دار نشر جامعة لوسيل
Lusail University Press

RESEARCH ARTICLE

الدور السيبراني لإيران في النزاعات الإقليمية: تحليل استراتيجيات إيران في الفضاء السيبراني وتأثيرها على الديناميكيات الإقليمية

خليفة أحمد خليفة آل دلهم الكواري
مخلد إرخيص سالم الطراونة

الملخص

تتناول الدراسة الدور السيبراني لإيران في النزاعات الإقليمية من منظور القانون الدولي، فتسعى لتحليل الاستراتيجية السيبرانية الإيرانية، وتقييم مدى توافق ممارساتها مع قواعد القانون الدولي العام، لا سيما في ظل غياب عتبة كمية ونوعية متفق عليها لتصنيف الهجمة السيبرانية، ضمن مفهوم استخدام القوة بمدلول المادة (4/2) من ميثاق الأمم المتحدة. وتستند الدراسة إلى الوثيقة الرسمية الإيرانية الصادرة عام 2020 بشأن تطبيق القانون الدولي في الفضاء السيبراني، وتتّبع منهجاً وصفياً تحليلياً نقدياً يقوم على مراجعة المصادر الأولية والثانوية، وتطبيقها على نماذج من العمليات السيبرانية المنسوبة لإيران، من بينها الهجوم على ألبانيا، واستهداف البنى التحتية في دول الخليج العربي، وتبادل الهجمات السيبرانية بينها وبين إسرائيل. وتخلص الدراسة إلى أنّ إيران توظّف الفضاء السيبراني سلاحاً للردع غير المتكافئ، مستثمرةً قصور قواعد الإسناد التقني، وارتفاع عتبة الإثبات أمام آليات المساءلة الدولية، بما يُرتّب انتهاكات صريحة لمبدأي السيادة وعدم التدخل، وقد يرقى في بعض الحالات إلى استخدام غير مشروع للقوة، فيما تواجه دول الخليج تحدّيات حقيقية في الإسناد والمساءلة. كما تكشف الدراسة عن إسهام النشاط السيبراني الإيراني في تسريع تبلور أعراف دولية مضادة، وتطوير آليات المساءلة. وتوصي الدراسة بتعزيز الأطر القانونية والدفاعية على الصعيدين الإقليمي والدولي، وتطوير قدرات الإسناد التقني، وبلورة استراتيجيات للردع السيبراني تنسجم مع قواعد القانون الدولي، بما يُسهم في صون الأمن والاستقرار الإقليميين والدوليين.

الكلمات المفتاحية: الفضاء السيبراني، إيران، القانون الدولي، النزاعات الإقليمية، الأمن الإقليمي، الهجمات السيبرانية، الردع السيبراني

Iran's Cyber Role in Regional Conflicts: Analyzing Iran's Cyber Strategies and Their Impact on Regional Dynamics

ABSTRACT

This study examines Iran's cyber role in regional conflicts from the perspective of public international law. It analyzes Iran's cyber strategy and assesses the compliance of its practices with rules of international law, particularly in light of the absence of an agreed quantitative and qualitative threshold for classifying a cyber operation as a 'use of force' within the meaning of Article 2(4) of the United Nations Charter. Drawing on Iran's 2020 official document on the application of international law in cyberspace, the study adopts a descriptive, analytical, and critical methodology based on primary and secondary sources, applied to selected cyber operations attributed to Iran, including the attack on Albania, the targeting of critical infrastructure in the Gulf states, and the cyber exchanges with Israel. The study finds that Iran employs cyberspace as a tool of asymmetric deterrence, exploiting the inadequacy of technical attribution rules and the high evidentiary threshold before international accountability mechanisms, in a manner that entails clear breaches of the principles of sovereignty and non-intervention and may, in certain instances, amount to an unlawful use of force, while Gulf states face genuine challenges in attribution and accountability. The study further demonstrates that Iranian cyber activity has accelerated the crystallization of counter-norms and the development of accountability mechanisms in international law. It recommends strengthening regional and international legal and defensive frameworks, enhancing technical attribution capabilities, and developing cyber deterrence strategies consistent with international law, so as to promote regional and international peace and security.

Keywords: Cyberspace; Iran; international law; regional conflict; regional security; cyberattacks; cyber deterrence

خليفة أحمد خليفة آل دلهم الكواري
أكاديمية الشرطة، كلية الشرطة، دولة قطر
Khalifa Ahmed Khalifa Al-Dilham Al-Kuwari
Police Academy, Police College, State of Qatar
ka4090@pa.edu.qa
ORCID ID: https://orcid.org/0009-0008-9762-3605

مخلد إرخيص سالم الطراونة
أكاديمية الشرطة، كلية الشرطة، دولة قطر
Mekhled Erkhyees Salem Al-tarawneh
Police Academy, Police College, State of Qatar
ma17126@pa.edu.qa
ORCID ID: https://orcid.org/0000-0002-4804-9749

Submitted: 09 April 2026
Accepted: 06 June 2026

https://doi.org/10.70139/rolacc.2026.1.5

للاقتباس: خليفة أحمد خليفة آل دلهم الكواري ومخلد إرخيص سالم الطراونة. الدور السيبراني لإيران في النزاعات الإقليمية: تحليل استراتيجيات إيران في الفضاء السيبراني وتأثيرها على الديناميكيات الإقليمية. مجلة مركز حكم القانون ومكافحة الفساد، 1:2026.
https://doi.org/10.70139/rolacc.2025.1.5

1. مقدمة

أصبح الفضاء السيبراني ساحة مواجهة رئيسية في الشرق الأوسط، وبرزت إيران كفاعل نشط يوظّف الهجمات السيبرانية لتعزيز نفوذه الإقليمي، من خلال اعتماد استراتيجية إقليمية تركز بشكل متزايد على هذه الهجمات، لتعويض نقاط الضعف في القدرات العسكرية والضغوط الاقتصادية.[1] فمن خلال الاستناد لآليات غير متماثلة تستخدم التكنولوجيا المتقدمة كالذكاء الاصطناعي والقدرات السيبرانية المتطورة، استطاعت إيران تحدي تفوّق خصومها التقني مثل إسرائيل وأمريكا، والتأثير فيهم عبر استهداف مواطن الضعف في الفضاء الرقمي.[2]

وقد برزت خلال حرب الاثني عشر يوماً أبعاداً أكثر تنظيماً، وتداخلت مستويات الفاعلين الإيرانيين بين الفاعل الحكومي الرسمي، والوكلاء السيبرانيين، ومجموعات متطوعة ذات طابع أيديولوجي متشعب، وأظهرت تقريراً معنوناً بـ"من أعماق الظلال: الحرس الثوري الإيراني ومجموعات القرصنة في حرب الاثني عشر يوماً" التحولات في أنماط الهجوم الإيراني، والتي شملت التكامل بين الجهد الدعائي والهجمات التخريبية مباشرة عقب التصعيد العسكري مع إسرائيل.[3] وتجدر الإشارة إلى أنّ قوة إيران السيبرانية ترتبط ارتباطاً وثيقاً بهدفها الأوسع، والمتمثل في دعم ما يُعرف بمحور المقاومة، والذي يضمّ دولاً وجماعات غير حكومية تعارض النفوذين الغربي والإسرائيلي في المنطقة، فمن خلال العمليات السيبرانية، تستطيع إيران إلحاق اضطراب بالبنية التحتية الحرجة، وشنّ عمليات مُنُسَّقَة دعماً لحلفائها الإقليميين.[4]

ولم يكن هذا التصاعد في النشاط السيبراني بمعزل عن الاعتبارات القانونية الدولية، إذ تستغلّ إيران الثغرات والغموض القانوني في قواعد القانون الدولي لتنفيذ عمليات خفية تُربك الخصوم، وتقوّض إمكانية إسناد الهجمات إليها ومساءلتها.[5] وبعبارة أخرى فتعمل إيران في "المناطق الرمادية" قانونياً، حيث لا تزال المفاهيم الدولية حول استخدام القوة في الفضاء السيبراني قيد التشكل. وقد أتاح هذا الغموض لإيران مساحة للمناورة، دون تحمّل تبعات قانونية واضحة. ويتزامن ذلك مع سياق جيواستراتيجي أوسع يتسم بمنافسات إقليمية محتدمة، وتطور تقني، وتحالفات متغيرة، مما أفرز معضلات أمنية ديناميكية، وتصعيداً تدريجياً في بيئة الصراع السيبراني.[6]

1.1. فكرة الدراسة

ترتكز الدراسة على تحليل طبيعة الاستراتيجية السيبرانية التي تعتمدها إيران في النزاعات الإقليمية، وتحري مدى اتساقها مع قواعد القانون الدولي العام، أو استنادها لمبادئ قانونية دولية رئيسية، وعلى رأسها مبدأ السيادة، ومبدأ عدم التدخل، وحظر استخدام القوة، وحق الدفاع عن النفس، وذلك من أجل تقييم السلوك السيبراني الإيراني ضمن إطار قانوني موضوعي.

1.2. أهمية الدراسة

تبرز أهمية الدراسة في تناولها أحد أهم التحولات الاستراتيجية في أمن الشرق الأوسط، والمتمثل في توظيف إيران للفضاء السيبراني كأداة نفوذ إقليمي، خصوصاً بعد إصدار "إعلان القانون الدولي السيبراني" لعام 2020،[7] من قِبل هيئة الأركان العامة الإيرانية. كما تكمن أهميتها في تحليل الكيفية التي تعيد بها إيران تفسير مبادئ القانون الدولي، وتطويعها لخدمة أهدافها، من خلال توسيع مفهوم السيادة الرقمية على نحو يمنحها مبرراً لاعتبار أي اختراق أجنبي انتهاكاً لسيادتها، مقابل تجنّب توصيف عملياتها الهجومية باعتبارها استخداماً للقوة، تفادياً لمنح خصومها حق الرد القانوني.

كما تتجلى أهمية الدراسة في سعيها للإجابة عن سؤال محوري يتعلق بطبيعة الاستراتيجيات السيبرانية الإيرانية في النزاعات الإقليمية، وكيفية تشكيلها للمشهد الجيوسياسي والأمني، ومدى توافقها أو تعارضها مع مبادئ القانون الدولي السيبراني. وتزداد أهمية هذا التحليل في ظل التصعيد السيبراني بين إيران وإسرائيل، والذي بلغ ذروته في حرب الاثني عشر يوماً في يونيو 2025، حيث أظهرت المواجهة حدود أو فعالية القدرات الإيرانية مقارنةً بتفوّق خصومها التقني. ومن ثم فتمثل هذه الدراسة إطاراً حيوياً لفهم انعكاسات النشاط السيبراني الإيراني على الاستقرار الإقليمي، وعلى تطور النظامين القانوني والمعياري الحاكمين للفضاء السيبراني.

1.3. منهجية الدراسة

تعتمد هذه الدراسة على منهج تحليلي وصفي ذي طابع قانوني، يهدف إلى تفسير السلوك السيبراني الإيراني في ضوء قواعد القانون الدولي العام، ولتحقيق ذلك فستقوم الدراسة بتحليل المبادئ القانونية الدولية ذات الصلة، مثل مبدأ السيادة، وعدم التدخل، وحظر استخدام القوة، وحق الدفاع الشرعي، مع بيان موقف إيران الرسمي كما ورد في "إعلان القانون الدولي السيبراني" الصادر عام 2020، وذلك لفهم الأسس القانونية التي تستند إليها في تبرير عملياتها السيبرانية.

كما تعتمد الدراسة منهج دراسة الحالة عبر تحليل عدد من الحوادث السيبرانية البارزة المنسوبة لإيران، بهدف الكشف عن أنماط السلوك والغايات الاستراتيجية الكامنة خلفها. مع مقارنة هذه الممارسات بالإطار القانوني الدولي، لتقييم مدى توافقها مع القواعد والأعراف الدولية المنظمة للفضاء السيبراني.

