الدراسة التاسعة:

الأضرار غير المادية الناتجة عن الأقمار الصناعية: عسكرة الأمن السيبراني والذكاء الاصطناعي في ضوء القانون الدولي

محمد عبد الهادي عبد الهادي[1]

Abstract

Intangible Damages Resulting from Satellites: The Militarization of Cybersecurity and Artificial Intelligence in the Light of International Law

This study dives into the legal and security changes brought about by the dual-use of satellites, especially considering the fast-paced advancements in cybersecurity and artificial intelligence. It also looks at the non-material damages that can affect international peace and security. Originally, satellite systems were created for humanitarian and scientific reasons, like enhancing inter-state communication, aiding in environmental and climate monitoring, and boosting precision navigation. However, the dual-use aspect of these technologies has opened the door for some states and private entities to misuse them for military or digital offensive actions, such as espionage, disrupting

[1] كلية الحقوق: قسم القانون العام / الجامعة الإسلاميّة في لبنان.

critical systems, interfering with vital infrastructure, and improperly accessing sensitive data. These actions can pose serious threats to international stability and national security.

The legal challenges stem from the reality that existing international agreements, like the 1967 Outer Space Treaty and the 1972 Convention on International Liability, fall short in addressing non-material damages. This includes the psychological, social, and economic impacts that arise from the misuse of these technologies. Additionally, the Rome Statute of the International Criminal Court (1998) has not yet included what could be called "technological aggression crimes." This is concerning, given the increasing need for a legal framework that criminalizes actions threatening international peace and collective security through cyber or space-based activities, ensuring that states or private entities that violate international law are held accountable.

This research takes a deep dive into the gaps in current international laws when it comes to tackling modern issues, particularly the non-material harms linked to the militarization of space, cybersecurity, and artificial intelligence. It suggests that we should add the idea of "space-based technological aggression" to the Rome Statute, aligning it with today's tech advancements. This would help protect the interests of nations and communities while also promoting international justice and collective security. The study highlights the urgent need to refresh international legal frameworks and create robust monitoring and accountability systems to ensure that space technology is used peacefully and sustainably, preventing any aggressive misuse of satellites and related digital systems.

Keywords: Satellites, Non-material harm, Cybersecurity, Artificial intelligence, Technological aggression, International law, Rome Statute.

المقدمة

في السنوات الأخيرة، شهد الفضاء الخارجي تحولات عميقة نتيجة للتطور السريع في تقنيات الذكاء الاصطناعي والأمن السيبراني. هذا التطور جعل الأقمار الصناعية تلعب دورًا محوريًا في أنظمة الدفاع والاستخبارات والاتصالات وإدارة البيانات على مستوى العالم. فقد تحولت الأقمار الصناعية من مجرد أدوات للمراقبة أو البث أو الملاحة إلى بنى تحتية رقمية حساسة تعتمد عليها الدول والمؤسسات في إدارة شؤونها الحيوية. ومع تزايد هذا الاعتماد، ظهرت أنماط جديدة من التهديدات التي تستهدف إلحاق أضرار غير مادية عبر الفضاء الخارجي، مثل تعطيل الأنظمة الرقمية الحيوية، واختراق شبكات الاتصالات، والتلاعب بالبيانات، أو شل البنى التحتية المعلوماتية. هذه الأضرار قد لا تترك أثرًا ماديًا مباشرًا، لكنها قادرة على إحداث تأثيرات استراتيجية تعادل، بل قد تفوق، الأفعال العسكرية التقليدية.

هذا التحوّل التكنولوجي أظهر مشكلة قانونية متزايدة تتعلق بحدود الإطار القانوني الدولي الذي ينظم الأنشطة الفضائية. وبالتحديد، يتعلق الأمر باتفاقية الفضاء الخارجي لعام 1967 واتفاقية المسؤولية لعام 1972، اللتين ركزتا بشكل شبه كامل على الأضرار المادية، مثل سقوط جسم فضائي أو التسبب في خسائر ملموسة. لكن الأضرار غير الملموسة الناتجة عن العمليات السيبرانية عبر الأقمار الصناعية لم تتناولها النصوص الحالية بشكل صريح أو لم تتضمن آليات واضحة للمسؤولية. هذا الفراغ القانوني أدى إلى ظهور منطقة رمادية تتيح نشوء نوع جديد من الاعتداءات، يمكن تسميته بـ "العدوان التكنولوجي الفضائي". هذا النوع من العدوان لا يمكن تصنيفه بسهولة ضمن التعريفات التقليدية للضرر أو استخدام القوة في القانون الدولي العام، رغم أنه يشكل تهديدًا للأمن القومي للدول واستقرار النظام الدولي بشكل عام.

لقد أدّى هذا الواقع إلى تعقيد المشهد الاستراتيجي العالمي، حيث لم تعد التهديدات الفضائية مقتصرة على الصدامات المادية أو سباقات التسلح التقليدي، بل أصبحت مرتبطة بقدرات رقمية متطورة تُدار عن بُعد، تستهدف المراكز الحيوية للدول دون الحاجة إلى تدخل عسكري مباشر. كما أن تداخل الفضاء الخارجي مع الفضاء السيبراني خلق بيئة جديدة تتشابك فيها المصالح الاقتصادية والعسكرية والتكنولوجية، مما جعل الدول تعتمد بشكل متبادل على البنى الفضائية. وهذا الأمر يزيد من خطورة أي اعتداء رقمي قد ينطلق من أحد الأقمار الصناعية

أو يستهدفها. وفي ظل هذا التعقيد، برزت الحاجة الملحة لتطوير مقاربات قانونية دولية تتماشى مع هذا التحول، وتعيد تعريف مفاهيم الضرر والاعتداء والسيادة في ضوء التهديدات الرقمية غير الملموسة.

– سبب اختيار الموضوع:

تم اختيار موضوع "**الأضرار غير المادية الناتجة عن الأقمار الصناعية: عسكرة الأمن السيبراني والذكاء الاصطناعي في ضوء القانون الدولي**" انطلاقًا من الحاجة العلمية الملحة لدراسة الفجوة القانونية التي تتسع مع الاستخدام المتزايد للتقنيات الفضائية الحديثة. في السنوات الأخيرة، أصبحت الدول تعتمد بشكل متزايد على الأقمار الصناعية في مجالات الاتصالات والملاحة وإدارة البيانات، بالتزامن مع دمج الذكاء الاصطناعي والأنظمة السيبرانية في هياكلها الوظيفية. هذا التداخل أدى إلى ظهور نوع جديد من المخاطر، يتمثل في الأضرار غير المادية التي قد تلحق بالدول دون أن تسبب دمارًا ماديًا تقليديًا، مثل تعطيل شبكات الاتصالات، شل أنظمة الملاحة، أو التلاعب بالبنى المعلوماتية. ونظرًا لأن الاتفاقيات الفضائية الحالية (وخاصة اتفاقية 1967 واتفاقية المسؤولية لعام 1972) لا تقدم معالجة واضحة لمسؤولية الدولة عن هذه الأضرار، فقد أصبح من الضروري اختيار هذا الموضوع لسد هذه الفجوة وتحليل الإشكاليات القانونية المرتبطة به من منظور معاصر يجمع بين القانون الفضائي والقانون الدولي السيبراني.

– أهمية الموضوع:

تتجلّى أهمية هذا البحث في تناوله لأحد أخطر التحولات التي يشهدها النظام الدولي اليوم، وهو عسكرة الذكاء الاصطناعي والأمن السيبراني عبر الأقمار الصناعية. فالأضرار غير المادية التي قد تنجم عن الهجمات الفضائية–السيبرانية تمتلك القدرة على زعزعة الأمن العالمي، حيث يمكن أن تستهدف البنى التحتية الحيوية للدول دون أن تترك أثرًا ماديًا مباشرًا، مما يجعل من الصعب إثبات المسؤولية الدولية وصد السلوك العدواني. كما أنّ الموضوع يكتسب أهميته من كونه يسلط الضوء على قصور الإطار القانوني الدولي الذي لا يزال يركز

بشكل رئيسي على الأضرار المادية التقليدية، متجاهلاً التهديدات الجديدة التي تطرحها الأنظمة الذكية والهجمات السيبرانية الموجهة عبر الفضاء. لذلك، يسهم البحث في فتح نقاش فقهي وقانوني حول ضرورة تحديث الأنظمة الدولية، مثل نظام روما الأساسي، لاستيعاب الجرائم ذات الطابع التكنولوجي، تمهيدًا لبناء منظومة قانونية أكثر قدرة على حماية السلم والأمن الدوليين في العصر الرقمي.

– إشكاليّة البحث:

إلى أي مدى يمكن اعتبار العمليات السيبرانية التي تُنفّذ عبر الأقمار الصناعية، والمدعّمة بالذكاء الاصطناعي، شكلاً من أشكال العدوان التكنولوجي المهدّد للسلم والأمن الدوليين؟

وينتج عن هذه الإشكالية سؤالين فرعيين:

– ما هو مفهوم الأضرار غير المادية الناشئة عن عسكرة الأمن السيبراني والذكاء الاصطناعي وما مدى خطورتها في الفضاء الخارجي على الأمن الإنساني والدولي؟

– إلى أي حد يكشف قصور اتفاقيتي 1967 و1972 عن حاجة لآلية دولية تُمكّن من تكييف العدوان التكنولوجي الفضائي كجريمة دولية وفق نظام روما الأساسي، ولا سيما المادة (8 مكرّر)؟

– هدف البحث:

يهدف هذا البحث إلى دراسة وتحليل الإطار القانوني الذي ينظّم استخدام الأقمار الصناعية، مع الأخذ في الاعتبار التطوّرات التكنولوجيّة في مجالي الأمن السيبراني والذّكاء الاصطناعي. يركّز البحث على الأبعاد القانونيّة والسياسيّة والأمنيّة للأضرار غير الماديّة الناتجة عن عسكرة هذه التقنيّات. كما يسعى إلى تقييم إمكانيّة إدراج المسؤوليّة الجنائيّة الدوليّة عن الأفعال العدوانيّة الرقميّة أو الفضائيّة ضمن إطار القانون الجنائي الدولي، وتحديد التحديّات التي تعيق ذلك. من جهة أخرى، يبرز البحث الدّور المزدوج للذكاء الاصطناعي؛ فهو أداة فعّالة لتعزيز أمن الفضاء ومراقبة السّلوكيات العدوانيّة، ولكنّه أيضًا يُشكّل خطرًا محتملاً إذا استُخدم لأغراض هجوميّة أو تجسسيّة عبر الأقمار الصناعيّة. كما ويهدف البحث

إلى تشكيل رؤية قانونية متكاملة توازن بين الاستخدام السّلمي للتكنولوجيا وحماية السلم والأمن الدوليين من التّهديدات غير الماديّة في الفضاء الخارجي.

– منهجية البحث:

اعتمد هذا البحث على منهج وصفي وتحليلي لدراسة الإطار القانوني الدولي المتعلق بالأضرار غير المادية الناتجة عن عسكرة الفضاء، مع التركيز على الأمن السيبراني والذكاء الاصطناعي. تم استخدام المنهج الوصفي لعرض وتحليل النصوص والمعاهدات الدولية الأساسية، مثل اتفاقية الفضاء الخارجي لعام 1967، واتفاقية المسؤولية الدولية لعام 1972، بالإضافة إلى اتفاقيات جنيف الأربع لعام 1949 والبروتوكولات الإضافية المتعلقة بالقانون الدولي الإنساني لعام 1977 و2005، ونظام روما الأساسي للمحكمة الجنائية الدولية. هذا المنهج ساعد في توضيح المبادئ القانونية السائدة ورصد الأسس التي تنظم حماية الأمن الدولي والبيئة الفضائية، بما في ذلك كيفية التعامل مع الأضرار غير المادية والتكنولوجية.

