Founding-Documents.pdf.

158. *See* BRUNDAGE ET AL., *supra* note 9, at 18.

159. *Id.* at 43.

States could also invest in cyber defenses, such as communications and GPS jamming technology, to combat autonomous drone swarms.[160] Autonomous weapon swarms could also be disrupted by "spoofing incoming data, generating signals in the environment to induce certain [] behaviors, or by direct communications hacking;"[161] as such, states could invest in technology and training to enhance autonomous weapon hijacking capability. While these defenses may be a good place for states to start, it is impossible to propose exactly what adequate defenses should look like, given that AI, as an emerging technology, is inherently in a state of flux.

Regardless of what form they take, increased defensive capabilities would help breach the aforementioned offense-defense gap, which contributes to the likelihood that an NSA could carry out an AI-enabled armed attack. Again, even if the gap could be breached overall, it is unlikely that *all* states could deploy comprehensive defenses to AI. Therefore, even with improved defenses against AI attacks, some NSAs may still carry out an AI attack from within the territory of or against a state lacking in such measures. While this means that further steps would be required to prevent the violation of state sovereignty, it does not suggest that states should forgo the pursuit of AI defense altogether. After all, if many states had adequate defenses in place to prevent the success of an attack, NSAs may determine that the cost of pursuing the technology is not worth the benefits. Furthermore, LDCs will ultimately benefit from the research and development of more developed states. As technology leaders like the United States enhance their capabilities to defend against weaponized AI, further implementation and development will likely become more feasible for LDCs. While improvement in defense will not eliminate the problem entirely, states should still invest in defenses against weaponized AI to reduce the potential success of an AI-enabled attack by NSAs.

160. *See* Stephen Carlson, *DARPA Tests Autonomous Drone Swarms Against Communications and GPS Jamming*, UNITED PRESS INT'L (Nov. 20, 2018, 3:17 PM), https://www.upi.com/Defense-News/2018/11/20/DARPA-tests-autonomous-drone-swarms-against-communications-and-GPS-jamming/2601542744659/ (reporting on DARPA test series for "autonomous drone operations in the face of enemy jamming and area-denial efforts.").

161. Paul Scharre, *Counter-Swarm: A Guide to Defeating Robotic Swarms*, WAR ON THE ROCKS (Mar. 31, 2015), https://warontherocks.com/2015/03/counter-swarm-a-guide-to-defeating-robotic-swarms/.

E. *Summary of Recommendations*

Investing in AI defense and implementing a multilateral control regime would reduce the likelihood that an NSA would be able to carry out an AI-enabled attack. However, as these actions alone will likely be insufficient to prevent all AI-enabled attacks by NSAs, the possibility remains that states would need to defend themselves. Therefore, this Note most strongly advocates for eliminating the "unable" element, not only within the context of emerging technologies but in all invocations of the doctrine. This recommendation most fairly addresses the competing interests of protecting state sovereignty and safeguarding the right to self-defense. Understanding that this modification may be opposed by some of the states that most frequently invoke and benefit from the current formulation of the doctrine, the alternative requirement of a showing of greater ability is strongly suggested. Although not as strong of a solution as eliminating the "unable" element altogether, this formulation of the doctrine will nonetheless increase transparency and promote autonomy and security. Each of these recommendations will help ensure that the UoU doctrine can address the challenges posed by the weaponization of emerging technologies.

VI. Conclusion

While this Note uses the AI case study to demonstrate the challenges associated with the use of the UoU doctrine in the age of emerging technologies, the doctrinal shift should not be limited to the context of AI or emerging technologies. Rather, an overall restriction on the invocation of the UoU doctrine will address many of the underlying issues with the current application of the doctrine; the recommendations set out herein will protect state sovereignty and help ensure that states can access necessary self-defense measures in an ever-changing world. The need for increased regulation and continued investment in defense similarly apply beyond the context of AI. Moreover, this Note demonstrates how some areas of international law are unprepared to cope with emerging technologies and evolving threats. Although the age of emerging technologies promises innovation and prosperity, it simultaneously threatens to destabilize global security and interrupt the legal regimes tasked with governing the use of force. States must be proactive in their efforts to anticipate and prepare for a new threat environment dominated by technological advancement.