1.4. خطة البحث

تنقسم الدراسة إلى ثلاثة مباحث رئيسية، يتناول المبحث الأول استعراض الإطار القانوني للصراع السيبراني، وتحليل موقف إيران تجاه المبادئ الأساسية للقانون الدولي المتعلقة بالفضاء السيبراني. بينما يتناول المبحث الثاني استعراض دراسات حالة تطبيقية لمجموعة من الهجمات السيبرانية البارزة المنسوبة لإيران، مع تقييم قانوني شامل لكل حادثة وفق المعايير الدولية السارية، مع التركيز على الاستراتيجيات والأهداف الإيرانية خلف هذه العمليات. بينما يتناول المبحث الثالث تحليل التداعيات الإقليمية والدولية لهذه الأنشطة، مبيّناً تأثيرها على تطور القانون السيبراني والأمنين الإقليمي والدولي، مع تقديم رؤى دقيقة حول الديناميات الجديدة، وتوازنات القوى التي تشكلها هذه العمليات على المشهدين الجيوسياسي والأمني في المنطقة.

---

1 V Veronika Netolická & Miroslav Mareš, *Arms Race "in Cyberspace" – A Case Study of Iran and Israel*, 37 COMPAR. STRATEGY 414, 421 (2018).

2 Michael Mieses, Noelle Kerr & Nakissa Jahanbani, *Artificial Intelligence Is Accelerating Iranian Cyber Operations*, LAWFARE 1, 1 (2024).

3 Ryan Sherstobitoff & Gilad Friedenreich Maizles, *From the Depths of the Shadows: IRGC and Hacker Collectives of the 12–Day War* 17–18 (2025).

4 Renad Mansour, Hayder Al–Shakeri & Haid Haid, *The Shape–Shifting "Axis of Resistance": How Iran and Its Networks Adapt to External Pressures*, CHATHAM HOUSE 2, 2 (2025).

5 Gary Corn, *Punching on the Edges of the Grey Zone: Iranian Cyber Threats and State Cyber Responses*, JUST SECURITY 1, 1 (2020).
انظر أيضاً: محمد معن محسن، "مستقبل مكانة القوة السيبرانية في استراتيجيات القوى الإقليمية، إيران نموذجاً"، **مجلة قضايا سياسية**، العدد 81 (نيسان، أيار، حزيران)، 2025، ص 3.

6 *Middle East: A Cyber Arms Race*, CYFIRMA 7, 7, https://www.cyfirma.com/research/middle–east–a–cyber–arms–race/ (last visited 13 March 2026).
انظر أيضاً: بهاء عدنان يحيى وشهد حمزة مير علي، "تأثير التهديدات السيبرانية في الصراعات الإقليمية: نماذج مختارة"، **مجلة مركز دراسات الكوفة**، العدد 76، مارس 2025، ص 169.

7 *Declaration of the General Staff of the Armed Forces of the Islamic Republic of Iran Regarding International Law Applicable to Cyberspace* (2020), https://nournews.ir/En/News/53144/General–Staff–of–Iranian–Armed–Forces–Warns–of–Tough–Reaction–to–Any–Cyber–Threat [hereinafter Iran General Staff Declaration].

2. التأصيل النظري والقانوني للصراع السيبراني

يؤسس المبحث الأول أرضية نظرية لفهم سياق النزاعات السيبرانية، بالتركيز على المبادئ القانونية الدولية الأساسية المطبّقة على الفضاء السيبراني، فيستعرض كيفية انطباق مفاهيم السيادة، وعدم التدخّل، وحظر استخدام القوة، وحق الدفاع عن النفس على العمليات السيبرانية، إضافةً إلى تحدي الإسناد الذي يعقّد تحديد المسؤولية عن الهجمات السيبرانية، مما يوفّر معياراً لقياس مدى التزام أو انتهاك الدول ومنها إيران لتلك المبادئ، عند انخراطها في نزاعات سيبرانية.

2.1. مبدأ السيادة

يُعدّ مبدأ السيادة حجر الزاوية في القانون الدولي، وينصرف إلى حق كل دولة في ممارسة سلطتها المطلقة على إقليمها وشؤونها دون تدخل خارجي غير مشروع. ومع بروز الفضاء السيبراني فقد انقسمت الآراء الدولية حول تطبيق السيادة في هذا المجال، فبينما ذهبت بعض الدول مثل المملكة المتحدة إلى نفي وجود قواعد قانونية ملزمة بشأن السيادة في الفضاء السيبراني،[8] اعتمدت الغالبية العظمى من الدول نهجاً مختلفاً، حيث أقرّت بامتداد السيادة للمجال السيبراني، وأنّ أي انتهاك لشبكات دولة أخرى قد يرقى إلى خرق للسيادة إذا بلغ حداً معيناً.[9]

وقد تبنّت إيران هذا الرأي الأخير بصورة لا لبس فيها، حيث صرّحت هيئة الأركان العامة الإيرانية عام 2020 بأنّ السيادة في الفضاء السيبراني ليست قضية فوق القانون، مؤكدة خضوع الفضاء السيبراني للقواعد الدولية، شأنه في ذلك شأن البر والبحر والجو والفضاء الخارجي.[10] وهو موقف يثير تساؤلات نقدية مهمة، فبينما يرى مؤيدو هذا التوجه أنّه يحمي سيادة الدول الرقمية، ينتقد فقهاء قانونيون هذا التفسير الموسع باعتباره يقيّد الحريات الرقمية، ويبرر رقابة مفرطة. ويعكس هذا التناقض الانقسام الدولي الأوسع حول حوكمة الإنترنت بين معسكر "السيادة الرقمية" الذي يضم إيران والصين وروسيا، وبين معسكر "الإنترنت المفتوح" الذي تتزعّمه الولايات المتحدة وأوروبا.[11]

وتتبنّى إيران موقفاً فريداً ومتقدماً مقارنة بمعظم الدول فيما يتعلق بتفسير نطاق الحماية السيبرانية للسيادة الوطنية. ففي حين ترى العديد من الدول أنّ انتهاك السيادة السيبرانية يقع فقط عند تسبب العملية السيبرانية بأضرار مادية جسيمة، أو تعطيل ملموس للبنى التحتية، ترى إيران أنّ أي عملية سيبرانية لها تبعات مادية أو غير مادية تهدد أمنها القومي تُعدّ انتهاكاً لسيادتها، شاملة التهديدات السياسية والاقتصادية والاجتماعية والثقافية.[12] إذ جاء في الإعلان الإيراني بأنّ: "أي استعمال للفضاء السيبراني ينطوي على اختراق غير مشروع للبنى السيبرانية العامة أو الخاصة التابعة لدولة أخرى، يمكن أن يشكّل انتهاكاً لسيادة تلك الدولة".[13]

ومن تطبيقات إيران الموسّعة لمفهوم السيادة أيضاً ربطها بالسيادة الاقتصادية، إذ ختمت المادة الثانية من إعلانها بالنص على أنّ أي تدابير تقييدية أو تجميد للأصول بما في ذلك العقوبات الدولية، تعتبرها انتهاكاً لسيادة الدول.[14] وقد أثار هذا الطرح اعتراض الفقهاء الدوليين، فالعقوبات تفرض عادةً خارج إقليم الدولة المستهدفة، ولا تعوق مباشرةً قيامها بوظائفها الأساسية، وبالتالي تُصنَّف كأعمال مشروعة وليست خرقاً لقاعدة قانونية. ويُفسّر تبنّي إيران لهذا الموقف لكونها خاضعة لسنوات طوال لعقوبات متعددة الأطراف، ما يعني أنّها أرادت تأطير تلك العقوبات على أنّها اعتداء على مبدأ المساواة السيادية بين الدول. لكن إجماع المجتمع الدولي لا يوافق إيران في هذا التوسّع، ويظلّ اعتبار العقوبات السلمية انتهاكاً للسيادة رأياً شاذاً لا سند له في ممارسات الدول.[15]

ومن جهة أخرى فتعكس الرؤية الإيرانية لمبدأ السيادة سعياً لترسيخ السيادة الرقمية، أي حق كل دولة في السيطرة المطلقة على بيئتها الرقمية الداخلية. وفي هذا السياق تتلاقى إيران فكرياً مع الصين فيما يتعلق بحوكمة الإنترنت، فكلا الدولتين تدعو إلى نظام إنترنت مقسّم قومياً، تفرض فيه كل دولة سيطرة سيادية على معمارية الشبكات والمحتوى ضمن حدودها.[16]

غير أنّ هذا التوسّع المفاهيمي في السيادة الرقمية لا يستقيم مع البنية المعيارية للقانون الدولي العام، فالسيادة بوصفها قاعدةً عرفيةً تحمي الاختصاص الإقليمي والوظيفي للدولة، لا تنصرف إلى احتكار المعلومات، أو ضبط التدفقات المعرفية العابرة للحدود. ومن ثَمَّ تُحوِّل التماهي بين السيادة بمدلولها القانوني والسيطرةِ على المحتوى القاعدةَ، من ضمانةٍ لاستقلال الدولة إلى أداةٍ لتقييد الحقوق الرقمية المعترف بها في المادة (19) من العهد الدولي للحقوق المدنية والسياسية، والمادة (19) من الإعلان العالمي لحقوق الإنسان. وعلى هذا الأساس يبقى الموقف الإيراني موقفاً سياسيّاً في إطار قانوني، ما يعني ضعف حجته، ما لم تتبلور حوله ممارسةٌ دوليةٌ عامةٌ، وقناعةٌ قانونيةٌ.

2.2. مبدأ عدم التدخل

يقضي مبدأ عدم التدخل في القانون الدولي بألا تتدخل أي دولة في الشؤون الداخلية أو الخارجية للدول الأخرى بطريقة تمس سيادتها، باستخدام وسائل تنطوي على إكراه. وهذا المبدأ مستقر في الفقه والممارسة الدوليين، وقد تم تأكيده في قرارات الأمم المتحدة، والتقارير الأممية ذات الصلة بالفضاء السيبراني.[17] فلا خلاف على وجود القاعدة العرفية التي تحظر التدخل، وعنصري الانتهاك المتفق عليهما هما: القسر أو الإكراه الموجَّهان ضد مجال داخلي محمي للدولة، كالنظام السياسي أو الاقتصادي أو الاجتماعي. فقد شددت الوثيقة الإيرانية على هذا المعنى بنصها على: "مبدأ عدم التدخل، وبلا أدنى شك، مبدأ مستقل من مبادئ القانون الدولي العرفي."

8 Mark Visger, *The International Law Sovereignty Debate and Development of International Norms on Peacetime Cyber Operations*, LAWFARE (2022), https://www.lawfaremedia.org/article/international-law-sovereignty-debate-and-development-international-norms-peacetime-cyber-operations.

9 Harriet Moynihan, *The Application of International Law to Cyberspace: Sovereignty and Non-Intervention*, JUST SECURITY 11, 11 (2019), https://www.chathamhouse.org/2019/12/application-international-law-state-cyberattacks/2-application-sovereignty-cyberspace.

10 Michael N. Schmitt, *Noteworthy Releases of International Cyber Law Positions—Part II: Iran* 2, 2, https://lieber.westpoint.edu/nato-release-international-cyber-law-positions-part-i/ (last visited 12 January 2026).

11 *Id.* at 2–3.
انظر أيضاً: زكريا عبدالله عودوان، "الحرب السيبرانية والأداء الاستراتيجي الفعال: دراسة حالة في الهجمات السيبرانية بين إيران وإسرائيل"، **مجلة الدراسات الإقليمية**، العدد الثاني، 2023حزيران/يونيو، ص 8–10.