أما المنهج التحليلي، فقد تم استخدامه لتقييم مدى كفاية هذه النصوص القانونية في مواجهة التحديات المعاصرة، مثل الهجمات السيبرانية على الأقمار الصناعية، واختراق أنظمة الذكاء الاصطناعي، وأشكال العدوان التكنولوجي غير التقليدية. يركز التحليل على تشخيص الثغرات القانونية في الاتفاقيات الحالية، واستكشاف إمكانية تطبيق المادة 8 مكرر من نظام روما الأساسي على هذه الأفعال.

– خطة البحث:

ينقسم هذا البحث إلى مبحثين مترابطين، حيث يركز المبحث الأول على توضيح الإطارين النظري والأمني لعسكرة الفضاء، مستعرضًا تطور مفهوم الاستخدام العسكري للفضاء الخارجي، وكيف يتداخل مع مفاهيم الأمن السيبراني والذكاء الاصطناعي. كما يقوم بتحليل طبيعة الأضرار غير المادية التي قد تنتج عن هذه الممارسات، مثل التهديدات الرقمية، التجسس المعلوماتي، وتعطيل الأنظمة الفضائية الحيوية. أمّا المبحث الثاني فيتناول موضوع الأضرار غير المادية والعدوان التكنولوجي من منظور نظام روما الأساسي، حيث يسلّط الضوء على

التحديات التي تواجه إدراج هذا النوع من الأفعال ضمن الجرائم الدولية. ويبرز بشكل خاص غياب تعريف واضح للعدوان التكنولوجي الفضائي، بالإضافة إلى نقص الآليات القانونية الدولية المناسبة لإثبات المسؤولية والمساءلة. كما يستعرض هذا المبحث الحاجة الملحة لتطوير إطار قانوني حديث يتماشى مع التطورات التكنولوجية، ويضمن تحقيق العدالة الدولية في مواجهة أشكال العدوان غير التقليدية.

المبحث الأول: الإطار النظري والأمني لعسكرة الفضاء والأضرار غير المادية

تعتبر عسكرة الفضاء الخارجي إحدى أبرز مظاهر التحوّل في موازين القوى الدوليّة في العصر الحديث. لقد أصبح الفضاء ساحة حيويّة تتداخل فيها المصالح العسكريّة والتكنولوجيّة والاقتصاديّة. وقد ساهم التطوّر الكبير في مجالي الأمن السيبراني والذّكاء الاصطناعي في نقل المنافسة بين الدول من الأرض إلى الفضاء، حيثُ أصبح التحكّم في الأقمار الصناعيّة وشبكات الاتّصالات والمعلومات سلاحًا استراتيجيًا يتفوّق في تأثيره على الأسلحة التقليديّة.

لقد أدّى هذا التحوّل إلى ظهور أشكال جديدة من الصّراع تتجاوز حدود المواجهة الماديّة، حيثُ يُمكن إلحاق الضرر من خلال عمليّات رقميّة غير مرئيّة تمسّ بالأمن القومي للدول دون أن تترك دمارًا ماديًا واضحًا، إذ إنّ اختراق أنظمة الأقمار الصّناعية، أو تعطيل إشارات الملاحة، أو التجسّس على البيانات المرسلة من الفضاء، أصبحت أدوات حرب غير تقليديّة تُستخدم للتّأثير على البنية التحتيّة الحيويّة والمصالح الاستراتيجيّة للدول.

إنّ الاعتماد المتزايد على الأقمار الصناعيّة في مجالات الاتّصالات والمراقبة والملاحة جعلها هدفًا رئيسيًا للهجمات السيبرانية، والتي يُمكن أن تؤدّي إلى شلل في قطاعات حيويّة مثل الدّفاع والطاقة والمصارف والنقل. وبالرّغم من أنّ هذه الأفعال لا تتضمّن تدميرًا ماديًّا مباشرًا، إلاّ أنّها تُعتبر أضرارًا غير ماديّة تترك آثارًا عميقة على سيادة الدّول واستقرارها الاقتصادي والأمني.

تُظهر الحقائق في القانون الدولي أنّ النّظام التّشريعي الفضائي لا يزال غير قادر على مواجهة هذه التحدّيات الجديدة بشكلٍ كامل، حيثُ يفتقر إلى قواعد واضحة تحدّد المسؤوليّة عن الأضرار غير المادية الناتجة عن إساءة استخدام التقنيّات الفضائيّة. كما أنّ مفهوم

"العدوان" في القانون الدولي لا يزال مرتبطًا بالأعمال المسلّحة الماديّة، دون أن يتوسّع ليشمل الاعتداءات الرّقميّة أو التكنولوجيّة التي قد تكون أكثر خطورة في بعض الأحيان.

يطرح هذا الوضع تساؤلات مهمّة حول مدى إمكانيّة تعديل القواعد الحاليّة، ولاسيّما مبدأ حظر استخدام القوّة في العلاقات الدوليّة ومبدأ المسؤوليّة الدّوليّة عن الأفعال غير المشروعة، لتشمل الأفعال المتعلّقة بالتّكنولوجيا الفضائيّة، ممّا قد يفتح المجال لإعادة التّفكير في مفهوم العدوان الفضائي وتطويره ليتماشى مع واقع الحروب الرّقميّة الحديثة، بحيثُ يتمّ الاعتراف بالأضرار غير الماديّة كأفعال عدوانيّة تستدعي المساءلة القانونيّة ضمن إطار القانون الدولي الجنائي.

▪ المطلب الأول: المفاهيم الأساسية للأمن السيبراني والذكاء الاصطناعي

يُعرّف الأمن السّيبراني الفضائي بأنّه مجموعة من الإجراءات التقنيّة والتنظيميّة والقانونيّة التّي تهدف إلى حماية الأنظمة الرقميّة في الفضاء من أي نوع من الاختراقات أو التّخريب أو التّلاعب بالبيانات، بالإضافة إلى ضمان استمراريّة الخدمات الحيويّة التي تعتمد عليها الدول والمؤسّسات. يعتمد هذا النّوع من الأمن على مبدأ الوقاية المسبقة، والرّصد المستمرّ، والاستجابة السّريعة لأي تهديد أو هجوم إلكتروني قد يستهدف الأقمار الصناعيّة أو مراكز التحكّم الأرضيّة أو الشّبكات المرتبطة بها. وبالتّالي، يُشكّل نظامًا متكاملًا لحماية الفضاء الرّقمي من المخاطر التقنيّة والعدوان التّكنولوجي الذي قد يحدث في الفضاء الخارجي.[1]

مع تزايد استخدام الأقمار الصناعيّة في مجالات مثل الاتّصالات والمراقبة والاستشعار عن بُعد والملاحة وإدارة البيانات، أصبح الأمن السّيبراني جزءًا أساسيًا لضمان سلامة الأنظمة على المستويين الوطني والدولي. لم تعد الأقمار الصّناعية تقتصر على المهام المدنيّة أو العلميّة، بل أصبحت أدوات استراتيجيّة في المجالات العسكريّة والاستخباراتيّة، ممّا جعلها أهدافًا محتملة للهجمات السيبرانيّة التي قد تؤدّي إلى اضطرابات كبيرة في البنية التحتيّة للدّول.

---

[1] العدوان التكنولوجي يعني استخدام تكنولوجيا متطورة : مثل الهجمات السيبرانية، أنظمة الذكاء الاصطناعي، الأقمار الصناعية، أو الوسائل التقنية المؤتمتة، بطريقة تسبب أضرارًا كبيرة لدولة أخرى، سواء على مستوى بنيتها التحتية أو وظائفها الأساسية أو أمنها القومي، بحيث تكون آثارها مشابهة لاستخدام القوة المسلحة وفقًا لمعايير القانون الدولي (المادة 4/2 من ميثاق الأمم المتحدة وقرار 3314 لعام 1974.)

لذلك، أصبح الأمن السيبراني الفضائي خط الدّفاع الأول لحماية السيادة الرقميّة للدول وضمان أمنها المعلوماتي.[1]

يكتسب هذا المفهوم أهميّة قانونيّة دوليّة متزايدة، حيثُ يثير قضايا معقّدة تتعلّق بالمسؤوليّة الدوليّة عن الأفعال الضارّة التي تستهدف الأنظمة الفضائيّة، وحدود استخدام القوّة في الفضاء السيبراني، وطرق إثبات مصدر الهجمات التي غالبًا ما تكون غامضة وصعبة التتبّع. كما أنّ القوانين الدّوليّة الحاليّة، مثل اتفاقيّة الفضاء الخارجي لعام 1967، لم تتناول بشكلٍ صريح الأبعاد السيبرانية للأمن الفضائي، ممّا يترك فجوة قانونيّة واضحة في مواجهة التّهديدات الرّقمية العابرة للحدود.[2]

إنّ حماية الفضاء من الهجمات السّيبرانية أصبحت اليوم جزءًا أساسيًا من نظام الأمن الجماعي الدولي، إذ إنّ أي اعتداء على البنى التّحتيّة الفضائيّة لا يؤثّر على دولة واحدة فقط، بل يُمكن أن يؤدّي إلى اضطراب شامل في الاتّصالات والملاحة والاقتصاد العالمي. لذلك، فإنّ وضع قواعد قانونيّة ملزمة لتنظيم الأمن السيبراني في الفضاء يُعتبر خطوة حيويّة نحو تحقيق الاستخدام السلمي والمسؤول للتّكنولوجيا الفضائيّة وضمان استدامة بيئة الفضاء الخارجي لخدمة الإنسانيّة جمعاء.

الفرع الأول: الذكاء الاصطناعي ودوره في تطوير المنظومات الفضائية

يُعتبر الذّكاء الاصطناعي الفضائي إحدى أبرز مظاهر التطوّر التّكنولوجي في مجال استكشاف الفضاء وإدارته، وقد أصبح عنصرًا أساسيًّا في تشغيل الأقمار الصّناعية وإدارتها وتحليل بياناتها. تُستخدم خوارزميّات الذّكاء الاصطناعي في مجموعة متنوّعة من المهام، مثل معالجة الصور الفضائيّة العالية الدّقة، والتنبؤ بالأعطال التّقنيّة، ورصد التّغييرات البيئية

[1] فهد بن عبد الله الشمري، الأمن السيبراني في ضوء القانون الدولي العام. دار الجامعة الجديدة، الإسكندرية، 2021، ص. 56

[2] United Nations, (2022), Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security. New York: United Nations, p. 75.

والمناخيّة، بالإضافة إلى تحسين كفاءة الاتّصال ونقل المعلومات[1]. لقد ساهم هذا التطوّر في رفع مستوى الدقّة والسّرعة في اتّخاذ القرارات ضمن الأنظمة الفضائيّة، ممّا عزّز الاعتماد على التّشغيل الذاتي وقلّل من الحاجة للتدخّل البشري في إدارة المهمّات الفضائيّة.