12 *Id.* at 3.

13 Iran General Staff Declaration, *supra* note 7.
انظر أيضاً: محمد ياسين سلمونة، **المسؤولية الدولية الناشئة عن الهجمات السيبرانية**، رسالة دكتوراة، جامعة العلوم الإسلامية العالمية، 2024، ص 83–91.

14 Iran General Staff Declaration, *supra* note 7.

15 Schmitt, Noteworthy Releases, *supra* note 10, at 14.

16 إبراهيم السيد رمضان، "مواجهة الهجمات السيبرانية في ضوء أحكام القانون الدولي"، **مجلة العلوم القانونية والاقتصادية**، المجلد 67، العدد الأول، يناير 2025، ص 1746.

17 Michael Schmitt, *The Sixth United Nations GGE and International Law in Cyberspace*, JUST SECURITY (2021), https://www.justsecurity.org/76864/the-sixth-united-nations-gge-and-international-law-in-cyberspace/.

كما أكّدت لزوم توافر العنصرين المذكورين، إذ نصّت على حظر: "جميع الأشكال الواضحة والدقيقة والأساليب المعقدة من الإكراه أو الإطاحة أو التعدّي، سيبرانياً كان أو غير سيبراني، للتدخل في النظام السياسي أو الاجتماعي أو الاقتصادي لدولة أخرى أو زعزعة الحكومات"، متفقة في ذلك مع التعريف الكلاسيكي للتدخل غير المشروع الوارد في قضية نيكاراغوا (1986).[18] والأمثلة النموذجية التي أوردها الإعلان الإيراني عن تغيير النظام بالقوة والتلاعب السيبراني بالانتخابات، تتفق عموماً مع ما يعتبره المجتمع الدولي والخبراء مثل فريق دليل تالين 0.2، انتهاكاً صارخاً لمبدأ عدم التدخل.[19] ويكشف التوسّع الإيراني في توصيف التدخل ليشمل أنماطاً واسعةً من النشاط المعلوماتي عن توظيفٍ معياريٍّ انتقائيٍّ، أكثر مما يعكس قراءةً قانونيةً محايدة، إذ يُضيّق هامش الفعل المشروع للخصوم، ويُوسّع في الوقت ذاته نطاق ما تَعدّه طهران مسّاً بسيادتها.

ومن التطبيقات العملية لمبدأ عدم التدخل سيبرانياً، ما أشار إليه الإعلان الإيراني بشأن عرقلة اتصالات دولة ما، أو تقييد قدرتها على نقل المعلومات وممارسة سيادتها. فإيران تعتبر أي إجراء يؤدي إلى منع دولة من استخدام وسائط الاتصال أو التحكم بمرافقها المعلوماتية، بما يعيقها عن أداء وظائفها السيادية، تدخلاً غير مشروع.[20] ويتفق هذا مع التفسير بأنّ حرمان أي دولة من وسائل جوهرية لممارسة صلاحياتها السيادية عن طريق هجوم سيبراني يُعدّ تدخلاً محظوراً. أما مجرد التدخل في الاتصالات الإلكترونية دون أن يرتقي لمستوى الإكراه في تسيير شؤونها الداخلية، فلا يعتبر تدخلاً بموجب القانون الدولي. ويُلاحظ أنّ إيران وإن تبنّت مبدأ عدم التدخل شكلياً، إلا أنّها توسّع في تفسير بعض جوانبه لتشمل نطاقاً أوسع من الأنشطة، كالحرب المعلوماتية السابقة للانتخابات، وهو ما يعكس هواجس طهران الأمنية حيال الحرب النفسية والإعلامية ضدها. ويبقى أنّه وفق القانون الدولي السائد يجب توافر عنصر الإكراه في الفعل السيبراني حتى يُصنّف كتدخل محظور.[21]

2.3. حظر استخدام القوة

يحظر مبدأ عدم استخدام القوة لجوء الدول إلى القوة المسلحة في علاقاتها الدولية، وفقاً لميثاق الأمم المتحدة في المادة 2(4) والقواعد العرفية ذات الصلة. ويُستثنى من ذلك حالتان: الأولى استخدام القوة المصرّح به من مجلس الأمن تحت الفصل السابع، والثانية ممارسة حق الدفاع الشرعي وفق المادة (51) من ميثاق الأمم المتحدة.[22] أما في السياق السيبراني فقد تَوافَق الرأي العام الدولي على أنّ الهجمات السيبرانية يمكن في بعض الظروف أن ترتقي إلى مستوى استخدام للقوة المحظور.[23] فوفقاً لتقرير خبراء الأمم المتحدة لعام 2015، فإنّ العمليات السيبرانية التي تسبب أضراراً أو خسائر مادية جسيمة تعادل تلك الناجمة عن وسائل تقليدية، قد تُعتبر استخداماً للقوة، ويستلزم ذلك تقييم حجم وتأثير الهجوم السيبراني، فهجمة إلكترونية تُعطّل شبكة الكهرباء في مدينة كبيرة متسببةً في أضرار وخسائر بشرية، قد تُعدّ استخداماً للقوة، أو حتى هجوماً مسلحاً بالمعنى المقصود في المادة (51) من ميثاق الأمم المتحدة.[24]

وفيما يخص الموقف الإيراني، فهو لافت بتقييده البارز لما يعتبره استخداماً للقوة سيبرانياً. فبحسب إعلان هيئة الأركان الإيرانية لا يُصنَّف الهجوم السيبراني كاستخدام محظور للقوة، إلا إذا أسفر عن أضرار مادية واسعة وخطيرة على الممتلكات أو الأشخاص، أو استهدف البُنى التحتية الوطنية الحيوية مسبباً ضرراً جسيماً لها.[25] وبعبارة أخرى فيعتمد التصور الإيراني على عتبة عالية، مثل الدمار الواسع أو الأذى البالغ للمرافق الحيوية، وهذا يتفق مع معيار الضرر المادي الملموس الذي تأخذ به دول عديدة.[26]

لكن إيران رغم تحديدها هذا المعيار المرتفع قد اكتنف إعلانها بعض الغموض حول الهجمات الأقل تدميراً. وعند مقارنة الموقف الإيراني بالمواقف الغربية يتضح أنّ إيران تتبنى موقفاً أشد تحفظاً. فمثلاً أعلنت فرنسا أنّها لا تستبعد أنّ عملية سيبرانية دون أضرار مادية استخداماً للقوة، إذا قيست بمعايير كالظروف والغايات ومدى التغلغل، كما أثارت هولندا عام 2019 التساؤل حول ما إذا كان الهجوم السيبراني ذو الأثر الاقتصادي الخطير قد يرقى إلى استخدام للقوة أم لا.[27] وهناك اتجاه متزايد تبنّاه خبراء دليل تالين 0.2 وحلف الناتو ودول كأستراليا، نحو تقييم الهجمات السيبرانية بناءً على شدة آثارها ونطاقها، وليس فقط بناءً على طبيعتها المادية.[28] ولا يرتقي رفع إيران لعتبة استخدام القوة عن قناعةٍ قانونيةٍ مجرّدة، بل يؤدّي وظيفةً دفاعيةً مزدوجة: تتمثل في تحصين عملياتها الهجومية من الوصف القانوني المُلزِم، وحرمان خصومها من السند المعياري للردّ المسلّح. ويكشف هذا الازدواج عن توظيف للقاعدة وليس تطبيقاً لحسن النية.

وتبدو إيران من خلال رفع سقف التعريف حريصة على تقييد الحالات التي يمكن أن تبرر رداً عسكرياً ضدها. فهي تدرك أنّ امتلاك خصومها ولا سيما الولايات المتحدة وإسرائيل، تفوقاً هائلاً في القدرات السيبرانية والتقليدية قد يمكّنهم من اتخاذ رد عسكري مشروع، إذا اعتُبرت أي هجمة إيرانية بسيطة استخداماً للقوة. لذا فإنّ تبنّيها لعتبة مرتفعة يضمن بقاء معظم عملياتها السيبرانية العدائية دون عتبة استخدام القوة المحظور، أو الهجوم المسلح الذي يتيح للخصم حق الدفاع الشرعي. وهذا يفسر ما خلص إليه الخبير مايكل شميت من أنّ إيران تريد وصف أي عملية ضدها بأنّها غير مشروعة، لكنّها

18 Military and Paramilitary Activities in and against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14 (June 27); see also: Iran General Staff Declaration, *supra* note 7.

19 MICHAEL N. SCHMITT, TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 41 (2d ed., Cambridge University Press 2017).

20 Iran General Staff Declaration, *supra* note 7; see also: Schmitt, Noteworthy Releases, *supra* note 10, at 10.

21 Moynihan, *supra* note 9, at 11.
انظر أيضاً: نادين هارون، **المسؤولية الدولية عن الهجمات السيبرانية في ظل القانون الدولي الإنساني**، رسالة ماجستير، جامعة العلوم التطبيقية الخاصة، عمان، 2023، ص 16.

22 Matthew C. Waxman, *Cyber Attacks as "Force" Under U.N. Charter Article 2(4)*, 87 INT'L L. STUD. 43, 43 (2011).

23 U.N. Grp. of Governmental Experts on Developments in the Field of Info. & Telecomms. in the Context of Int'l Sec., Note, U.N. Doc Symbol A/70/174 (2025), at 8.

24 Levi Grosswald, *Cyberattack Attribution Matters under Article 51 of the U.N. Charter*, 36 BROOK. J. INT'L L. 1151, 1157 (2011).
انظر أيضاً: عمر السعيدي وزياد جفال، "مدى اعتبار الهجمات السيبرانية انتهاكاً للحظر المفروض على استخدام القوة أو التهديد بها في ضوء أحكام القانون الدولي للجوء للحرب"، **مجلة جامعة الإمارات للبحوث القانونية**، المجلد 38، العدد 99، سبتمبر 2024، ص 397، 412.

25 Iran General Staff Declaration, *supra* note 7.

26 Schmitt, Noteworthy Releases, *supra* note 10, at 2.

27 Ministry of Defense of France, *International Law Applied to Operations in Cyberspace* (Sept. 9, 2019), https://cyberlaw.ccdcoe.org/wiki/National_position_of_France_(2019); see also: Michael Schmitt, *France's Major Statement on International Law and Cyber: An Assessment*, JUST SECURITY (2019), https://www.justsecurity.org/66194/frances-major-statement-on-international-law-and-cyber-an-assessment/; see also: Gov't of the Kingdom of the Neth., *Appendix: International Law in Cyberspace* (Sept. 26, 2019), https://cyberlaw.ccdcoe.org/wiki/National_position_of_the_Netherlands_(2019); see also: Michael Schmitt, *The Netherlands Releases a Tour de Force on International Law in Cyberspace: Analysis*, JUST SECURITY 3, 3 (2019), https://www.justsecurity.org/66562/the-netherlands-releases-a-tour-de-force-on-international-law-in-cyberspace-analysis/.

28 Dep't of Foreign Affairs & Trade (Austl.), *Australia's Position on How International Law Applies to State Conduct in Cyberspace* (2020), https://cyberlaw.ccdcoe.org/wiki/National_position_of_Australia_(2020).

تخشى وضع تعريف منخفض لسقف القوة السيبرانية، كي لا تمنح خصومها مسوغاً قانونياً لاستخدام قوتهم الساحقة رداً على عملياتها المعادية.[29]

وتأسيساً على ما سبق فيتضح أنّ الموقف الإيراني يتميز بازدواجية، فهو صارم ومنخفض العتبة في تحديد ما يعتبره انتهاكاً لسيادتها أو تدخلاً في شؤونها، حيث يُعدّ معظم الاختراقات عدواناً على سيادته، وفي الوقت ذاته مرن ومرتفع العتبة فيما يتعلق بتوصيف أعماله العدائية ضمن مفهوم استخدام القوة، إذ لا يعترف بكونها استخداماً محظوراً إلا في الحالات القصوى. وتمنح هذه الازدواجية إيران ميزة جدلية، فهي دائماً في موقع المُدّعي المظلوم عندما تتعرض لهجمات سيبرانية، وتطالب الآخرين باحترام سيادتها، وفي الوقت ذاته تُبقي أفعالها تحت سقف التصعيد الذي لا يستدعي رداً قانونياً قوياً.

2.4. حق الدفاع عن النفس

يُمثّل حق الدفاع الشرعي عن النفس استثناءً ضيقاً على حظر استخدام القوة، ويخوّل الدول المتضررة من هجوم مسلح الرد بالقوة اللازمة والمتناسبة لصد العدوان. وفي الفضاء السيبراني تطرح مسألة الدفاع عن النفس تحديات خاصة، أولها تحديد متى يبلغ الهجوم السيبراني حدّ الهجوم المسلح.[30] وكما بيّنّا فتعتقد إيران أنّ هذا الحد لا يُستوفى إلا إذا تسبب الهجوم في أضرار بالغة للبنى الحيوية، أشبه بهجوم عسكري تقليدي، وبالتالي فلن تعتبر نفسها في حالة دفاع شرعي إلا في مواجهة هجمات سيبرانية غاية في الخطورة.[31] أما الدول الغربية فتتبنى مواقف أكثر مرونة، فبعضها يترك الباب مفتوحاً لاعتبار الهجمات السيبرانية الكبيرة حتى بدون ضرر مادي، بمثابة هجوم مسلح إن كان أثرها الاستراتيجي جسيماً.[32] وعملياً لم تعلن أي دولة حتى الآن ممارستها الدفاع عن النفس عسكرياً، رداً على هجوم سيبراني، لكن احتمال ذلك قائم، بل ويزداد مع تزايد خطورة الهجمات السيبرانية العالمية.[33]

كما أنّ هناك تحدي آخر يتعلق بمبدأ الضرورة والتناسب، فإذا اعتُبر الهجوم السيبراني هجوماً مسلحاً، فإنّ أي رد دفاعي يجب أن يكون ضرورياً لوقف العدوان، ومتناسباً مع حجم الضرر. وفي الحالة الإيرانية فقد عبّرت هيئة الأركان عن معادلة واضحة: إذا بلغ الهجوم السيبراني عتبة العدوان المسلح، فإنّ إيران تحتفظ بحق الرد بشكل حازم.[34] ومن منظور قانوني فإذا تعرضت إيران لهجوم سيبراني جسيم، فإنّ أمامها جملة من الخيارات القانونية للرد قبل الوصول لعتبة استخدام القوة، كأعمال الانتقام غير العسكرية، والتدابير المضادة، وإحالة الأمر لمجلس الأمن. أما استخدام القوة المضادة فلا يُسمح به إلا دفاعاً عن النفس ضد هجوم مسلح.[35]

وأخيراً، فلم تتطرق إيران صراحةً في وثيقتها إلى حق توجيه ضربات سيبرانية وقائية لإحباط هجوم وشيك، وهو موضوع جدلي في القانون الدولي. غير أنّ ممارسات بعض الدول تشير إلى تبني مفهوم "الدفاع السيبراني الوقائي"، الذي يعني ضرب مصادر التهديد السيبراني قبل شن هجماتها. ويوازي هذا المفهوم عقيدة الضربات الاستباقية في الحرب التقليدية، وهو غير مقبول قانونياً إلا إن استوفى شرط الضرورة الملحة والتهديد الوشيك.

وبناءً على ما تقدّم، فيتبيّن أنّ الموقف الإيراني من الدفاع الشرعي يُعاني اختلالاً معيارياً مزدوجاً: فمن جهةٍ أولى يرفع عتبة "الهجوم المسلح" المُجيز للردّ الذاتي رفعاً يُفرغ المادة (51) من ميثاق الأمم المتحدة من فاعليتها الردعية في البيئة السيبرانية، إذ يحصر الردّ المشروع في صورةٍ افتراضيةٍ شبه مستحيلةٍ من حيث الأثر المادي. ومن جهةٍ ثانية يتغافل الإعلان الإيراني عن تنظيم التدابير المضادة السيبرانية بوصفها الأداة الوسطى بين الإدانة الدبلوماسية والردّ المسلّح، وهو سكوتٌ غيرُ بريء يُتيح لطهران الإفادة من المرونة العملية لتلك التدابير، دون أن تتحمّل أعباء انضباطها بشروط المشروعية المستقرّة في مشروع لجنة القانون الدولي لمسؤولية الدول (2001).

والمعالجة الأمثل في تقدير هذه الدراسة، أنّ الأمر يستوجب صياغةً تفصيليةً لعتبتين متمايزتين: عتبة الفعل غير المشروع دوليّاً التي تُتيح تدابير مضادةً غير قسرية، وعتبة الهجوم المسلح التي تُجيز الدفاع الشرعي، مع التمسّك بشرطَي الضرورة والتناسب، ورفض الصيغة المفتوحة للدفاع السيبراني الوقائي، التي تُخفي تحت غطاء الوقاية فعلاً عدوانيّاً سابقاً لأوانه.

2.5. التطبيق العملي والتحليل القانوني للحوادث السيبرانية

يركّز المبحث الثاني على تحليل أبرز الهجمات السيبرانية الإيرانية، وتأثيرها على القانون الدولي والعلاقات الدولية، بما في ذلك هجوم ألبانيا 2022، والهجمات على دول الخليج، والصراع السيبراني مع إسرائيل، إضافة إلى دعم إيران لمحور المقاومة. مع توضيح الوقائع والسياق السياسي لكل حادثة وتقييمها قانونياً، من حيث انتهاك السيادة أو التدخل أو استخدام القوة، مقارنة بالمبررات الإيرانية. وبيان كيف استغلت إيران الثغرات القانونية لصالحها، مع تصاعد التكاليف السياسية والقانونية نتيجة رفض دولي متزايد لهذه السلوكيات.

2.6. الهجوم على ألبانيا

في عام 2022 شهدت ألبانيا، العضو في حلف الناتو، هجمات سيبرانية خطيرة استهدفت البنية الرقمية الحكومية، بما في ذلك منصات خدمات المواطنين والمواقع الرسمية.[36] وقد بدأت المؤشرات الأولى في يوليو 2022 عندما تعطلت مواقع وزارات وخدمات إلكترونية مركزية، وانتشرت برمجيات خبيثة أدت إلى مسح بيانات وتعطيل أنظمة. واضطرت الحكومة لقطع الإنترنت عن المؤسسات الرسمية، كما تأثرت قدرة المواطنين على الوصول للخدمات العامة الرقمية لعدة أيام. وقد كان توقيت الهجوم حساساً، إذ تزامن مع استضافة ألبانيا لمؤتمر جماعة معارضة إيرانية، هي منظمة مجاهدي خلق، التي تتخذ من الأراضي الألبانية مقراً لها.[37]

شكّت السلطات الألبانية بارتباط الهجوم بهذا الحدث، حيث عارضت طهران بشدة سماح ألبانيا لمجاهدي خلق بالعمل من أراضيها. وقد أظهرت التحقيقات التقنية التي قامت بها السلطات الألبانية بمساعدة شركة مايكروسوفت وشركات أخرى، أدلة قوية على وقوف قراصنة إيرانيين خلف الاختراق، حيث تبيّن وقوف أربع مجموعات قرصنة وراء هذا الاختراق، أحدها

29 Schmitt, Noteworthy Releases, *supra* note 10, at 4.

30 Ferry Oorsprong, Paul Ducheine & Peter Pijpers, *Cyber–Attacks and the Right of Self–Defense: A Case Study of the Netherlands*, 6 POL'Y DESIGN & PRAC. 217, 218 (2023).

31 Iran General Staff Declaration, *supra* note 7.

32 Michael N. Schmitt, *Cyber Symposium—The Evolution of Cyber Jus Ad Bellum Thresholds*, WEST POINT 2, 2 (2022).

33 سارة العنبورية، **المسؤولية الدولية الجنائية عن الهجمات السيبرانية أثناء النزاعات المسلحة**، رسالة ماجستير، جامعة السلطان قابوس، 2023، ص 110.

34 Iran General Staff Declaration, *supra* note 7.

35 Przemyslaw Roguski, *Iran Joins Discussions of Sovereignty and Non–Intervention in Cyberspace*, JUST SECURITY (2020), https://www.justsecurity.org/72181/iran–joins–discussions–of–sovereignty–and–non–intervention–in–cyberspace/ [hereinafter Roguski].

انظر أيضاً: محمد ياسين سلمونة، مرجع سابق، ص 111.

36 Tal Pavel, *The Ripple Effect: Bilateral, Regional, and International Implications of Iranian Cyber Attacks on Albania*, INST. FOR CYBER POL'Y STUD. 109, 109 (2025).

37 *Id.* at 109.

مجموعة عدالة الوطن التي تعمل كواجهة لمجموعات تابعة للحرس الثوري الإيراني.[38] وتمثل الهدف المعلن في تسريب وثائق من الخوادم الحكومية الألبانية لإحراج الحكومة أو ابتزازها، حيث نشر المهاجمون لاحقاً معلومات شخصية لموظفين ألبان ورسائل بريد إلكتروني، كدليل على اختراقهم.

وقد استغرق التحقيق الألباني أسابيع قليلة، وفي سبتمبر 2022 خرج رئيس الوزراء الألباني إيدي راما ببيان رسمي، يتهم إيران صراحةً بالوقوف وراء الهجوم السيبراني، واصفاً إياه بمحاولة تعطيل مؤسسات الدولة، وشلّ الخدمات العامة بناءً على الأدلة الجنائية الرقمية.[39] وفور ذلك أعلنت ألبانيا قطع علاقاتها الدبلوماسية مع إيران، وطردت جميع موظفي السفارة الإيرانية. ما يُعدّ سابقة دولية تاريخية، فأول مرة تقطع دولة علاقاتها بسبب هجوم سيبراني. وأوضح راما أنّ القرار أتى بعد التشاور مع حلفاء الناتو، معتبراً الهجوم عدواناً سيبرانياً على سيادة بلاده.[40] وقد أدانت الولايات المتحدة والاتحاد الأوروبي وبريطانيا الهجوم، وعبروا عن تضامنه مع ألبانيا، بل إنّ حلف الناتو أصدر بياناً غير معتاد دعماً لعضوه، ندّد فيه بالهجوم، ودعا الدول الأخرى للتعاون لردع مثل هذه التهديدات.[41]

وعلى الجانب الإيراني فقد أتت ردة الفعل بالنفي والتنديد. حيث نفت وزارة الخارجية الإيرانية أي تورط، واعتبرت اتهامات ألبانيا مسيّسة ولا أساس لها، وزعمت أنّ قطع العلاقات خطوة غير مدروسة. لكنّها ألمحت إلى موقفها من تواجد مجاهدي خلق في ألبانيا، إذ أشار المتحدث باسم خارجيتها إلى إيواء ألبانيا لجماعة إرهابية تهدد الأمن الإيراني، في تلميح يُفهم منه محاولة تبرير مبطن لما حدث. أي أنّ إيران أرادت القول بأنّه حتى لو قامت بذلك، وإن كان دون اعتراف، فهو بسبب استضافة أراضي ألبانيا منصة للتآمر ضدها. وهذا يمثّل ذريعة سياسية حاولت طهران إثارتها، لكنّها لم تجد تعاطفاً دولياً يذكر.[42]