ومع ذلك، فإنّ التّمادي في دمج الذّكاء الاصطناعي مع التقنيّات الفضائيّة قد أثار تحدّيات أمنيّة وأخلاقيّة وقانونيّة معقّدة، وبالتالي، يُمكن أن تتحوّل هذه الأنظمة المتطوّرة من أدوات علميّة وخدماتيّة إلى وسائل هجوميّة ذات طابع سيبراني. فالذكاء الاصطناعي الموجّه عسكريًّا أو الذي يتمّ التحكّم فيه عن بُعد يُمكن أن يُستخدم في التّلاعب بالبيانات الملاحيّة، أو تعطيل شبكات الأقمار الصناعيّة، أو تنفيذ هجمات رقميّة دقيقة تستهدف البنى التحتيّة الحيويّة للدول دون أن تترك آثارًا ماديّة واضحة.[2]

إنّ تسليح الذّكاء الاصطناعي في مجال الفضاء ينقل النّزاعات من إطارها التّقليدي إلى ساحة جديدة تُمارَس فيها أشكال من العدوان غير المادي، ممّا يعني أنّه يمكن إحداث أضرار استراتيجيّة، مثل تعطيل أنظمة الاتّصالات أو التّشويش على إشارات الملاحة أو اختراق أنظمة المراقبة، دون الحاجة إلى استخدام أسلحة تقليديّة. وبالتّالي، يُثير هذا النّوع من الأضرار تساؤلات عميقة حول كيفيّة إثبات المسؤوليّة الدوليّة وتحديد طبيعة العدوان الفضائي التّكنولوجي، ولاسيّما في ظلّ غياب نصوص قانونيّة واضحة تنظم هذا المجال.[3]

وبالتّالي، يظهر الذّكاء الاصطناعي الفضائي كأداة ذات حدين، فمن جهة يُمثّل وسيلة فعّالة لتعزيز الأنشطة الفضائيّة المدنيّة والعلميّة، ومن جهةٍ أخرى يُمكن أن يتحوّل إلى تهديد للأمن السّيبراني الفضائي وللسّيادة الرقميّة للدّول. لذا، من الضّروري إعادة النّظر في الأطر القانونيّة الدوليّة الحاليّة لضمان استخدام تقنيّات الذكاء الاصطناعي في الفضاء بشكلٍ مشروع، مع التّركيز على الشّفافيّة، والمساءلة، وحماية المصالح المشتركة للبشريّة.

---

(1) BRYSON, J. J., (2020), The Artificial Intelligence and International Law: How AI is Changing Global Security and Ethics. Cambridge University Press, p. 85.

(2) فهد بن عبد الله الشمري، الأمن السيبراني في ضوء القانون الدولي العام مرجع سابق، 2021، ص. 58.

(3) كريم العوضي، القانون الدولي للفضاء الخارجي وتحديات التكنولوجيا الحديثة. دار النهضة العربية، بيروت، 2019.

الفرع الثاني: التفاعل بين الذكاء الاصطناعي والأمن السيبراني

يشكّل التفاعل بين الذكاء الاصطناعي والأمن السيبراني نظامًا ديناميكيًا بيئة حاضنة للتّهديدات الرّقميّة العابرة للحدود. في الواقع، لم تعد الأدوات السّيبرانيّة تقليديّة، بل أصبحت مدعومة بخوارزميات قادرة على التعلّم الذاتي، والتكيّف، واتّخاذ قرارات تشغيليّة بسرعة تفوق الاستجابة البشريّة. يُمكن استخدام الذّكاء الاصطناعي في الهجمات عبر أدوات تستهدف نقاط الضّعف في شبكات الأقمار الصناعيّة، ومحرّكات الملاحة، وأنظمة التحكّم الأرضيّة، ممّا يُتيح بناء هجمات متزامنة ومنسّقة تقلّل من فرص اعتراضها أو تتّبع مصدرها.[1] من ناحية أخرى، يُستخدم الذّكاء الاصطناعي في آليّات الدّفاع لاكتشاف التّسلّلات، والتّنبؤ بسلوك المهاجمين، وإغلاق الثّغرات بشكل تلقائي، ممّا يخلق سباق تسلّح تقني بين نظم الهجوم والدفاع.

ينتج عن هذا التّفاعل نوع جديد من العدوان التّكنولوجي غير المادي، والذي يتميّز بعدم وجود عنف مادي مباشر، ويعتمد عوضًا عن ذلك على إحداث خلل في الوظائف الحيويّة والقدرات التّشغيليّة للدّول والمؤسّسات، ممّا يُثير مجموعة من المشكلات القانونيّة العمليّة، مثل صعوبة تحديد الجهة المسؤولة، وتعقيدات إثبات الأصل والتتبّع الجنائي الدولي، بالإضافة إلى التحدّي المتمثّل في مطابقة هذه الأفعال لمعايير تعريف "العدوان" أو "استخدام القوّة" في القانون الدّولي. كما أنّ السّرعة والتّلقائية في اتّخاذ القرارات من قبل الأنظمة المدعومة بالذّكاء الاصطناعي تُثير تساؤلات حول المسؤوليّة القانونيّة والاعتبارات الأخلاقيّة المتعلّقة بتفويض صلاحيّات حسّاسة لآلات قد تتخّذ قرارات لها تأثير سيادي.

وعليه، يتبيّن لنا وجود نقصًا في النّصوص الدّوليّة والآليّات القضائيّة والقانونيّة التي يمكن أن تُنظّم هذا التّفاعل الجديد، ممّا يستدعي التّفكير في تطوير معايير دوليّة متخصّصة تشريعيّة وتقنيّة تتعامل مع خصائص الذّكاء الاصطناعي مثل التلقائيّة، القابليّة للتعلّم، وغموض الخوارزميّات. كما يجب تحديد معايير لإثبات المسؤوليّة، وآليّات للتّعاون الاستخباراتي والقضائي بين الدول، بالإضافة إلى وضع ضوابط قانونيّة تتناسب مع الموقف. هذه المحاور

[1] Natarajan, R. (2019). The militarization of space: History and implications. Routledge.

أصبحت محطّ اهتمام متزايد في الأدبيّات الحديثة المتعلّقة بالأمن الفضائي والعدوان التّكنولوجي.[1]

▪ المطلب الثاني: القصور القانوني في الاتفاقيات الدولية المنظِّمة للفضاء الخارجي

بالرغم من التقدم التكنولوجي الهائل في مجالات الفضاء الخارجي، لا يزال النظام القانوني الدولي غير قادر على مواكبة هذا التحول السريع، خاصةً عندما يتعلق الأمر بالعدوان السيبراني والهجمات التكنولوجية غير المادية على الأقمار الصناعية. فبينما تركز الاتفاقيات الأساسية المتعلقة بالفضاء، مثل معاهدة الفضاء الخارجي لعام 1967 واتفاقية المسؤولية لعام 1972، على تنظيم استخدام الفضاء لأغراض سلمية ومنع الأسلحة، إلا أنها تفتقر إلى نصوص واضحة تتعلق بالهجمات السيبرانية أو التدخلات عبر الذكاء الاصطناعي، مما يترك ثغرات قانونية واسعة يمكن استغلالها لأغراض عدائية.

من ناحية أخرى، تُظهر اتفاقيات جنيف الأربع وبروتوكولاتها اللاحقة، التي تُعتبر الأساس للقانون الدولي الإنساني، محدوديتها في مواجهة الأفعال العدائية الرقمية والفضائية. فقد تم تصميم هذه الاتفاقيات لحماية المدنيين والممتلكات خلال النزاعات المسلحة التقليدية، مع التركيز على الأضرار المادية المباشرة، مثل القتل أو الإصابات أو تدمير الممتلكات، ولا تتناول الأضرار غير المادية الناتجة عن تعطيل الأنظمة الرقمية للأقمار الصناعية أو شبكات الاتصال، والتي يمكن أن تهدد الأمن القومي والاقتصاد العالمي دون أن تترك أثراً مادياً واضحاً.

تواجه المفاهيم التقليدية في اتفاقيات جنيف مثل "الهجوم"، و"الضرر"، و"الأعيان المحمية" تحديات كبيرة عند تطبيقها على النزاعات السيبرانية والفضائية. فاختراق الأقمار الصناعية يمكن أن يؤدي إلى شلل في البنى التحتية الحيوية، وتعطيل نظم الملاحة والاتصالات، أو حتى نشر الحطام الفضائي، مما يوازي التأثيرات المادية للهجمات العسكرية التقليدية. وهذا

[1] Zhang, L, (2023), Cyber Warfare and Outer Space Security: The Legal Challenges of Satellite-Based Artificial Intelligence Systems, Oxford University Press, p. 112.

يبرز الحاجة الملحة لتطوير تفسير حديث للمبادئ الأساسية للاتفاقيات، بحيث تشمل الأضرار غير المادية والتهديدات الرقمية. علاوةً على ذلك، لا توفر اتفاقيات جنيف وآليات البروتوكولات اللاحقة وسائل فعّالة للتحقيق، أو التتبع، أو الإثبات في الجرائم السيبرانية الفضائية. فغياب هياكل قضائية متخصصة وعدم وجود معايير موحدة لتحديد المسؤولية الدولية عن الأفعال غير المادية يجعل من الصعب محاسبة الدول أو الكيانات الفاعلة، مما يفتح المجال للاجتهادات السياسية أكثر من القانونية.

الفرع الأول: الثغرات القانونية في اتفاقيتي 1967 و1972 بشأن الأضرار غير الماديّة

تُعتبر اتفاقيّة الفضاء الخارجي التي تمّ اعتمادها في 27 كانون الثاني عام 1967، الأساس الذي بُنيت عليه القوانين الدّوليّة التي تُنظّم الأنشطة الفضائيّة. لقد وضعت هذه الاتفاقيّة المبادئ الأساسيّة التي تُحدّد سلوك الدّول في الفضاء، مثل مبدأ الاستخدام السّلمي للفضاء الخارجي، ومبدأ المنفعة المشتركة للبشريّة، بالإضافة إلى عدم خضوع الفضاء لأيّة سيادة وطنيّة، ومسؤوليّة الدول عن الأنشطة الفضائيّة التي تقوم بها كياناتها العامّة أو الخاصّة. وقد لعبت هذه الاتفاقيّة دورًا مهمًّا في تنظيم التّنافس الفضائي خلال فترة الحرب الباردة، حيثُ منعت تحويل الفضاء إلى ساحة للصّراع النّووي أو ميدان لتجارب الأسلحة التقليديّة.[1]

ومع ذلك، ورغم أهميّتها التّاريخيّة، جاءت الاتفاقيّة بصياغة عامّة ومجرّدة لا تتناسب مع التطوّرات التقنيّة السّريعة التي شهدناها في العقود الأخيرة. فهي لم تُميّز بين الاستخدام العسكري المشروع للفضاء (مثل المراقبة والاستطلاع والاتّصال) وبين الاستخدام العدواني الذي يحمل طابعًا هجوميًّا، ممّا جعل بعض الدول تستغلّ هذا الغموض لتبرير عسكرة أنشطتها الفضائيّة تحت ذريعة "الاستخدام السّلمي للأغراض الدفاعيّة". إنّ النّصوص الحاليّة لا تمنع نشر الأقمار الصّناعيّة ذات الأغراض العسكريّة أو تطوير أنظمة هجوميّة رقميّة في الفضاء، طالما لم يُثبت استخدامها الفعلي في أعمال عدوانيّة.

[1] سامي حداد، القانون الدولي العام وتحديات الفضاء السيبراني. بيروت: دار النهضة العربية، 2015، ص. 88.

إضافةً إلى ذلك، لم تتناول الاتفاقيّة الأضرار غير الماديّة التي قد تنجم عن الأنشطة السّيبرانيّة أو إساءة استخدام الذكاء الاصطناعي في إدارة الأقمار الصّناعيّة. في عام 1967، لم تكن موجودة مفاهيم الأمن السيبراني، والهجمات الرّقميّة، والاختراق الإلكتروني للأنظمة الفضائيّة ضمن الإطار التّقني أو القانوني الدولي[1]. لذا، تبقى نصوص الاتفاقيّة غير كافية للتّعامل مع الهجمات التي لا تترك أضرارًا ماديّة مباشرة، لكنّها قادرة على تعطيل البنى التحتيّة الفضائيّة، أو إيقاف الاتّصالات، أو التّلاعب بالبيانات المداريّة الحسّاسة. كما أنّ مبدأ المسؤوليّة الدّولية عن الأضرار المذكور في الاتفاقية ينطبق فقط على الأضرار الماديّة التي تُصيب الأشخاص أو الممتلكات، دون أن يشمل الأضرار الرقميّة أو الاقتصاديّة أو المعلوماتيّة التي قد تنتج عن أعمال عدائيّة غير ملموسة. وبالتّالي، يُشكّل هذا الفراغ القانوني تحديًا أمام إمكانيّة محاسبة الدول أو الشّركات الخاصّة عند تنفيذها هجمات سيبرانيّة فضائيّة لا تترك أثرًا ماديًا يمكن إثباته بسهولة.

وعليه، يُمكن القول أنّ اتّفاقيّة الفضاء الخارجي لعام 1967، رغم أنّها تُعتبر الأساس في القانون الدولي الفضائي، لم تعد كافية لتنظيم العلاقات الفضائيّة في عصرنا الحديث. فهي لم تُحدّد بوضوح مسؤوليّة الدول عن الأضرار غير الماديّة، ولم تقدّم آليّات للتّحقيق أو التّعويض عن الأفعال الرقميّة الضارّة، كما أنّها لم تتطرّق إلى أهميّة حماية البنية التحتيّة الرقميّة في الفضاء[2]. لذا، تبرز الحاجة إلى إعادة تفسير نصوص الاتفاقيّة بما يتماشى مع التطوّرات التّكنولوجيّة الحاليّة، أو حتّى وضع بروتوكول إضافي يوضح كيفيّة تنظيم القضايا المتعلّقة بالأمن السّيبراني في الفضاء، وتحديد مفهوم "العدوان التكنولوجي" كفعل قد يُشكّل تهديدًا للسّلم والأمن الدوليين، حتّى في ظلّ غياب استخدام الوسائل العسكريّة التقليديّة.

تُعتبر اتفاقيّة المسؤوليّة لعام 1972 من الرّكائز والأسس المهمّة في القانون الدّولي الذي يُنظّم الأنشطة الفضائيّة، حيثُ تهدف إلى تحديد المسؤوليّة عن الأضرار الماديّة التي قد تُسبّبها الأجسام الفضائيّة للدّول أو الأفراد. ومع ذلك، يبقى نطاقها محدودًا، حيثُ يركز فقط على الأضرار الماديّة الملموسة، متجاهلاً الأضرار غير الماديّة أو الرقميّة التي أصبحت تمثل

---

(1) Bryson, J. J., (2020), The Artificial Intelligence and International Law: How AI is Changing Global Security and Ethics, op cit, p. 87.

(2) فهد بن عبد الله الشمري، الأمن السيبراني في ضوء القانون الدولي العام مرجع سابق، 2021، ص. 60.

التّهديد الأكبر في عصر التّكنولوجيا الحديث، مثل التّجسّس السّيبراني، التّعطيل الرقمي، والتّأثير النفسي والاقتصادي على الدّول والمجتمعات[1].

إنّ هذا القصور في الفهم التّقليدي للمسؤوليّة الفضائيّة يعكس ضعفًا هيكليًا في الإطار القانوني للاتفاقيّات الفضائيّة، التي لم تتكيّف بعد مع التحولات الرّقميّة العميقة في بيئة الفضاء الخارجي. وفي ظلّ الزّيادة الكبيرة في استخدام الأقمار الصناعيّة وأنظمة الذّكاء الاصطناعي لإدارة الاتّصالات والملاحة والتّحليل الاستخباراتي، ظهرت أنماط جديدة من العدوان تُعرف بـ "العدوان التّكنولوجي الفضائي"، وهي أعمال عدائيّة تُنفّذ عبر الفضاء السّيبراني باستخدام تكنولوجيا متقدّمة قد تُسبّب أضرارًا استراتيجيّة كبيرة، دون أن تترك أثرًا ماديًّا مباشرًا.

تُعتبر معظم الاتفاقيّات الفضائيّة، مثل اتفاقيّة الفضاء الخارجي لعام 1967، واتفاقيّة المسؤوليّة لعام 1972، واتفاقيّة التسجيل لعام 1975، مصمّمة للتّعامل مع الحوادث التّقليديّة، مثل تحطم الأقمار الصناعيّة أو سقوط الحطام الفضائي على الأرض، ولكنّها لم تتطرّق إلى الأفعال العدوانيّة الرقميّة التي يمكن أن تعطّل أنظمة الملاحة، أو تزعج شبكات الاتّصالات، أو تخترق قواعد البيانات الفضائيّة الحيويّة. لذلك، يتّضح أنّ النظام القانوني الدولي يعاني من فراغ تشريعي كبير، ممّا يجعل من الصعب تصنيف هذه الأفعال ضمن مفهوم "العدوان" أو "استخدام القوة" كما هو محدّد في ميثاق الأمم المتّحدة. فالهجمات الرقميّة قد لا تترك آثارًا ماديّة، لكنّها قادرة على تدمير البنى التحتيّة الإلكترونيّة، ممّا يُهدّد الأمن القومي للدّول ويزعزع الاستقرار الدولي.[2]

يترتّب على هذا الفراغ غياب آليّات واضحة للمساءلة والتّعويض، سواء من حيثُ تحديد الجهة المسؤولة أو كيفيّة إثبات وقوع الضّرر الرّقمي، في ظلّ طبيعة هذه الهجمات التي تتّسم بالغموض وسرعة التّنفيذ والانتشار عبر الحدود. فالهجمات السّيبرانيّة يُمكن أن تُنفّذ من عدّة مصادر متداخلة، ممّا يجعل تتبّعها وإثبات صلتها بدولة أو كيان معيّن أمرًا بالغ الصّعوبة، ممّا يُعيق تطبيق مبدأ المسؤوليّة الدّوليّة أو فرض العقوبات المناسبة.

---

(1) TRONCHETTI, F., Fundamentals of space law and policy, Kluwer Law International, 2020, p.63.

(2) سامي حداد، القانون الدولي العام وتحديات الفضاء السيبراني، مرجع سابق، 2015، ص. 89

لذلك، ظهرت الحاجة الملحّة إلى تطوير الإطار القانوني الدولي، سواء من خلال تعديل اتّفاقية المسؤوليّة لعام 1972 لتشمل الأضرار غير الماديّة، أو عبر إبرام معاهدات جديدة تُنظّم العدوان التّكنولوجي الفضائي ضمن قواعد واضحة للمساءلة والردّ. ويُفترض أن يتضمن هذا التحديث القانوني تعريفًا دقيقًا للعدوان التّكنولوجي، ومعايير لتحديد النيّة العدائيّة، إضافةً إلى آليّات للرّصد، والتّحقيق، والتّعويض.

إنّ حماية الفضاء الخارجي من التهديدات الرقميّة أصبحت ضرورة حتميّة لضمان استدامة الأنشطة الفضائيّة وسلامتها، ولمنع تحوّل الفضاء إلى ساحة مواجهة إلكترونيّة تُهدّد السلم والأمن الدّوليين. ومن ثمّ، فإنّ إصلاح النّظام القانوني الفضائي الدّولي لم يعد خيارًا ترفيهيًا، بل مطلبًا استراتيجيًّا يفرضهُ التطوّر التّكنولوجي السّريع وواقع الترابط بين الفضاءين الفيزيائيّ والرّقمي.

الفرع الثاني: محدودية اتفاقيات جنيف في النزاعات السيبرانية والفضائية

رغم أن الفضاء الخارجي لم يُعتبر بشكل صريح ضمن مجالات النزاعات المسلحة التقليدية التي تناولتها اتفاقيات جنيف لعام 1949 والبروتوكولات الإضافية لعامي 1977 و2005، إلا أن مبادئ القانون الدولي الإنساني التي تشكل جوهر هذه الاتفاقيات تظل ذات صلة وثيقة عند النظر في عسكرة الفضاء وظهور الأضرار غير المادية الناتجة عن الهجمات السيبرانية عبر الأقمار الصناعية. فقد وضعت هذه الاتفاقيات قواعد عامة تتعلق بضرورة التمييز بين الأهداف المدنية والعسكرية، والتناسب في استخدام القوة، وحظر الهجمات العشوائية، بالإضافة إلى واجب اتخاذ الاحتياطات اللازمة عند التخطيط أو تنفيذ أي عملية عسكرية[1]. وعلى الرغم من أن هذه المبادئ صيغت في سياق النزاعات الأرضية التقليدية، إلا أنها أصبحت اليوم تُطبق على العمليات العسكرية الرقمية التي تتم عبر الأنظمة الفضائية، حيث أن القانون الدولي الإنساني لا يقتصر على وسيلة القتال، بل يركز على المخاطر التي تشكلها على المدنيين والبنى التحتية الحيوية.

(1) SCHMITT, N., (2020), "International Law and Military Operations in Space." Harvard National Security Journal, p.76-83

تكتسب البروتوكولات الإضافية أهميتها لأنها وسّعت نطاق الحماية ليشمل الأعيان المدنية الحيوية التي قد تتأثر بشكل مباشر بالعمليات السيبرانية الفضائية، مثل شبكات الكهرباء، أنظمة النقل الجوي، الاتصالات، والمنشآت الحيوية ذات الطابع الإنساني[1]. لذا، فإن الهجمات الرقمية التي تُنفّذ عبر الأقمار الصناعية والتي تؤدي إلى تعطيل هذه المنشآت أو تقليل قدرتها على أداء وظائفها قد تُعتبر، وفقًا لمبادئ جنيف، استخدامًا غير مشروع للقوة أو حتى هجومًا محظورًا إذا أثرت على حياة المدنيين أو تسببت في أضرار لا تتناسب مع الهدف العسكري المراد تحقيقه. ومع ذلك، يبقى الإشكال قائمًا في غياب قواعد واضحة تُحدد كيفية توصيف "الضرر غير المادي" ضمن إطار هذه الاتفاقيات، خاصة عندما لا يترك الهجوم أثرًا ماديًا مباشرًا[2]، بل يؤدي إلى شلل وظيفي بالغ الخطورة.

إنّ هذا الواقع يطرح تحديًا آخر، وهو أن اتفاقيات جنيف لم تتناول استخدام الأنظمة الفضائية كوسيلة أو ساحة للهجمات السيبرانية. وهذا الفراغ يستغله عدد من الدول لتبرير ممارسات هجومية يصعب إخضاعها لمساءلة قانونية واضحة، خاصة عندما تتم عبر شبكات اصطناعية أو أقمار صناعية تُدار بواسطة الذكاء الاصطناعي. لذا، هناك حاجة ملحة لتطوير تفسير حديث لاتفاقيات جنيف يأخذ في الاعتبار خصوصية الفضاء الخارجي، حيث تشكل الأضرار غير المادية تهديدًا مباشرًا للسلم والأمن الدوليين. ومن الضروري بالتالي إدماج مفهوم "العدوان التكنولوجي" ضمن قواعد القانون الدولي الإنساني.