2.6.1. التكييف القانوني للهجوم

انتهاك السيادة وعدم التدخل أم استخدام للقوة؟ من منظور القانون الدولي فقد شكّل الهجوم السيبراني على ألبانيا انتهاكاً جسيماً لسيادة دولة مستقلة. فقيام عناصر مرتبطة بدولة أجنبية باختراق أنظمة حكومية وتعطيلها ومسح بياناتها، هو تدخل مباشر في الوظائف الجوهرية للدولة المستهدفة. وبحسب قواعد القانون الدولي العرفي فهذا الفعل يرقى إلى مستوى انتهاك سيبراني للسيادة، حيث تم التعدي على بنى تحتية معلوماتية تقع ضمن الاختصاص الإقليمي الألباني دون موافقتها. إضافة لذلك فيمكن اعتباره خرقاً لمبدأ عدم التدخل، لأن الهجوم استهدف أجهزة حكومية في صميم مجال ألبانيا المحفوظ، واقترن بفعل إكراهي تمثّل في تعطيل البنى، وإجبار الدولة على قطع خدماتها مؤقتاً، وهو بذلك قد استوفى عنصري عدم التدخل المحظور. ولم تدّعِ إيران أي تبرير قانوني مشروع له، وبالتالي فلا يوجد ما يضفي عليه شرعية.[43]

وهذا الهجوم السيبراني رغم شلّه مؤقتاً للخدمات الحكومية الأساسية، إلا أنّه لم يتسبب في دمار مادي أو خسائر بشرية، لذا لا يُصنّف غالباً كاستخدام للقوة بالمعنى التقليدي للمادة 2(4).[44] ومع ذلك فيُعدّ انتهاكاً جسيماً للسيادة وتدخلاً فادحاً، وقد يلامس معيار استخدام القوة إذا أعاق الدولة بشكل خطير أداء مهامها الأساسية. وقد تعاملت ألبانيا مع الحادث على أنّه حدث خطير دون مستوى الحرب، لذا اعتمدت إجراءات دبلوماسية وعقابية، وطلبت دعماً تقنياً من حلفائها، دون تفعيل المادة (5) للدفاع الجماعي.

ويمكن أن يكيف هجوم 2022 على ألبانيا على أنّه انتهاك للسيادة بلغ حدّ المساس الفعلي بالوظائف الحكومية الأصيلة للدولة، دون أن يبلغ عتبة استخدام القوة بمدلول المادة (4/2) من ميثاق الأمم المتحدة.

ويقوم هذا التكييف على ثلاث ركائز:

- الركيزة الأولى. أنّ العملية عطّلت أداءَ وظائف حكوميةٍ أصيلة حين أجبرت الإدارة الألبانية على وقف خدماتها الرقمية المركزية، وهو ما يستوفي معيار انتهاك السيادة وفق القاعدة (4) من دليل تالين 2.0، وإذا أُريد إسنادُه إلى مبدأ عدم التدخّل بمدلوله المستقرّ في قضية نيكاراغوا (1986)، فإنّ ذلك يتوقّف على إثبات الإكراه الموجَّه إلى خياراتٍ تقع في صميم الاختصاص المحجوز للدولة، وهو عنصرٌ يصعب التسليم به في عمليةٍ تدميريةٍ عقابيةٍ لم تستهدف ثنيَ إرادة ألبانيا عن خيارٍ سياديٍّ بعينه، ومن ثَمَّ يبقى انتهاك السيادة هو السند الأمتن، والتدخّلُ سنداً احتياطيّاً متنازَعاً فيه.
- الركيزة الثانية. أنّ غياب الأثر المادي الجسيم على الأشخاص والممتلكات يُخرج الفعل من نطاق "استخدام القوة" المُقاس بمعيار "النطاق والآثار" الذي تبنّاه فريق دليل تالين 2.0 (القاعدة 69)، استناداً إلى عوامل التقدير الثمانية.
- الركيزة الثالثة. أنّ انعدام الإيذاء البشري والضرر العسكري المادي يُبعد الفعل عن عتبة الهجوم المسلح، التي يتوقّف عليها حقّ الدفاع الشرعي بمقتضى المادة (51) من الميثاق، وهي العتبة ذاتها التي تُحيل إليها المادة (5) من معاهدة شمال الأطلسي، دون أن تُنشئ معياراً مستقلّاً عنها.

وعلى هذا الأساس فقطع ألبانيا علاقاتها الدبلوماسية مع إيران لا يندرج في باب التدابير المضادة، وإنّما في باب الردّ غير الوُدّي: فهو فعلٌ مشروعٌ في ذاته لا تتوقّف مشروعيته على وجود فعلٍ غير مشروعٍ سابق، إذ لا تلتزم الدولة ابتداءً بإقامة علاقاتٍ دبلوماسية، ولها أن تُعلن أيّ عضوٍ في البعثة شخصاً غير مرغوبٍ فيه دون إبداء أسباب، وفقاً للمادة (9) من اتفاقية فيينا للعلاقات الدبلوماسية 1961. وبهذا يكون قطعُ العلاقات الردَّ المتناسب الذي يُجسّد سُلَّماً تدرّجيّاً للردّ السيبراني يربط شدّة الردّ بدرجة الانتهاك: من الردّ غير الوُدّي المتاح دائماً، إلى التدابير المضادة غير القسرية متى تحقّق فعلٌ غير مشروعٍ دوليّاً، فالدفاع الشرعي عند بلوغ عتبة الهجوم المسلح دون قفزةٍ مباشرةٍ من الصمت إلى استخدام القوة. وهو ما تدعو إليه هذه الدراسة.

2.6.2. التداعيات القانونية وقطع العلاقات الدبلوماسية

ترتب على هذا الهجوم سابقة دبلوماسية وقانونية مهمة، إذ أصبحت إيران أول دولة يُقطع الاتصال الدبلوماسي معها بسبب هجمة سيبرانية.[45] هذا

38 Davi Ottenheimer, *Albania Breaks Ties with Iran after 2022 Microsoft Investigation of CVE-2019-0604*, https://www.flyingpenguin.com/albania-breaks-ties-with-iran-following-a-2022-microsoft-investigation-of-cve-2019-0604/ (last visited 9 March 2026).

39 James Andrew Lewis, *Iran's Cyberattacks on Albania Highlight NATO's Cyber Gaps*, WORLD POL. REV. (Oct. 14, 2022), https://www.worldpoliticsreview.com/albania-nato-iran-cyberattack-mek/.

40 NATO Coop. Cyber Def. Ctr. of Excellence, *Homeland Justice Operations against Albania (2022)*, INT'L CYBER L.: INTERACTIVE TOOLKIT (Mar. 1, 2024), https://cyberlaw.ccdcoe.org/wiki/Homeland_Justice_operations_against_Albania_(2022).

41 North Atl. Council, *Statement by the North Atlantic Council Concerning the Malicious Cyber Activities against Albania* (Sept. 8, 2022), https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2022/09/08/statement-by-the-north-atlantic-council-concerning-the-malicious-cyber-activities-against-albania.

42 Iranian Ministry of Foreign Affairs, *The Iranian Ministry of Foreign Affairs Strongly Condemns Albania's Anti-Iran Measure*, https://en.mfa.gov.ir/portal/newsview/en.mfa.gov.ir (last visited 28 March 2026).

43 فاضل عبد الزهرة، "التكييف القانوني لدور المدنيين في الهجمات السيبرانية"، **مجلة الكوفة للعلوم القانونية والسياسية**، المجلد 17، العدد 59، حزيران 2024، ص 1458.

44 Waxman, *supra* note 22, at 47.

45 Tim Starks & Aaron Schaffer, *Albania Is the First Known Country to Sever Diplomatic Ties over a Cyberattack*, WASH. POST (Sept. 8, 2022), https://www.washingtonpost.com/politics/2022/09/08/albania-is-first-known-country-sever-diplomatic-ties-over-cyberattack/.

التطور يحمل رسالة قانونية مفادها أنّ الدول باتت تنظر لبعض الهجمات السيبرانية كأفعال عدائية جسيمة تبرر إجراءات مضادة مشددة. فقطع العلاقات يعتبر إجراء انتقامياً مشروع لا ينتهك القانون الدولي كونه ضمن حقوق الدولة السيادية في تقرير علاقاتها. لذا فقد كان الرد الألباني متوافقاً مع القانون وأرسل إشارة قوية لإيران أنّ المجتمع الدولي لن يتساهل مع هذه الاعتداءات الرقمية.

ومن التداعيات الأخرى، أنّ ألبانيا رفعت قضية الهجوم إلى مجلس الناتو باعتبارها تهديداً لأمن الحلف. وعلى الرغم من أنّ الحلف لم يعتبره حالة تستدعي دفاعاً عسكرياً جماعياً، لكنّه فعّل لأول مرة آلية الدعم السيبراني الجماعي بتقديم خبرات تقنية وتعاون استخباراتي.[46] وهو تطور مهم يدل على أنّ الحلفاء يرون في الهجمات السيبرانية الخطيرة أمراً يستوجب الرد الجماعي المنسق، حتى لو لم يكن عسكرياً. كذلك ناقش الاتحاد الأوروبي الأمر وأصدر الاتحاد الأوروبي بياناً رسمياً يدين الهجمات ويعبّر عن التضامن الكامل مع ألبانيا، بينما فرضت الولايات المتحدة عقوبات فعلية ضد وزارة الاستخبارات الإيرانية ووزيرها.[47]

الخلاصة في حالة ألبانيا: لدينا هجوم سيبراني قامت به إيران بدافع كبح معارضيها، فكان غير مشروع وانتهاكاً صارخاً لسيادة دولة أخرى، ولم تنجح إيران في تفادي المسؤولية إذ تمت تسميتها علناً، ودفعت ثمناً دبلوماسياً باهظاً. تؤشر هذه الحادثة إلى خط تصعيدي خطير في سلوك إيران، قابله رفع في مستوى الرد الدولي. وهو ما يجعلها محطة محورية في تطور الأعراف القانونية السيبرانية، من الآن فصاعداً، تعرف الدول أنّ الهجوم على بنى دولة رقمية قد يعتبر عدواناً يتجاوز مجرد التجسس الخفي، بل عمل عدائي يؤدي لعواقب فورية كقطع العلاقات.