على الرغم من أن اتفاقيات جنيف الأربع وضعت قواعد شاملة لحماية المدنيين والممتلكات المدنية، إلا أنها تفتقر إلى نصوص واضحة تتعلق بالهجمات السيبرانية أو الأضرار الرقمية غير المادية. كما أن البروتوكولين الإضافيين لعام 1977، رغم تطور محتوياتهما، لم يتناولا مسألة الهجمات التي تستهدف الأنظمة الفضائية أو الرقمية، لأن التكنولوجيا لم تكن قد وصلت إلى هذا المستوى في ذلك الوقت. ومع ذلك، تظل مبادئ اتفاقيات جنيف قابلة للتطبيق من حيث الوظيفة، حيث يُلزم المبدأ العام للتمييز بعدم استهداف الأعيان المدنية حتى لو كان

(1) BORELLI, S., (2017), "Cyber Operations and the Notion of ‘Attack’ in International Humanitarian Law." Yearbook of International Humanitarian Law, p.127.

(2) DORADO, J., (2022), "Artificial Intelligence and Autonomous Systems in Space Security", Space Policy, p.75-78.

الهجوم سيبرانيًا أو غير مادي. لكن غياب النصوص الواضحة يخلق فراغًا قانونيًا يسمح للدول باستخدام الأقمار الصناعية لتنفيذ عمليات رقمية عدوانية دون وجود آلية واضحة للمساءلة.

تزداد خطورة هذا الفراغ عندما نتحدث عن الذكاء الاصطناعي، حيث يمكن استخدام الأنظمة الذاتية لتنفيذ هجمات رقمية معقدة تستهدف شبكات الملاحة، أقمار الاتصالات، أو مراكز التحكم، دون أن تُسجل أي أضرار مادية، ودون أن يتضح ما إذا كانت هذه الهجمات تُعتبر "هجومًا" وفقًا للقانون الدولي الإنساني[1]. لذلك، يتضح أن النظام القانوني الحالي، سواء كان قانون الفضاء أو قانون النزاعات المسلحة، غير قادر على استيعاب الطبيعة الجديدة للتهديدات الناجمة عن عسكرة الأمن السيبراني والذكاء الاصطناعي في الفضاء.[2] هذا القصور يمثل العقبة الرئيسية أمام تصنيف "العدوان التكنولوجي الفضائي" كجريمة دولية مستقلة، ويبرز الحاجة إلى تطوير آليات قانونية أكثر حداثة تتناسب مع طبيعة الأضرار غير المادية وطرق تنفيذها.

وعليه، يكشف تحليل هذا الإطار القانوني عن مشكلة أساسية تتعلق بمدى قدرة مبادئ القانون الدولي على التكيف مع التحولات الكبيرة في طبيعة النزاعات المسلحة. فالاتفاقيات التي وُضعت في منتصف القرن العشرين كانت تستند إلى افتراضات تقليدية حول طبيعة الضرر، حيث كانت تحدد الضرر غالبًا بالأفعال الحركية التي تترك أثرًا ماديًا يمكن قياسه أو تقديره. لكن مع ظهور التكنولوجيا الفضائية والسيبرانية، تغير مفهوم "الضرر" بشكل جذري ليشمل أنماطًا غير مادية تعتمد على تعطيل وظائف الأنظمة بدلاً من تدمير بنيتها.

المبحث الثاني: الأضرار غير المادية والعدوان التكنولوجي في ضوء نظام روما الأساسي

تتّخذ الأضرار غير الماديّة النّاتجة عن عسكرة الفضاء، وخاصّة من خلال الأمن السّيبراني والذّكاء الاصطناعي في الأقمار الصّناعيّة، أشكالًا متعدّدة تتجاوز مجرّد الخسائر الماديّة التّقليديّة. فهي تشمل شلّ الأنظمة الحيويّة للدّول، وتعطيل شبكات الاتّصالات والملاحة،

[1] ibid

[2] ESTEFAN, N., (2021), "Non-Kinetic Warfare and International Law: The Challenge of Non-Material Harm", Journal of Conflict & Security Law, p.59.

والتلاعب بالبيانات المداريّة، والتّأثير على نظم الإنذار المبكر، والتدخّل في عمليّات التحكّم وإدارة المعلومات الاستراتيجيّة. كما يمكن أن تؤدّي إلى خسائر اقتصاديّة وأمنيّة بعيدة المدى تؤثّر على الاستقرار الوطني والدولي، خصوصًا عند استهداف البنى التحتيّة الحرجة المرتبطة بالفضاء، مثل أنظمة الطّاقة، والنقل، والدفاع، والاتّصالات.

تُثير هذه الأفعال تساؤلات قانونيّة معقّدة حول إمكانيّة تصنيفها ضمن مفهوم العدوان التكنولوجي، ممّا قد يسمح بإدراجها ضمن نطاق اختصاص المحكمة الجنائيّة الدّوليّة وفق نظام روما الأساسي. فالأفعال الرقميّة التي تُحدث أضرارًا استراتيجيّة غير ملموسة، رغم عدم تسبّبها في دمار مادي مباشر، قد تُعتبر انتهاكًا للسلم والأمن الدّوليين إذا ارتكبت على نطاق واسع أو استهدفت البنى التحتيّة الحيويّة، ممّا يستدعي إعادة التّفكير في تعريف العدوان وأشكاله في القانون الدولي المعاصر.

إنّ هذا النّوع من الأضرار يُسلّط الضّوء على الفجوات القانونيّة والتّشريعيّة الواضحة في النّظام الدولي. فالمعاهدات الفضائيّة التّقليديّة، مثل اتفاقيّة الفضاء الخارجي لعام 1967، تفتقر إلى نصوص واضحة تتناول الأضرار الرقميّة وغير الماديّة، بالإضافة إلى المسؤولية عن الأفعال السّيبرانيّة في الفضاء. وهذه الثّغرات القانونيّة تجعل من الصّعب محاسبة الجهات الفاعلة، سواء كانت دولًا أو كيانات خاصّة، كما تُعيق فرض عقوبات محدّدة أو توفير آليات تعويض فعّالة للمتضررين.

▪ المطلب الأول: طبيعة الأضرار غير المادية الناتجة عن عسكرة الأقمار الصناعية

تظهر الأضرار غير الماديّة النّاتجة عن عسكرة الأقمار الصّناعيّة على شكل خسائر استراتيجيّة ومعلوماتيّة تتجاوز الأضرار الماديّة التقليديّة، ممّا يؤثّر على الأمن القومي والدّولي وقدرة الدول والمؤسّسات على حماية ممتلكاتها الحيوية. وتشمل هذه الأضرار تعطيل الأنظمة الحيويّة للأقمار الصناعيّة المستخدمة في الملاحة والاتّصالات والمراقبة، ممّا قد يؤدّي إلى

شلل مؤقّت أو دائم في العمليّات المدنيّة والعسكريّة ويؤثر بشكل مباشر على القدرة التشغيلية للدول.[1]

تتجاوز آثار هذه الأضرار المعلومات الاستراتيجيّة، حيثُ تُعتبر الأقمار الصّناعيّة المصدر الرّئيسي للبيانات الاستخباراتيّة والملاحيّة والمناخيّة. إنّ أي تدخّل أو تعديل في هذه البيانات يُمكن أن يؤدي إلى خلل في اتّخاذ القرارات الاستراتيجيّة ويخلق تشويشًا متعمّدًا في العمليّات المدنيّة والعسكريّة. بالإضافة إلى ذلك، فإن الأضرار الاقتصاديّة النّاتجة عن عسكرة الأقمار الصناعيّة قد تكون كبيرة، حيثُ يؤدّي تعطيل شبكات الاتّصالات والملاحة إلى توقّف الخدمات الحيويّة وتعطّل البنية التّحتيّة الرّقميّة، ممّا يؤثّر على النّقل والطّاقة والتجارة والخدمات المصرفيّة، ويترتّب عليه خسائر ماليّة ضخمة.

إنّ الاعتماد المتزايد على الذّكاء الاصطناعي والأمن السيبراني في إدارة الأقمار الصناعيّة يُمكن أن يضعف الاقتصاد الوطني والدولي. بالإضافة إلى ذلك، إنّ بعد أمني سيبراني يجعل هذه الأنظمة عرضة للاختراقات والهجمات الرقميّة المستمرّة، ممّا يصعّب حماية البيانات والمعلومات الفضائيّة الحسّاسة بشكلٍ كامل، وبالتّالي تحمل هذه الأفعال أبعادًا استراتيجيّة ونفسيّة تؤثّر على الثّقة بين الدّول في استخدام الفضاء لأغراض سلميّة.

كما يمكن أن تساهم في تصعيد التوتّرات السّياسيّة أو العسكريّة بسبب المخاطر المرتبطة باختراق الأنظمة الحيويّة أو سرقة المعلومات الاستراتيجيّة الحسّاسة. من الواضح أنّ الأضرار غير الماديّة النّاتجة عن عسكرة الأقمار الصناعية لها تأثيرات طويلة المدى على الأمن الدولي والاستقرار الاقتصادي والسياسي والاجتماعي. لذا، لا بدّ من تطوير أطر قانونيّة دوليّة متقدّمة تضمن التصدّي لهذه المخاطر وتحقّق مساءلة فعّالة للجهات المسؤولة عن العدوان التّكنولوجي الفضائي، سواء كانت دولًا أو كيانات خاصّة. كذلك، يجب وضع معايير واضحة لتحديد المسؤوليّة وآليّات للرّصد والتتبّع والرد القانوني المناسب مع طبيعة هذه الهجمات الرقميّة، لضمان الاستخدام السلمي والمستدام للفضاء وحماية المصالح المشتركة للبشريّة، وجعل الفضاء بيئة آمنة وموثوقة للنّشاط العلمي والتكنولوجي.

---

[1] LEWIS, J. A., (2021), Cybersecurity and the Militarization of Outer Space: Emerging Legal and Ethical Issues. International Review of Law and Security Studies, 9(1), p.56.

الفرع الأول: التهديدات القانونية الناشئة عن التجسس الرقمي في البيئة الفضائية

تُستخدم الأقمار الصناعيّة الحديثة لجمع معلومات حساسة عن الدول الأخرى أو عن المواطنين، بما في ذلك البيانات الاستخباراتيّة والملاحيّة والاقتصاديّة والمناخيّة، ممّا قد يؤدّي إلى انتهاك السّيادة الوطنيّة ويعرّض الدول لمخاطر استراتيجيّة كبيرة، دون أن تترتب أضرار ماديّة مباشرة.[1] يُعتبر هذا النّوع من الأنشطة ضمن الأضرار غير الماديّة، والتي يمكن تصنيفها كجزء من العدوان الرقمي الدولي. فالتجسّس الرّقمي يمكّن المهاجم من السّيطرة على المعلومات الحيويّة والتّأثير على قرارات الدولة في المجالات العسكريّة والاقتصاديّة والسياسيّة.

كما أنّه يخلق حالة من عدم اليقين تُضعف الثّقة الدّوليّة في استخدام الفضاء لأغراض سلميّة. بالإضافة إلى ذلك، يُمكن أن يؤدّي هذا النّوع من التجسّس إلى آثار طويلة المدى، تشمل الاستغلال الاقتصادي، والتّشويش على العمليّات المدنيّة والعسكريّة، والإضرار بالمصالح الحيويّة للدّولة، ممّا يجعلها في موقف ضعف أمام التّهديدات الخارجيّة. من الواضح أنّ التجسّس الرّقمي عبر الأقمار الصناعيّة يُمثّل تحدّيًا كبيرًا[2].

لا يُعتبر هذا مجرّد نشاط استخباراتي تقني، بل يُشكّل تهديدًا حقيقيًا للأمن الدّولي والاستقرار السياسي والاقتصادي للدّول. كما يؤثّر على قدرتها في حماية البنى التحتيّة الرقميّة والاستراتيجيّة. بالإضافة إلى ذلك، يخلق هذا الوضع فجوة قانونيّة واضحة، حيثُ تفتقر معظم الاتفاقيّات الدّوليّة إلى نصوص صريحة تعالج هذه الممارسات الرقميّة وتتعامل مع الأضرار غير الماديّة الناتجة عنها. لذا، يتطلّب الأمر تطوير أطر قانونيّة دوليّة متخصّصة لتحديد مسؤوليّة الدول والجهات الفاعلة الخاصة عن التجسّس الرّقمي، ووضع معايير واضحة للرّصد والتتبع والمساءلة.[3]

---

[1] سامر محمد فاخوري، القانون الدولي للفضاء الخارجي بين الأمن السيبراني والتطبيقات العسكرية، دار الحامد، عمّان، 2023، ص. 112–114.

[2] خالد إبراهيم منصور، "تحديات التجسس الفضائي في ظل الثورة الرقمية: قراءة قانونية." مجلة البحوث القانونية والسياسية، العدد 18، 2021، ص. 76–85.

[3] Al TAMIMI, H., (2021), Cyber threats and satellite security, International Journal of Cyber Studies, 14(2), p. 43.

علاوةً على ذلك، يجب توفير آليّات فعالّة للرّد القانوني تضمن حماية السّيادة الوطنيّة واستدامة الاستخدام السّلمي للفضاء. ويؤكّد هذا التوسّع في نطاق التجسّس الرّقمي على الحاجة الملحّة لتعزيز التعاون الدولي بين الدول لضبط الأنشطة السيبرانية الفضائيّة، ووضع بروتوكولات وقواعد تحكم جمع المعلومات واستخدامها، بما يوازن بين المصالح الوطنيّة والأمن الدولي، ويحمي الأفراد والمجتمعات من الأضرار غير الماديّة النّاتجة عن الاستغلال غير المشروع للأقمار الصناعيّة[1].

الفرع الثاني: الآثار النفسية والاجتماعية للهجمات الرقمية الفضائية

إنّ الأضرار غير الماديّة الناتجة عن عسكرة الأقمار الصناعيّة تظهر على شكل خسائر استراتيجيّة ومعلوماتيّة، تمتدّ آثارها إلى الأمن القومي والدولي دون أن تترك أثرًا ماديًا مباشرًا على الأفراد أو الممتلكات. تشمل هذه الأضرار تعطيل الأنظمة الحيويّة للأقمار الصّناعيّة المستخدمة في الملاحة والاتّصالات والمراقبة، ممّا يؤدّي إلى شلل مؤقّت أو دائم في العمليّات المدنيّة والعسكريّة، ويؤثّر بشكل مباشر على القدرة التشغيليّة للدول.[2]

كما تمتدّ هذه الأضرار إلى المعلومات الاستراتيجيّة، حيثُ تُعتبر الأقمار الصناعيّة المصدر الرّئيسي للبيانات الاستخباراتيّة والملاحيّة والمناخيّة. إنّ أي تدخل أو تعديل في هذه البيانات يمكن أن يؤدّي إلى خلل في اتّخاذ القرارات الاستراتيجيّة، ويخلق تشويشًا متعمدًا في العمليّات المدنيّة والعسكريّة.

علاوةً على ذلك، فإنّ تعطيل البنية التحتيّة الرّقميّة الحيويّة للدول، بما في ذلك شبكات الطّاقة والاتّصالات والملاحة، يؤدّي إلى أضرار اقتصاديّة جسيمة وتأثيرات نفسيّة واجتماعيّة غير ماديّة تؤثّر على المجتمعات والدول على حد سواء. وقد أظهرت التّجارب الدوليّة أن نشر التقنيّات الفضائيّة السّيبرانية العدائيّة يُحدث تأثيرًا نفسيًا ملموسًا على المجتمع الدولي، خاصّةً

(1) LEWIS, J. A. (2021), Cybersecurity and the Militarization of Outer Space: Emerging Legal and Ethical Issues, 9(1), p.58.
(2) ZHANG, L., (2023), AI and cybersecurity in outer space: Emerging threats, Springer, p. 129.

عند استخدامها لتهديد الأمن المدني أو تعطيل الخدمات الحيويّة، ممّا يؤدي إلى زعزعة الثّقة في المؤسّسات الوطنيّة والدّولية وخلق حالة من عدم اليقين[1].

إنّ التجسّس الرقمي عبر الأقمار الصناعيّة يطرح تحدّيات كبيرة للدول من حيث انتهاك السّيادة الوطنيّة، حيثُ يمنح الجهات الفاعلة القدرة على التحكّم في المعلومات الحيويّة والتّأثير على القرارات في المجالات العسكريّة والاقتصاديّة والسياسيّة. يُعتبر هذا النّوع من الأضرار غير المادية جزءًا من مفهوم العدوان الرقمي الدولي، ممّا يستدعي تطوير أطر قانونيّة واضحة للتّعامل معه.

ولا بدّ من الإشارة إلى أنّ الأضرار غير الماديّة الناتجة عن عسكرة الأقمار الصناعيّة لها تأثيرات طويلة المدى واستراتيجيّة على الأمن الدولي والاستقرار الاقتصادي والسياسي والاجتماعي. لذا، من الضّروري تطوير أطر قانونيّة دوليّة متقدّمة تضمن مساءلة الجهات المسؤولة عن العدوان التكنولوجي الفضائي، سواء كانت دولًا أو كيانات خاصّة.

كما ويجب وضع معايير واضحة للرّصد والتتبع والرد القانوني بما يتناسب مع طبيعة هذه الهجمات الرقميّة، لضمان الاستخدام السلمي والمستدام للفضاء وحماية المصالح المشتركة للبشريّة وتعزيز الثّقة الدوليّة في تكنولوجيا الفضاء الحديثة.[2]

▪ المطلب الثاني: العدوان التكنولوجي وإشكاليّة إدراجه ضمن نظام روما الأساسي

يشير مفهوم العدوان التكنولوجي إلى الاستخدام المتعمد للتقنيات الحديثة، مثل الأقمار الصناعية، والأنظمة السيبرانية، والذكاء الاصطناعي، بهدف إلحاق أضرار غير مادية بالدول أو المجتمعات، دون الحاجة إلى تدمير مادي مباشر. يتضمن ذلك تعطيل البنى التحتية الحيوية، والتدخل في نظم المعلومات الوطنية، والتجسس الرقمي، واستغلال البيانات الاستراتيجية بطرق غير مشروعة. هذا النوع من العدوان يشكل تهديدًا معاصرًا للأمن الدولي،

[1] Al TAMIMI, H. (2021), Cyber threats and satellite security, op cit, p. 45–63.
[2] LEWIS, J. A. (2021). Cybersecurity and the Militarization of Outer Space: Emerging Legal and Ethical, op cit, p. 45–72.

حيث يتيح للجهات الفاعلة تحقيق أهداف سياسية واستراتيجية عبر وسائل رقمية وتقنيات فضائية متقدمة، مما يقلل من احتمالية اندلاع النزاعات العسكرية التقليدية. وهذا يطرح على القانون الدولي تحديات جديدة تتعلق بمفهوم العدوان والمساءلة.

على الرغم من وجود نظام روما الأساسي للمحكمة الجنائية الدولية، إلا أن النصوص الحالية لا تتناول بشكل صريح الهجمات التكنولوجية غير المادية، بما في ذلك استخدام الأقمار الصناعية لأغراض عدوانية. وقد أصبحت المادة 8 مكرر أداة مهمة محتملة لتوسيع نطاق تعريف العدوان، حيث تشير إلى الأفعال التي تلحق أضرارًا جسيمة وطويلة الأمد بالبيئة. يمكن توسيع مفهوم البيئة ليشمل الفضاء الخارجي والأنظمة المدارية، مما يجعل الهجمات السيبرانية والفضائية ذات الطابع العدواني قابلة للتصنيف كأعمال عدوانية ذات مسؤولية دولية.

ومع ذلك، لا يزال تحدي إرساء المسؤولية الدولية قائمًا، بسبب التعقيد الذي يميز الفضاء السيبراني والفضاء الخارجي. فإثبات وقوع الهجوم، وتعقب المسؤولين، وإثبات التعمّد والنية العدائية يمثل تحديًا كبيرًا أمام الأنظمة القانونية التقليدية، خاصة في ظل غياب آليات فعّالة للتحقيق الدولي في الجرائم الرقمية المتعلقة بالفضاء. كما أن الإطار القانوني الحالي، بما في ذلك اتفاقيات جنيف الأربع والبروتوكولات اللاحقة، يركز بشكل أساسي على النزاعات المسلحة التقليدية والأضرار المادية، ولا يتناول بشكل واضح التهديدات الرقمية أو التدخلات السيبرانية في الفضاء، مما يترك فراغًا قانونيًا يمكن أن تستغله الدول أو الفاعلون غير الدوليين.

علاوة على ذلك، يتضح القصور في تنسيق القوانين الوطنية والدولية المتعلقة بالأنشطة الفضائية والأمن السيبراني، حيث لا تزال معظم التشريعات تركز على حماية الأضرار المادية التقليدية، متجاهلة الأبعاد الرقمية والفضائية للتهديدات المعاصرة. وهذا يؤدي إلى غموض في كيفية الرد القانوني على العدوان التكنولوجي في الفضاء، مما يفتح المجال للاجتهاد السياسي أكثر من القانوني، ويضعف قدرة المجتمع الدولي على ضمان المساءلة والردع الفعال.

الفرع الأول: الإطار القانوني للعدوان التكنولوجي

تعتبر المادة 8 مكرّر[1] (2)(4) من نظام روما الأساسي واحدة من الأسس الحديثة التي تحدد الأعمال التي يمكن أن تُصنف كجرائم عدوان، خاصة عندما تُنفذ بطريقة تلحق أضرارًا جسيمة وطويلة الأمد بالبيئة الطبيعية، مما يتعارض مع أحكام القانون الدولي الإنساني. وتحدد هذه المادة معيارين رئيسيين لقيام الجريمة: الأول هو الطابع المتعمد للفعل وارتباطه باستخدام القوة المسلحة، والثاني هو النتيجة الضارة التي تتمثل في الأضرار الواسعة النطاق والطويلة الأمد التي تلحق بالبيئة الطبيعية. ورغم أن النص يشير بوضوح إلى "البيئة الطبيعية" على اليابسة، إلا أن الفقه المعاصر في القانون الدولي البيئي يرى أن مفهوم البيئة يمتد ليشمل كل نظام طبيعي يتأثر بالنشاطات البشرية، سواء على اليابسة أو في أعالي البحار أو حتى في الفضاء الخارجي.[2]

يمكن اعتبار الفضاء الخارجي بيئة طبيعية بالمعنى الواسع للمادة 8 مكرّر، نظرًا لحساسية توازناته المدارية واعتماده على استقرار الأقمار الصناعية لأداء وظائف حيوية. فالأضرار الناتجة عن الأنشطة العدائية في الفضاء، مثل الهجمات السيبرانية على الأقمار الصناعية أو اختراق أنظمة الذكاء الاصطناعي التي تدير المدارات، يمكن أن تؤدي إلى تعطيل واسع النطاق للبنية المدارية، وزيادة الحطام الفضائي، وتدمير طويل الأمد للمدارات القابلة للاستخدام المستدام (Long Term Sustainability – LTS).

---

[1] نصت المادة 8 مكرر من نظام روما: لغايات هذا النظام الأساسي، يُقصد بـ "جريمة العدوان": تخطيط أو إعداد أو الشروع أو تنفيذ شخص، يتمتع بسلطة تمكّنه فعليًا من ممارسة السيطرة على العمل السياسي أو العسكري للدولة أو توجيهه، لعمل عدواني يشكّل، بحكم طبيعته وخطورته ومداه، انتهاكًا صارخًا لميثاق الأمم المتحدة.