2.7. العمليات ضد دول الخليج

لطالما اعتبرت إيران بعض دول الخليج العربي منافسين إقليميين وأطرافاً في معسكر مناوئ لها. ومع تنامي قدراتها السيبرانية، بدأت في مطلع العقد الثاني من الألفية الثالثة توظيف الهجمات السيبرانية ضد هذه الدول، مركزةً على قطاعاتها الاقتصادية الحيوية. ولقد كانت أبلغ رسالة سيبرانية إيرانية هجوم شمعون عام 2012 على شركة أرامكو السعودية، حيث ضرب الفيروس شبكة حواسيب أرامكو فمسح بيانات حوالي 30 ألف حاسوب وأدى إلى توقف عملياتها الرقمية بالكامل وتعطل خدمات الإنتاج النفطية جزئياً.[48] وسرعان ما تبيّن أنّ الفيروس الذي حمل صورة علم أمريكي محترق قد صُمم ليُحدث أقصى ضرر عبر حذف سجلات الإقلاع واستبدالها. وعلى الرغم من عدم تأثيره على منشآت المعالجة الفيزيائية للنفط، إلا أنّه كبّد الشركة خسائر كبيرة وكان أكبر هجوم إلكتروني معروف ضد شركة نفطية حتى تاريخه.[49] وقد حمّلت الولايات المتحدة إيران المسؤولية عن الهجوم. ولكن رغم أنّ بعض الباحثين يميزون بين المجموعة التي استخدمت فيروس شمعون ومجموعات إيرانية أخرى معروفة مثل APT33 التهديد المستمر المتقدم رقم 33، إلا أنّ الإجماع يشير إلى أنّ الهجوم كان جزءاً من عمليات سيبرانية إيرانية أوسع.[50]

ومما يؤكّد أنّ هجوم 2012 لم يكن حادثة معزولة، وإنّما جزءاً من نمط مستمر، تكرّر ظهور سلالات مطوّرة من شمعون في 2016 و2017 استهدفت شركات في قطاع الطاقة السعودي، كما تعرضت شركة رأس غاز القطرية لهجوم مشابه في 2012.[51] وهو ما يشير إلى حملة إيرانية ممنهجة لضرب قطاع النفط الخليجي بغرض إيصال رسائل انتقامية. والملفت للانتباه أنّه بالتزامن، قامت إيران بسلسلة هجمات على قطاع المال والمصارف، فبين 2012 و2013 تعرضت بنوك أمريكية كبرى لعشرات هجمات حجب الخدمة الموزعة مما عطل مواقعها الإلكترونية.[52] وأُعلن أنّ تلك الهجمات نفذتها مجموعة مرتبطة بإيران باسم "عملية أبابيل"، رداً على فيلم مسيء للإسلام وعلى السياسات الأمريكية.[53] والمؤكد من مصادر استخباراتية أنّ العملية نسقها الحرس الثوري واستهدفت المصارف الأمريكية ومؤسسات مالية خليجية، متسببة بأضرار مالية وهلع بين العملاء وتُعدّ سابقة خطيرة لاستهداف النظام المالي.[54]

إلى جانب هذا المسار التدميري العلني فقد فتحت إيران جبهة موازية أقل ضجيجاً وأبعد أثراً، إذ انخرطت في عمليات تجسس إلكتروني مكثّفة ضد حكومات خليجية وشركاتها، إذ كُشفت حملة (أول ريج OilRig) التي نفذتها مجموعة APT34 الإيرانية (التهديد المستمر المتقدم رقم 34)، استهداف وزارات خارجية وداخلية وشركات اتصالات في السعودية والإمارات والبحرين، مستخدمة برمجيات خبيثة للحصول على بيانات حساسة واختراق بريد مسؤولين.[55] وهذا جانب آخر من الحرب السيبرانية الإيرانية ضد الخليج لجمع المعلومات الاستخباراتية وتحسين موقفها الاستراتيجي.

2.7.1. التكييف القانوني

مبدأ عدم التدخل مقابل الضرورة الأمنية، فالهجمات الإيرانية على دول الخليج وخاصة الهجمات التدميرية كعمليات شمعون تشكل من منظور القانون الدولي تدخلاً عدائياً سافراً في شؤون تلك الدول. فاستهداف شركة وطنية كبرى كأرامكو أو تعطيل بورصة مالية سعودية هو تعدٍّ على العمود الفقري الاقتصادي للدولة، ويعطل وظائف أساسية لها علاقة برفاه شعبها واستقرارها، لذلك فهي انتهاك للسيادة، لأنّه اختراق لبنى تحت سيطرة

46 Maggie Miller, *Albania Weighed Invoking NATO's Article 5 over Iranian Cyberattack*, POLITICO (Oct. 5, 2022), https://www.politico.com/news/2022/10/05/why-albania-chose-not-to-pull-the-nato-trigger-after-cyberattack-00060347.

47 Council of the EU, *Cyber-Attacks: Declaration by the High Representative on Behalf of the European Union Expressing Solidarity with Albania and Concern Following the July Malicious Cyber Activities* (Sept. 8, 2022), https://www.consilium.europa.eu/en/press/press-releases/2022/09/08/cyber-attacks-declaration-by-the-high-representative-on-behalf-of-the-european-union-expressing-solidarity-with-albania-and-concern-following-the-july-malicious-cyber-activities/.

48 Salem Alelyani & Harish Kumar G.R., *Overview of Cyberattack on Saudi Organizations*, 1 J. INFO. SEC. & CYBERCRIMES RES. 32, 32 (2018).

49 United Against Nuclear Iran, *History of Iranian Cyber Attacks and Incidents* (2025), https://www.unitedagainstnucleariran.com/history-of-iranian-cyber-attacks-and-incidents [hereinafter UANI].

50 Jacqueline O'Leary et al., *Insights into Iranian Cyber Espionage: APT33 Targets Aerospace and Energy Sectors and Has Ties to Destructive Malware*, GOOGLE CLOUD BLOG, https://cloud.google.com/blog/topics/threat-intelligence/apt33-insights-into-iranian-cyber-espionage (last visited 3 February 2026).

51 UANI, *supra* note 49.

52 Gabrielle Christello, *The Rise of Iran's Cyber Capabilities and the Threat to U.S. Critical Infrastructure*, 12 CTR. FOR SEC. STUD. 12, 12 (2024).
انظر أيضاً: باخان ئاكو نجم الدين، "تأثير الحرب السيبرانية على رفع مستوى الصراع بين الولايات المتحدة الأمريكية وإيران"، **مجلة جامعة رابرين**، العدد 4، ديسمبر 2021، ص 12.

53 Matan Mimran, *Iran Strikes Back?*, CYBEREASON BLOG, https://www.cybereason.com/blog/iran-strikes-us-with-cyberattack-over-nuclear-deal (last visited 19 January 2026).

54 Christello, *supra* note 52, at 13.
انظر أيضاً: إيناس سليمان، "دور الأمن السيبراني في مواجهة الإرهاب الإلكتروني"، **مجلة العلوم القانونية والاقتصادية**، المجلد 64، العدد الأول، يناير 2022، ص 9.

55 Daryna Antoniuk, *Alleged Iranian Hackers Target Victims in Saudi Arabia with New Spying Malware*, THE RECORD, https://therecord.media/alleged-iran-hackers-target-saudi-arabia-with-new-spy-malware (last visited 23 January 2026).

الدولة، وانتهاك لمبدأ عدم التدخل لأنّها أعمال إكراهية تضر باقتصاد الدولة وهو مجال محفوظ داخلي.[56]

والظاهر أنّ ن أتأن بعض الدول لم تستبعد ذلك ففي حالة أرامكو، تم مسح بيانات 30 ألف حاسوب وقُدّرت التكلفة المباشرة بأكثر من 15 مليون دولار عدا الخسائر غير المباشرة. وإن كان ذلك لا يبلغ مستوى قصف منشأة نفطية بالطائرات، فإنّه يُعادل عملية تخريب صناعية محدودة، وبالتالي قد يكون عتبة دنيا من استخدام القوة بالمفهوم الاقتصادي. لكن الرأي السائد خاصة في 2012 أنّه لم يصل لتلك المرحلة لعدم وقوع أضرار مادية، وموقف السعودية العلني دعم ذلك إذ لم تعتبره هجوماً مسلحاً واكتفت بالإدانة وتعزيز أمنها السيبراني. ومن ثم يرجح أنّ هذه الهجمات تبقى في إطار الأعمال العدائية غير المسلحة المحظورة، أي تدخلات سيبرانية غير مشروعة دون مستوى الحرب.[57]

2.7.2. تحديات الإسناد القانوني والإفلات من المساءلة

بالرغم من وضوح عدم مشروعية هذه الهجمات، فوّت معظمها عقاباً دولياً مباشراً لإيران بسبب تحديات الإسناد. ففي 2012، عندما ضرب شمعون أرامكو، لم تملك السعودية قدرة رقمية كافية لتحديد الفاعل فوراً. اتجهت الشكوك نحو إيران، لكن لم يكن هناك إعلان رسمي سعودي باتهامها. وحتى حين نُسبت الهجمات لاحقاً إلى إيران، اختارت الرياض الرد بشكل غير مباشر عبر زيادة إنفاقها على الأمن السيبراني لكنّها لم تلجأ لمحافل دولية. هذا يبرز كيف أنّ ضعف أدوات الإسناد العلني سمح لإيران بالإنكار والإفلات، فلم تواجه أي عقوبة أممية أو حملة إدانة جماعية على هجماتها السيبرانية، لانشغال العالم بملفها النووي والصراعات العسكرية في المنطقة.

وتترتّب على ثغرة الإسناد هذه نتيجة أبعد مدى، إذ لم تحاول أي دولة خليجية حتى الآن رفع قضية مسؤولية دولية ضد إيران لدى محكمة العدل الدولية بخصوص هجوم سيبراني، وهكذا بقيت إيران بمنأى عن المحاسبة القانونية المباشرة. لكنّها دفعت ثمناً إستراتيجياً، فقد عجّل سلوكها بقيام تحالفات إقليمية ضدها، إذ كانت مواجهة الخطر السيبراني الإيراني أحد دوافع تقارب بعض دول الخليج مع إسرائيل. كما دفعت دول الخليج للإنفاق بسخاء على تطوير أمنها السيبراني وسد الثغرات التي عبرت منها إيران. ومن المفارقات أنّ هجمات إيران قوّت خصومها سيبرانياً على المدى البعيد، فأنشأت دول الخليج وكالات وطنية للأمن السيبراني وأصبحت أكثر جاهزية، مما قد يردع إيران عن شن هجمات مماثلة خشية الفشل أو الكشف الفوري.[58]

ولا يعود تعذُّرُ المساءلة القانونية المباشرة عن الأفعال المنسوبة إلى إيران في عمليات شمعون وأبابيل وأويل ريغ إلى قصورٍ في القاعدة الموضوعية، بل إلى قصورٍ في الآليات الإجرائية للإسناد والإثبات أمام المحافل الدولية. فالقانون الدولي يملك من الأدوات ما يكفي لتكييف هذه الأفعال على تفاوتٍ في طبيعتها، ليس فقط بوصفها انتهاكاً للسيادة، بل تدخّلاً محظوراً، حيث يتوافر عنصر الإكراه، غير أنّ التطبيق الفعّال يصطدم بثلاث عقبات بنيوية، وهي:

- الأولى: الطابع التقني لأدلة الإسناد، إذ تتطلّب قدراتٍ في الأدلة الجنائية الرقمية لا تملكها كثيرٌ من الدول المُستهدَفة.
- الثانية: انعدام المحفلِ القضائيِّ المتخصّصِ الذي ينظر النزاعات السيبرانية بقواعد إثباتٍ تُراعي طبيعتها.
- الثالثة: أنّ لجوء دول الخليج إلى الردّ غير المباشر، وإن كان مفهوماً من زاوية الواقعية السياسية، إلا أنّه قد أسهم في ترسيخ ممارسةٍ سلبيةٍ تُضعف تبلوُر عنصرٍ مادّيٍّ لعرفٍ دوليٍّ مقاومٍ لهذا السلوك.

ومن هنا تدعو هذه الدراسة إلى قبول الإثبات بالقرائن القاطعة، متى حالت سيطرةُ الدولة المصدر على بنيتها التقنية دون الوصول إلى الدليل المباشر، وذلك اقتداءً بمسلك محكمة العدل الدولية في قضية مضيق كورفو (1949)، حين أجازت الاستدلال بسلسلةٍ من القرائن لا تدع مجالاً معقولاً لتفسيرٍ بديل، باعتباره الأقدر على ردم فجوة الإسناد دون التضحية بضمانات العدالة.

2.8. الصراع السيبراني مع إسرائيل

يُمثّل الصراع السيبراني الإيراني الإسرائيلي نموذجاً تطبيقياً بالغ الدلالة لإشكالية لتكييف العمليات السيبرانية في القانون الدولي، إذ تتداخل فيه ثلاث مسائل فقهية دقيقة: الأولى عتبة استخدام القوة، والثانية إسناد العمليات إلى الدول، والثالثة تكييف الرد المشروع في غياب الإعلان الرسمي.

ويُمكن إرجاع بداية هذا الصراع إلى هجوم "ستاكسنت" عام 2010 الذي استهدف البرنامج النووي الإيراني بتخطيط أمريكي إسرائيلي، إذ يُعدّ أول عملية سيبرانية رأى فيها عدد من الفقهاء تجسيداً فعلياً لعتبة استخدام القوة، وذلك بسبب ما أحدثه من تلف مادي في أجهزة الطرد المركزي، وقد اضطرّ هذا الهجوم إيران إلى تعجيل تعزيز دفاعاتها السيبرانية.[59] منذ ذلك الحين، اعتبرت إيران نفسها في حالة مواجهة مع إسرائيل في الفضاء الرقمي فشرعت بتطوير وحداتها الهجومية للرد. ومن 2012 فصاعداً، رصد الخبراء عمليات إيرانية تستهدف إسرائيل، من محاولات اختراق أنظمة البنية التحتية كالكهرباء والمياه، إلى حملات تأثير إعلامي عبر الإنترنت.[60]

أحد أبرز الأمثلة كان في أبريل 2020، حين تعرضت شبكة توزيع المياه الإسرائيلية لهجوم سيبراني كاد يعبث بجرعات المواد الكيميائية في المياه. اتهم مسؤولون إسرائيليون إيران بالمسؤولية عن هذا الهجوم الذي لو نجح لأحدث أزمة صحية.[61]

وتثير هذه الواقعة تساؤلاً فقهياً دقيقاً: هل يبلغ الهجوم على مرفق مدني حيوي لو أفضى إلى أذى بشري واسع عتبة الهجوم المسلح بمفهوم المادة (51) من ميثاق الأمم المتحدة؟ ويرى فقهاء التيار الغالب ومنهم فريق تالين 0.2 أنّ الجواب بالإيجاب، إذا بلغت الآثار المرجوّة من الخسائر البشرية والمادية مستوى الأذى الناجم عن سلاح تقليدي. وعلى إثر هذه الواقعة فقد ردّت إسرائيل بهجوم إلكتروني على ميناء الشهيد رجائي الإيراني في مايو 2020، فأصاب نشاطه بالشلل عدة أيام. ويطرح هذا الردّ بدوره إشكالية قانونية مزدوجة: فهل يتم تكييفه تدبيراً مضاداً مشروعاً تحت مواد مسؤولية الدولة عن الأفعال غير المشروعة دولياً، أم بوصفه دفاعاً شرعياً استباقياً؟ ولعلّ اختيار إسرائيل عدم إعلان المسؤولية رسمياً رغم تناقل الصحافة الدولية للرواية، يُعبّر عن خيار محسوب لتجنّب تغليظ التكييف القانوني

56 انظر أيضاً: نادين هارون، مرجع سابق، ص 36.

57 Christopher Bronk & Eneken Tikk-Ringas, *Hack or Attack? Shamoon and the Evolution of Cyber Conflict*, JAMES A. BAKER III INST. FOR PUB. POL'Y 7, 7 (2013).

58 مشعل راضي راشد الفهيد الهاجري، "الحوكمة الرقمية كمدخل لتعزيز الأمن السيبراني في المؤسسات القطرية"، **مجلة الباحث للدراسات والأبحاث العلمية**، العدد 84، أكتوبر 2025، ص 337.

59 Mariusz Kamiński, *Operation "Olympic Games": Cyber-Sabotage as a Tool of American Intelligence Aimed at Counteracting the Development of Iran's Nuclear Programme*, 29 SEC. & DEF. Q. 63, 64 (2020).

60 Gawdat Bahgat, *Iranian–Israeli Confrontation: The Cyber Domain*, 27 MIDDLE EAST POL'Y 115, 118 (2020).
انظر أيضاً: علي فارس حميد، "نقاط الانكشاف والضعف في الصراع الإيراني الإسرائيلي: قراءة استراتيجية"، **مجلة تكريت للعلوم السياسية**، العدد 31، مارس 2023، ص 15.

61 JD Work & Richard Harknett, *Troubled Vision: Understanding Recent Israeli–Iranian Offensive Cyber Exchanges*, ATL. COUNCIL (July 22, 2020), https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/troubled-vision-understanding-israeli-iranian-offensive-cyber-exchanges/.

لفعلها، وهو مسلك تلتقي فيه الدولتان باعتباره أداة إدارة للتصعيد تحت سقف المساءلة.[62]

منذ ذلك الحدث، انخرط الطرفان فيما يشبه حرب ظلال سيبرانية، هجمات مستمرة منخفضة الحدة دون اعتراف رسمي. فظهرت مجموعات قرصنة موالية لإيران تحمل أسماء مثل "عصا موسى" و"الأيادي السوداء" تستهدف مواقع ومنشآت إسرائيلية.[63] فيما برزت مجموعات موالية لإسرائيل مثل Predatory Sparrow المعروفة بالصقر المفترس، والتي تبنّت مسؤولية هجوم سيبراني تسبب في حريق بمصنع إيراني للصلب، كما هاجمت مجموعات إيرانية شركات تأمين ومستشفيات في إسرائيل وسربت بيانات حساسة.[64] وفي سياق متصل، جاءت حرب الاثني عشر يوماً في يونيو 2025 لتكشف بصورة أوضح عن بنية الفاعلين السيبرانيين الإيرانيين وتكامل أدوارهم. فقد برزت ثلاث دوائر رئيسية:

وفي شهر مايو 2020 نُشرت رسالة كاذبة عن حادث كيميائي في إسرائيل أثارت بلبلة اتهمت إسرائيل إيران بنشرها.[65] كذلك استخدم الطرفان جيشاً من الحسابات الوهمية على مواقع التواصل لنشر محتوى دعائي أو مضلل. وبرز استخدام تقنيات الذكاء الاصطناعي، فعّلت إيران منظومة روبوتات تدار بالذكاء الاصطناعي لخلق محتوى إعلامي موجّه بالعبرية أثناء حرب غزة لتأليب المواطنين ضد حكومتهم، فيما تستعين إسرائيل بتقنيات تعلّم الآلة لتحليل الثغرات في شبكات إيرانية وللقيام بهجمات دقيقة على أهداف محددة.[66]

وتكتسب هذه الديناميكية دلالتها القانونية حين تُقرأ في ضوء مفهوم سباق التسلح السيبراني، والذي يتراوح تكييفه الفقهي بين الوسيلة الدفاعية المشروعة، وبين الترسّخ التدريجي لحالة عدائية سيبرانية مستديمة، تخرق واجب حلّ النزاعات بالوسائل السلمية. فكلتا الدولتين تُوظّفان موارد ضخمة وتتبادلان الخبرات مع حلفائهما، لتطوير أدوات اختراق ودفاع، فيما يُشبه بنية ردع متبادل غير معلن.[67] كما تترافق الهجمات أحياناً مع توترات عسكرية، عند اغتيال إسرائيل لقاسم سليماني مطلع 2020، حصلت محاولات اختراق إيرانية مكثفة ضد أهداف إسرائيلية وأمريكية، وحين قصفت إسرائيل مواقع إيرانية في سوريا، تلا ذلك نشاط متزايد لقراصنة إيرانيين. أي أنّ الفضاء السيبراني بات جبهة رد موازية يلجأ إليها كل طرف لمعادلة الضغوط.[68]

وما يجري بين إيران وإسرائيل يشكل، من منظور القانون الدولي، تحدياً للأطر القانونية. فرسمياً، لا توجد حرب معلنة بين البلدين، لكنّهما منخرطان في نزاع مسلح فعلي غير مباشر في ساحات عدة. فالهجمات السيبرانية المتبادلة تضفي بعدًا آخر، ومعظمها يُصنف كعمليات سيبرانية عدائية غير مرتبطة بمواجهة تقليدية مباشرة، فتنطبق عليها قواعد السلم، من سيادة وعدم تدخل وحظر استخدام القوة. وهنا مكمن خطورة، والذي يتجلى خاصة في غياب ردع قانوني واضح سمح بتصاعد الهجمات. فكل طرف يعلم أن الآخر منخرط أيضاً، فاستبعدا احتمال اللجوء لمنظومة قانونية. وهكذا تحوّل الفضاء السيبراني لساحة مفتوحة دون قواعد.

بالنتيجة، يمكن وصف النزاع السيبراني بين إيران وإسرائيل بأنّه صراع منخفض الحدة عالي التقنية، ينشط في فجوات القانون، حيث يهاجم كل منهما بما يتعارض مع القانون الدولي دون إعلان ذلك. ويُبدي المجتمع الدولي قلقه إزاء ذلك، غير أنّه يجد صعوبة في التدخل. إنهاء هذا النزاع أو ضبطه قانونياً يتطلب تسوية سياسية أوسع أو إرساء أعراف قوية. وإلى أن يحصل ذلك، سيبقى مثالاً على محدودية القانون الحالي في وقف حرب سيبرانية باردة بين خصمين لدودين، ومجالاً خصباً لتطوير مفاهيم جديدة حول الأمن الجماعي السيبراني.

غير أنّ التوصيف الفقهي السائد لهذا الصراع بوصفه حرب ظلال يُغفل بُعداً معيارياً جوهرياً: فصمت الطرفين عن إعلان المسؤولية لا يرفعها عنهما، بل يُفاقمها، إذ يقترن بانتهاك القاعدة الموضوعية إخلالٌ بالتزام العناية الواجبة، وبمبدأ التسوية السلمية للنزاعات المكرّس في المادة (3/2) من ميثاق الأمم المتحدة، على نحوٍ ينمّ عن سوء نيةٍ في أداء الالتزامات الدولية. ويصطدم ادّعاءُ كلٍّ من الطرفين "التدبير المضاد" تكييفاً مشروعاً لأفعاله بعقبةٍ أعمق من الشكل الإجرائي، فالمادة (49) من مشروع مسؤولية الدول تشترط أن يكون غرض التدبير حمل الدولة المسؤولة على الامتثال، لا ردعها ولا معاقبتها، والردعُ المتبادل بحكم طبيعته العقابية يفشل في هذا الشرط.

ويُضاف إلى ذلك أنّ السرّية والإنكار يناقضان بنية التدبير المضاد ذاتها، التي تفترض ظهور الدولة المتّخِذة له ردّاً على فعلٍ منسوبٍ معلوم، حفظاً لطابعه المؤقّت القابل للارتداد متى توقّف الفعل الأصلي غير المشروع (المادتان 49 و53). ومن ثَمَّ فإنّ ما يُسمّى بالردع المتبادل غير المعلن ليس قاعدةً قانونيةً ناشئة، بل ممارسةٌ غير مشروعةٍ ثنائية، لا ينبغي للفقه أن يُسبغ عليها شرعيةً ضمنيةً عبر التطبيع الوصفي.

وفي هذا السياق فتدعو هذه الدراسة إلى تفعيل وسائل التسوية السلمية المنصوص عليها في المادة (33) من الميثاق من وساطةٍ وتوفيقٍ وتحكيم، بل إلى عرض النزاع على محكمة العدل الدولية متى قَبِل الطرفان ولايتها، بوصفها المحفل الأقدر على تقرير المسؤولية عن الانتهاكات السيبرانية المتبادلة.

2.9. الدعم السيبراني لمحور المقاومة

إلى جانب انخراطها المباشر، تستخدم إيران الفضاء السيبراني كأداة رئيسية لدعم حلفائها الإقليميين فيما يُعرف بمحور المقاومة، وذلك كجزء من استراتيجيتها الأوسع للحرب غير المتكافئة. ويأخذ هذا الدعم أشكالاً مختلفة تتناسب مع قدرات كل حليف، فيُعتبر حزب اللّه في لبنان الشريك الأكثر تطوراً، حيث تُعزى مهاراته السيبرانية العالية جزئياً إلى علاقاته الوثيقة بالحكومة الإيرانية، واستخدامه لتقنيات مستمدة على الأرجح من أساليب إيرانية.[69] أما حماس في فلسطين، فتتلقى دعماً إيرانياً مباشراً، خاصة في مجال عمليات التأثير، حيث شنّت جهات فاعلة إيرانية عمليات سيبرانية ونفسية منسقة لدعمها في أعقاب هجوم أكتوبر 2023 بهدف تقويض الدعم الدولي لإسرائيل.[70] وبالنسبة للحوثيين في اليمن وبعض الفصائل في العراق، يتركز

62 Work & Harknett, *supra* note 61.

63 Chuck Freilich, *The Iranian Cyber Threat*, INST. FOR NAT'L SEC. STUD. 4, 4 (2024).

64 Joe Tidy, *Predatory Sparrow: Who Are the Hackers Who Say They Started a Fire in Iran?*, BBC (2022), https://www.bbc.com/news/technology-62072480.