2– لغايات الفقرة (1)، يقصد بـ "العمل العدواني":

استخدام دولة للقوة المسلحة ضد سيادة دولة أخرى أو سلامتها الإقليمية أو استقلالها السياسي، أو بأي طريقة أخرى تتعارض مع ميثاق الأمم المتحدة.

ويُعدّ أيٌّ من الأفعال التالية، عملاً عدوانيًا، وفقًا لقرار الجمعية العامة للأمم المتحدة رقم 3314 (الدورة 29) المؤرخ في 14 كانون الأول/ديسمبر 1974، سواء أُعلنت الحرب أم لم تُعلن: .... د: مهاجمة القوات البرية أو البحرية أو الجوية التابعة لدولة ما، أو الأساطيل البحرية أو الجوية العائدة لها.....

[2] BIRNIE, P., & BOYLE, A.,(2009), International Law and the Environment, Oxford University Pres, p.84.

إنّ هذه النتائج تتوافق مع معايير المادة 8 مكرّر الثلاثة، حيث تجمع بين الأثر الواسع، وطول الأمد، والجسامة في النتائج. مما يجعل العدوان التكنولوجي في الفضاء الخارجي جريمة محتملة وفق الإطار الدولي الحالي. وهذا يستدعي تطوير آليات قانونية لمحاسبة الدول أو الفاعلين غير الدوليين عن الأفعال العدائية الرقمية في الفضاء التي تهدد الأمن والسلم الدوليين.

يتبين من خلال الأبحاث القانونيّة الحديثة أنّ الحاجة لتوسيع نطاق الجرائم الدّولية لتشمل العدوان التكنولوجي في الفضاء باتت ضروريّة، ويتطلّب ذلك وضع تعريفات دقيقة للأفعال الضارّة غير الماديّة وتحديد المسؤوليّة الجنائيّة للأطراف التي ترتكبها، سواء كانت دولًا أو كيانات خاصّة. هذا سيساعد في ضمان عدم إفلات مرتكبي هذه الأفعال من العقاب، ممّا يحدّ من التّداعيات الخطيرة على الأمن الدولي. كما تُظهر الدّراسات القانونيّة أهميّة تطوير آليّات مراقبة دوليّة ورصد مستمرّ للهجمات السّيبرانية في الفضاء، وتطبيق العقوبات المناسبة، وكذلك يجب أن تُدرج هذه الآليّات ضمن الاتفاقيّات الدّولية الحاليّة أو من خلال إبرام اتفاقيّة دوليّة جديدة تركز على العدوان التكنولوجي.[1]

كما وتظهر الحاجة أيضًا لتعزيز التّعاون الدولي بين الدول لوضع معايير واضحة لقياس الضّرر غير المادي الناتج عن العدوان التكنولوجي، حيثُ ينبغي توفير إطار قانوني شامل يحمي البنى التحتيّة الرّقميّة والمعلومات الحيويّة، ويضمن الاستخدام السّلمي والمستدام للفضاء. كما يُعزّز ذلك الثّقة الدّوليّة في التّكنولوجيا الحديثة، ويحدّ من سباق التسلّح الرقمي في الفضاء، ويمنع أي استغلال غير مشروع للأقمار الصناعيّة والأنظمة الفضائيّة لأغراض هجوميّة، ممّا يعكس تطوّر القانون الدولي لمواكبة التحديّات المعاصرة.

نصّت المادة 8 مكرر من نظام روما الأساسي على إمكانيّة إدراج أيّة جريمة كبرى إذا توفّرت شروط النّظام الأساسي، بما في ذلك العدوان التّكنولوجي الفضائي في حال أدّى إلى خطر جسيم على السّلم والأمن الدوليين. وتعكس المادّة المذكورة أعلاه المرونة القانونيّة التي تُتيح للمحكمة الجنائيّة الدوليّة مواجهة الجرائم الحديثة والمعقّدة التي لم تكن متوقّعة عند صياغة

[1] محمد عبد الرحمن، القانون الدولي الإنساني في مواجهة التهديدات الرقمية والفضائية الحديثة. المجلة العربية للقانون الدولي، العدد (5)، 2020، ص. 128

النّظام الأساسي، بما في ذلك الأفعال التي تستغلّ التكنولوجيا المتقدّمة والأقمار الصناعيّة والأنظمة الذكيّة.[1]

كما ويُتيح نصّ المادّة المذكورة أعلاه التعامل مع آثار العدوان التّكنولوجي الفضائي، الذي قد لا يتسبّب في أضرار ماديّة مباشرة، لكنّه يمكن أن يؤدّي إلى تعطيل البنى التّحتيّة الحيويّة، أو التّأثير على الأنظمة الماليّة والتّجاريّة للدول، أو حتّى التّأثير على الأمن السيّبراني العالمي، ممّا يعكس اهتمام المشرّع الدّولي بمواكبة التطوّرات التقنيّة الحديثة وضمان قدرة القانون الدولي على ردع أي تهديدات تمسّ السّلم والأمن الدوليين، حتّى وإن كانت الأساليب المستخدمة غير تقليديّة أو تعتمد على تقنيّات مستقبليّة[2].

إنّ النّص المذكور أعلاه يقدّم إطارًا قانونيًا واضحًا لتقييم مسؤوليّة الأفراد والدول في حالات العدوان التكنولوجي، ممّا يضمن مساءلة ومحاسبة الفاعلين وحماية الحقوق الدوليّة، كما يُظهر أهميّة الرّبط بين المعايير التقليديّة للجرائم الكبرى والآليات الحديثة لمواجهة المخاطر الفضائيّة والرقميّة.

كما ويوجب القانون توافر مجموعة من الشّروط الأساسيّة لتأصيل الأفعال التكنولوجيّة ضمن نطاق الجرائم الكبرى، حيثُ يفترض وجود نيّة عدائيّة واضحة من الجهة الفاعلة تستهدف دولة أو مجموعة من الدول، وفي هذه الحالة يُعتبر الفعل تهديدًا للسّلم والأمن الدّوليين.[3] كما ويوجب استخدام وسائل تكنولوجيّة متقدّمة، مثل الأقمار الصّناعيّة أو الأنظمة الذكيّة المعتمدة على الذّكاء الاصطناعي، ممّا يمنح الفاعل القدرة على إحداث تأثير واسع دون الحاجة إلى وسائل تقليديّة للعدوان. وكذلك يشترط القانون أن يكون للأفعال تأثير ملموس أو محتمل على الأمن الدولي، حتّى في ظلّ غياب الأثر المادي المباشر، إذ يكفي أن تُشكّل تهديدًا للبنية التحتيّة الحيويّة أو للأنظمة الاقتصاديّة أو للاتّصالات الدوليّة.

---

(1) NATARAJAN, R., (2019), The militarization of space: History and implications, Routledge, p.136.

(2) يوسف خالد، الذكاء الاصطناعي والقانون الدولي الإنساني: مقاربة تحليلية. مجلة دراسات قانونية، العدد 12، 2022، ص. 72–74.

(3) BRYSON, J. (2020). Artificial Intelligence and Space Security: Legal Challenges in the Age of Digital Warfare. Journal of International Law and Technology, 15(2), p.115–140.

يُظهر هذا التوسّع في نطاق الجرائم الكبرى إدراك المجتمع الدولي للطّبيعة المعقّدة للتّهديدات الحديثة، إذ لم تعد الجرائم تقتصر على الأفعال الماديّة المباشرة، بل أصبحت تشمل المخاطر الرّقميّة والتكنولوجيّة التي يمكن أن تزعزع الاستقرار الدولي وتُسبب أضرارًا جسيمة للحقوق العامّة والأنظمة القانونيّة للدّول. كما يسلّط القانون الضّوء على العلاقة بين النيّة العدائيّة والوسائل التكنولوجيّة والنتائج المحتملة، ممّا يضمن محاسبة الفاعلين ومواجهة الابتكارات التقنيّة التي قد تُستخدم لأغراض عدوانيّة على المستوى الدولي.[1] كما وتوفّر المادة 8 مكرر من نظام روما الأساسي المرونة اللاّزمة لتحديد الجرائم الكبرى في سياق التّهديدات الحديثة، ممّا يُعزّز قدرة المجتمع الدولي على التصدّي للمخاطر النّاشئة عن الاستخدام العدواني للتّكنولوجيا الفضائيّة والرقميّة، ويضمن حماية السّلم والأمن الدّوليين من المخاطر المتجدّدة والمتطورة.

الفرع الثاني: تحدّيات إرساء المسؤوليّة الدوليّة تجاه العدوان التكنولوجي الفضائي

تواجه عمليّة إدراج العدوان التّكنولوجي الفضائي ضمن نطاق الجرائم الكبرى مجموعة من التحدّيات القانونيّة والفنيّة المعقّدة التي تتطلّب تكييف النّظام الدولي مع التطوّرات التكنولوجيّة الحديثة[2]. وتظهر هذه التحديّات من خلال صعوبة إثبات الأضرار غير الماديّة أمام المحاكم، حيثُ قد تقتصر هذه الأضرار على تعطيل الأنظمة الرقميّة الحيويّة أو التّأثير على البنى التحتيّة التكنولوجيّة للدّولة المستهدفة، دون وجود آثار ماديّة ملموسة يمكن قياسها بسهولة، ممّا يتطلّب ابتكار معايير جديدة لتقييم المخاطر الرّقميّة على الأمن الدولي[3].

كذلك، فإنّ النّقص في النّصوص القانونيّة المحدّدة التي تعالج التّجريم في إطار اتّفاقيات الفضاء التّقليديّة، والتي لم تُصمّم لمواجهة التّهديدات التّكنولوجيّة المتقدّمة، بما في ذلك استخدام

---

[1] Ibid

[2] محمد أحمد الربيع، العدوان في القانون الدولي الإنساني: دراسة تحليلية في ضوء نظام روما الأساسي، دار الجامعة الجديدة، 2020، ص. 182.

[3] يوسف خالد، الذكاء الاصطناعي والقانون الدولي الإنساني: مقاربة تحليلية، مرجع سابق، 2022، ص. 75.

الأقمار الصّناعية والذّكاء الاصطناعي في أنشطة عدائيّة، ممّا يترك فجوة تشريعيّة تهدّد فعاليّة النّظام القانوني الدولي في الرّدع.

علاوةً على ذلك، ينبغي توسيع نطاق نظام روما الأساسي لضمان شمول العدوان التكنولوجي الفضائي ضمن اختصاص المحكمة الجنائيّة الدوليّة، ممّا يُتيح مساءلة جميع الجهات الفاعلة، سواء كانت دولًا أو كيانات خاصّة، عن الأفعال التي تُهدّد السلم والأمن الدّوليين.

إنّ تعقيدات هذه الجريمة تنبع أيضًا من الخصائص الفريدة للأفعال التّكنولوجية الحديثة، التي تتميّز بالسّرعة والدقّة والقدرة على الإخفاء، ممّا يعيق التحقّق من النّوايا العدائيّة واستهداف دولة أو مجموعة دول.[1] لذا، نحتاج إلى أدوات وتقنيّات قانونيّة وتقنيّة متطوّرة لضمان دقّة الإثبات وتحقيق العدالة، ومن هنا تظهر الحاجة الملحّة لتعزيز الإطار القانوني الدّولي وتطوير قواعد واضحة تتماشى مع تطوّر العدوان الرّقمي والفضائي، ممّا يضمن حماية الأمن الدولي وفعاليّة آليّات المساءلة الجنائيّة أمام المحكمة الجنائيّة الدوليّة، ويعكس قدرة القانون الدولي على التكيّف مع المخاطر الحديثة والمتغيّرة باستمرار.

علاوةً على ذلك، يوجد تحدٍّ آخر يتمثّل في غياب آليّات مؤسّساتيّة دوليّة متخصّصة لمراقبة الأنشطة الرقميّة والفضائيّة العدائيّة، ممّا يجعل التّنسيق بين الدول والهيئات الدّوليّة أمرًا في غاية الصّعوبة. ففي ظلّ غياب جهة مختصّة تجمع البيانات، وتحلّل التّهديدات، وتنسّق الرّدود القانونيّة والفنيّة، يؤدّي إلى بطء الاستجابة وتأخّر فرض العقوبات، ممّا يترك مجالًا كبيرًا لإفلات الجهات الفاعلة من المسؤوليّة. كما أنّ الطّبيعة العابرة للحدود لهذه الأفعال تفرض ضرورة إيجاد أطر تعاون دولي متكاملة تشمل تبادل المعلومات، وإجراءات تحقيق مشتركة، وآليّات تحكيم فعّالة، حتّى تتمكّن المحاكم من التّعامل مع هذه التّحديات بشكلٍ فعّال[2].

ولكن لا بدّ من الإشارة إلى أنّه تعتبر الهجمات السيبرانية التي تستهدف الأقمار الصناعية بهدف إلحاق الضرر بالمدارات أو تعطيل الخدمات العالمية الأساسية مثل الاتصالات،

---

[1] محمد عبد الرحمن، القانون الدولي الإنساني في مواجهة التهديدات الرقمية والفضائية الحديثة، مرجع سابق،2020، ص. 132.

[2] سامي محمد القاضي، الجريمة الدولية في الفقه والقضاء: تحليل لنظام روما الأساسي، دار الكتاب الحديث، 2018، ص. 160–165.

الملاحة، الإنقاذ، وأنظمة الإنذار المبكر، أعمالًا عدوانية ذات طابع تكنولوجي. ومن منظور فقهي وقانوني، يمكن تصنيفها ضمن "جرائم العدوان التكنولوجي" إذا توافرت الأركان التالية: القصد الجنائي، أي توجيه الهجوم السيبراني أو عبر الذكاء الاصطناعي بهدف الإضرار بالقمر الصناعي أو زعزعة الأمن الدولي؛ العمل العدواني، من خلال استخدام وسائل تقنية (Cyber/AI) لها تأثير فعلي يعادل استخدام القوة المسلحة؛ النتيجة البيئية الفضائية، حيث يتسبب الهجوم في خلل واسع في البيئة المدارية ويؤدي إلى آثار طويلة الأمد على الاستدامة الفضائية؛ صلة الهجوم بالنزاع أو العدوان، بحيث يُنفذ العمل ضمن سياق نزاعي أو بنية عدوانية واضحة.

لذلك، يبدو من المنطقي علميًا وقانونيًا القول بأن إساءة استخدام الأمن السيبراني والذكاء الاصطناعي في الفضاء قد ترتقي إلى جريمة حرب بيئية أو جريمة عدوان تكنولوجي خارجي وفق المادة 8 مكرّر من نظام روما الأساسي، خاصة في ظل توسع التفسير الفقهي لمفهوم البيئة الطبيعية ليشمل الفضاء الخارجي والأنظمة المدارية الحيوية، مما يعكس الحاجة الملحّة لتطوير آليات قانونية لمساءلة.

الخاتمة

يظهر من خلال هذا البحث أن عسكرة الفضاء الخارجي وزيادة الاعتماد على الأقمار الصناعية في المجالات العسكرية والأمنية والاقتصادية قد أدت إلى ظهور نوع جديد من المخاطر، تتمثل في الأضرار غير المادية الناتجة عن الهجمات السيبرانية والذكاء الاصطناعي. وقد أوضح المبحث الأول أن الأمن السيبراني الفضائي لم يعد مجرد مسألة تقنية، بل أصبح جزءًا أساسيًا من مكونات الأمن الدولي. بينما أظهر المبحث الثاني أن هذه الأضرار، رغم خطورتها، لا تزال تقع في منطقة قانونية رمادية بسبب عدم تحديث الإطار القانوني الدولي.

من الواضح أن الاتفاقيات الدولية التي تنظم الفضاء الخارجي، بما في ذلك اتفاقية الفضاء الخارجي لعام 1967 واتفاقية المسؤولية لعام 1972، لم تتناول بشكل صريح الأضرار غير المادية أو الهجمات الرقمية على الأقمار الصناعية، مما جعلها غير قادرة على مواكبة

التهديدات التكنولوجية الحديثة. كما أن اتفاقيات جنيف الأربعة لعام 1949 والبروتوكولات الإضافية، رغم اتساع نطاقها في حماية المدنيين والبنى التحتية الحيوية، لم تتطرق إلى الفضاء الخارجي أو إلى الطبيعة الرقمية للهجمات السيبرانية، مما خلق فجوة كبيرة بين قواعد النزاعات المسلحة التقليدية وطبيعة العمليات الفضائية الحديثة.

تظهر هذه الفجوة بشكل واضح عندما نحاول إدراج الهجمات السيبرانية على الأقمار الصناعية ضمن نظام روما الأساسي. فالمادة 8 من هذا النظام تركز على الجرائم التقليدية التي تؤثر على "البيئة الطبيعية" أو تمثل "عدوانًا مسلحًا"، لكنها لا تقدم تعريفًا واضحًا للأضرار غير المادية أو التأثيرات الرقمية التي قد تكون لها آثار تعادل أو تفوق تلك الناتجة عن الهجوم العسكري التقليدي. ومع ذلك، فإن التفسير الواسع للمادة 8، خصوصًا فيما يتعلق بالهجمات التي تسبب أضرارًا واسعة وطويلة الأمد وخطيرة للبيئة الطبيعية، يفتح المجال لإمكانية اعتبار الإضرار بالبيئة المدارية ضمن جرائم الحرب البيئية أو العدوان التكنولوجي، إذا تم تطوير المعايير التطبيقية وتكييف المفاهيم لتناسب خصوصية الفضاء الخارجي.

وعليه، يبرز بوضوح الحاجة إلى إعادة النظر في الإطار القانوني الدولي وتطويره ليتماشى مع واقع عسكرة الفضاء وظهور الأسلحة الرقمية، بالإضافة إلى وضع قواعد أكثر فعالية لتنظيم السلوك الدولي وحماية الأصول الفضائية ذات الطابع المدني والحيوي.

علاوةً على ذلك، تظهر الحاجة ملحة لتعزيز التّعاون الدولي لوضع معايير وقواعد ملزمة تضمن خدمة تكنولوجيا الفضاء للبشريّة، وتحقّق الاستخدام السلمي والمستدام للفضاء، مع حماية الأمن والاستقرار الدوليين من التهديدات الرقميّة والتّكنولوجيّة الحديثة.

التوصيات والمقترحات:

- تحديث اتفاقية الفضاء الخارجي لعام 1967 من خلال بروتوكول إضافي يحدد الأضرار غير المادية ويشمل الهجمات السيبرانية كأعمال محظورة في الفضاء الخارجي.
- إدراج الفضاء الخارجي ضمن نطاق تطبيق اتفاقيات جنيف والبروتوكولات اللاحقة، أو اعتماد بروتوكول جديد يتناول النزاعات الفضائية والهجمات الرقمية.
- تعديل المادة 8 من نظام روما الأساسي لتشمل بشكل واضح الأضرار السيبرانية التي تلحق بالأقمار الصناعية والبيئة المدارية، وتصنيفها كجرائم حرب أو عدوان تكنولوجي.

- إنشاء آلية دولية مشتركة لمراقبة الهجمات السيبرانية على الأقمار الصناعية وتوثيق آثارها القانونية، مما يمكّن المحاكم الدولية من تقييم مسؤولية الدول أو الفاعلين غير الدوليين.
- إقرار مدوّنة دولية لسلوك الفضاء السيبراني (Space Cyber Code of Conduct) تعتمدها الأمم المتحدة لتنظيم استخدام الذكاء الاصطناعي والعمليات الرقمية في المدار وتعزيز الشفافية والثقة بين الدول.
- وضع معايير واضحة لتحديد المسؤوليّة، وآليّات للرّصد والتّتبع، وإجراءات قانونية متناسبة، مع الأخذ في الاعتبار طبيعة التقنيات الحديثة، بما في ذلك الذكاء الاصطناعي، والتلقائية، والقدرة على التعلم الذاتي للخوارزميات الفضائية، لضمان الاستخدام السلمي للمجال الفضائي، وحماية الأمن القومي والدولي، واستدامة الفضاء كمورد مشترك للبشرية جمعاء.

قائمة المراجع:

أولاً: المراجع العربية

1- المؤلفات

- كريم العوضي. (2019). القانون الدولي للفضاء الخارجي وتحديات التكنولوجيا الحديثة. بيروت: دار النهضة العربية.
- سامر محمد فاخوري. (2023). القانون الدولي للفضاء الخارجي بين الأمن السيبراني والتطبيقات العسكرية. عمّان: دار الحامد.
- سامي محمد القاضي. (2018). الجريمة الدولية في الفقه والقضاء: تحليل لنظام روما الأساسي. بيروت: دار الكتاب الحديث.
- محمد أحمد الربيع. (2020). العدوان في القانون الدولي الإنساني: دراسة تحليلية في ضوء نظام روما الأساسي. الإسكندرية: دار الجامعة الجديدة.
- فهد بن عبد الله الشمري. (2021). الأمن السيبراني في ضوء القانون الدولي العام. الإسكندرية: دار الجامعة الجديدة.

2- الدوريات والمقالات

- خالد إبراهيم منصور. (2021). تحديات التجسس الفضائي في ظل الثورة الرقمية: قراءة قانونية. مجلة البحوث القانونية والسياسية 85–76 ,18.
- محمد عبد الرحمن. (2020). القانون الدولي الإنساني في مواجهة التهديدات الرقمية والفضائية الحديثة. المجلة العربية للقانون الدولي 5.

- يوسف خالد. (2022). الذكاء الاصطناعي والقانون الدولي الإنساني: مقاربة تحليلية. مجلة دراسات قانونية 12.

ثانياً: في اللغة الأجنبية

1- Ouvrages
- Birnie, P., & Boyle, A. (2009). International Law and the Environment. Oxford University Press.
- Bryson, J. (2020). Artificial Intelligence and Ethical Space Governance. Oxford University Press.
- Lewis, J. A. (2021). Cybersecurity and Space Operations: Threats and Solutions. Center for Strategic & International Studies.
- Natarajan, R. (2019). The Militarization of Space: History and Implications. Routledge.
- Tronchetti, F. (2020). International Responsibility for Space Activities. Brill.
- Zhang, L. (2023). AI and Cybersecurity in Outer Space: Emerging Threats. Springer.

2- Articles et chroniques
- Al Tamimi, H. (2021). Cyber threats and satellite security. International Journal of Cyber Studies, 14(2), 45–63.
- Borelli, S. (2017). Cyber Operations and the Notion of 'Attack' in International Humanitarian Law. Yearbook of International Humanitarian Law, 127.
- Dorado, J. (2022). Artificial Intelligence and Autonomous Systems in Space Security. Space Policy, 75–78.
- Estefan, N. (2021). Non-Kinetic Warfare and International Law: The Challenge of Non-Material Harm. Journal of Conflict & Security Law, 59.
- Schmitt, N. (2020). International Law and Military Operations in Space. Harvard National Security Journal, 76–83.

3- Rapports internationaux
- United Nations. (2022). Report on Cybersecurity in Outer Space. UN Office for Outer Space Affairs.