65 Ayesha Haroon, *AI and Cyber Drove Warfare in the Israeli–Iran Conflict and Its Impact on Gulf States' Security*, 10 J. POL. & INT'L STUD. 145, 145 (2024).

66 Basim Tweissi, *Iran vs. Israel: How Deception and the Information War Shaped Public Perceptions*, ARAB CTR. FOR RES. & POL'Y STUD. 7, 7 (2025).

67 Netolická & Mareš, *supra* note 1, at 414.
انظر أيضاً: هبة عبدالسلام خطاب الناصري ومثنى فائق مرعي، "مؤسسات الفضاء السيبراني في منطقة الشرق الأوسط: إيران وإسرائيل أنموذجاً"، **مجلة تكريت للعلوم السياسية**، العدد 30، ديسمبر 2022، ص 5.

68 Annie Fixler, *The Cyber Threat from Iran after the Death of Soleimani*, COMBATING TERRORISM CTR. AT W. POINT 1, 1 (2020), https://ctc.westpoint.edu/cyber-threat-iran-death-soleimani/.

69 Daniel Byman & Emma McCaleb, *Understanding Hamas's and Hezbollah's Uses of Information Technology*, CTR. FOR STRATEGIC & INT'L STUD. (July 31, 2023), https://www.csis.org/analysis/understanding-hamass-and-hezbollahs-uses-information-technology.

70 Microsoft Threat Intelligence, *Iran Surges Cyber-Enabled Influence Operations in Support of Hamas* (Aug. 1, 2025), https://www.microsoft.com/en-gb/security/security-insider/intelligence-reports/iran-surges-cyber-enabled-influence-operations-in-support-of-hamas/ [hereinafter Microsoft, Iran Surges].

الدعم الإيراني على المساعدة التقنية في تطوير أسلحة متقدمة كالصواريخ والطائرات بدون طيار، والتي تعتمد على مكونات إلكترونية معقدة.[71] هذا الدعم السيبراني والتقني هو جزء لا يتجزأ من استراتيجية الدفاع المتقدم الإيرانية، التي تهدف إلى مواجهة الخصوم في ساحات بعيدة، وتصدير التهديدات خارج حدودها، وتعزيز نفوذها الإقليمي عبر شبكة من الوكلاء المتمكنين تكنولوجياً.

وترى إيران بصفة رسمية أنّ دعمها لحلفائها يندرج ضمن عقيدة الدفاع المتقدم لمواجهة التهديدات بعيداً عن أراضيها. وعلى الرغم من أنّ هذه العقيدة تركز على الجانب العسكري التقليدي، إلا أنّه يمكن القياس عليها لفهم منطق الدعم الإيراني في الفضاء السيبراني. ويتوافق هذا الدعم مع الموقف الإيراني المعلن.[72] حيث أوضح وزير الخارجية أنّ دعم إيران لجماعات المقاومة يستند إلى رؤيتها بأنّ هذه الجماعات تقاتل من أجل الحقوق المشروعة لأممها، وهو ما يبرر الدعم الإيراني المتواصل رغم الضغوط الدولية.[73] غير أنّ استدعاء مفهوم الدفاع المتقدّم في هذا السياق، توسّعٌ غير مسنودٍ في القانون الدولي. فحقّ الدفاع عن النفس بمقتضى المادة (51) من ميثاق الأمم المتحدة معلّقٌ على وقوع هجومٍ مسلّح، وحتى في أوسع قراءاته المتنازَع فيها، فلا يتجاوز حدّ التهديد الوشيك وفق معايير كارولاين، أمّا الدفاع المتقدّم فيتخطّى ذلك إلى استباقِ تهديدٍ غير وشيك، وهو ما يفتقر إلى سندٍ في القانون الساري. وأبعدُ من ذلك فإنّ ما يقترنُ به من نقلٍ للقدرات السيبرانية إلى فاعلين من غير الدول لتنفيذ عملياتٍ من أراضي دولٍ ثالثة، يصطدم بعقبتين مستقلّتين عن مسألة الهجوم الوشيك: الأولى انتهاكِ سيادة الدولة الثالثة، والثانية تعذُّرِ إسناد الفعل إلى الدولة الموجّهة ما لم يبلغ التوجيهُ عتبة الإرسال أو السيطرة الفعلية المقرّرة في الاجتهاد الدولي.

2.9.1. فلسطين

تعتبر إيران نفسها راعياً للمقاومة الفلسطينية ضد إسرائيل، وتزوّد فصائل مثل حماس بالدعم المالي والعسكري والسياسي. وفي السنوات الأخيرة بدأت تظهر بوادر تعاون سيبراني، فعلى الرغم من أنّ قدرات حماس السيبرانية متواضعة، يُعتقد أنّ مهندسين إيرانيين ساعدوا في بناء وحدة الحرب السيبرانية التابعة لحماس.[74] خلال جولات الصراع الأخيرة لوحظت هجمات سيبرانية من غزة لاختراق هواتف جنود إسرائيليين، وتعطيل مواقع إعلامية. وهناك شواهد على أنّ إيران شاركت بأدوات، كبرمجيات تجسس استخدمتها حماس تبيّن أنّها نسخة من أدوات إيرانية.

وخلال حرب أكتوبر 2023 ذكرت تقارير أنّ قراصنة موالين لإيران شنّوا هجمات إلكترونية متزامنة مع الهجوم العسكري استهدفت مواقع إسرائيلية.[75] وأكّد مسؤولون إسرائيليون أنّ إيران كثفت هجماتها السيبرانية دعماً لحماس، مما يوضح كيفية استخدام إيران للجبهة السيبرانية لتخفيف الضغط عن حلفائها. من زاوية القانون الدولي، وهو ما يُعدّ تدخلاً في نزاع مسلح غير دولي لصالح طرف غير دولي ضد دولة، أي مشاركة غير مباشرة في الأعمال العدائية.[76]

ويستوي هذا النمط من المشاركة متى بلغ حدّ التوجيه التشغيلي للعمليات بعينها، معيارَ "السيطرة الفعلية" المقرَّر في قضية نيكاراغوا والمكرَّس في المادة (8) من مشروع مسؤولية الدول (2001)، فيُرتّب على إيران مسؤوليةً دوليةً عن الأفعال المنسوبة إلى الجماعات المدعومة منها. أمّا معيار "السيطرة الشاملة" الذي أرسته محكمة يوغوسلافيا السابقة في قضية تاديتش (1999)، فقد قصرته تلك المحكمة على تكييف طبيعة النزاع المسلّح، ورأت محكمة العدل الدولية في قضية الإبادة الجماعية (2007) أنّه يتجاوز حدود مسؤولية الدولة المقرَّرة في القانون الساري، ومن ثَمّ فالاستناد إليه لترتيب الإسناد المباشر يتطلّب الإقرار بأنّه طرحٌ بحاجةٍ إلى تطوير القاعدة، لا تطبيقٌ لها بصيغتها الراهنة.

2.9.2. لبنان

يمتلك حزب اللّه تاريخاً وثيقاً من الشراكة الاستخباراتية والعملياتية مع إيران، ويتلقى دعماً مباشراً من وزارة المخابرات الإيرانية (MOIS – Ministry of Intelligence and Security)، وفيلق القدس التابع للحرس الثوري.[77] ويتمثل هذا الدعم في تأهيل وتزويد عناصر حزب اللّه بالتدريب والأسلحة والخبرات التقنية اللازمة لتنفيذ عمليات استطلاع ومراقبة متقدمة، وهو تنسيق عالي المستوى يجعل من الصعب أحياناً التمييز بين عمليات الحرس الثوري وعمليات حزب اللّه، حيث يعمل الطرفان غالباً ككيان واحد في الساحات الخارجية.[78] وقانونياً فإيران تنقل قدراتها لطرف ثالث يستخدمها لضرب مصالح إسرائيلية وغربية، وهذا تقويض لواجبها في عدم السماح باستخدام مقدراتها لشن هجمات ضد دول أخرى. هو استخدام قوة بالوكالة، والقانون الدولي يحمل الدولة المسؤولية عن أعمال وكلائها إذا كان لهم ارتباط سيطرة، والتنسيق عالي المستوى يجعل المسؤولية مشتركة.[79]

2.9.3. سوريا

وتعتبر إيران حليفة للنظام السوري السابق، بل وتقاتل معه ضد جماعات معارضة مدعومة خارجياً. فلقد قدّمت خبرتها السيبرانية للنظام السوري الذي أسس جيشاً إلكترونياً مارس اختراقات ضد معارضي الأسد.[80] ويُعتقد أنّ إيران زودت الاستخبارات السورية ببرمجيات مراقبة لالتقاط اتصالات الناشطين،

71 Veena Ali-Khan, *Down but Not Out: Reassessing the Axis of Resistance*, THE CENTURY FOUND. (Mar. 19, 2025), https://tcf.org/content/report/down-but-not-out-reassessing-the-axis-of-resistance/.

انظر أيضاً: رسول آل حائي، استراتيجية محور المقاومة بعد التهدئة: استخلاص الدروس وإعادة البناء، شبكة الجزيرة، متوفر على الرابط:
https://www.aljazeera.net/politics/2025/1/25/%D8%A5%D8%B3%D8%AA%D8%B1%D8%A7%D8%AA%D9%8A%D8%AC%D9%8A%D8%A9-%D9%85%D8%AD%D9%88%D8%B1-%D8%A7%D9%84%D9%85%D9%82%D8%A7%D9%88%D9%85%D8%A9-%D8%A8%D8%B9%D8%AF-%D8%A7%D9%84%D8%AA%D9%87%D8%AF%D8%A6%D8%A9.

72 Amr Yossef, *Upgrading Iran's Military Doctrine: An Offensive "Forward Defense"*, MIDDLE EAST INST. (2019), https://www.mei.edu/publications/upgrading-irans-military-doctrine-offensive-forward-defense.

73 *Iran FM Reaffirms Commitment to Support Resistance against Israel*, TEHRAN TIMES (Sept. 17, 2024), https://www.tehrantimes.com/news/503822/Iran-FM-reaffirms-commitment-to-support-Resistance-against-Israel.

74 Simon Handler, *The Cyber Strategy and Operations of Hamas: Green Flags and Green Hats*, ATL. COUNCIL 13, 13 (2022).

75 Microsoft, Iran Surges, *supra* note 70.

76 Michael N. Schmitt & Sean Watts, *Beyond State-Centrism: International Law and Non-State Actors in Cyberspace*, 21 J. CONFLICT & SEC. L. 595, 596 (2017).
انظر أيضاً: سارة العنبورية، مرجع سابق، ص 130.

77 Matthew Levitt, *Hezbollah's Regional Activities in Support of Iran's Proxy Networks*, MIDDLE EAST INST. 2, 2 (2021).

78 Ioan Pop & Mitchell D. Silber, *Iran and Hezbollah's Pre-Operational Modus Operandi in the West*, 44 STUD. CONFLICT & TERRORISM 156, 156 (2021).

79 Michael Schmitt & Liis Vihul, *Proxy Wars in Cyberspace: The Evolving International Law of Attribution*, 1 FLETCHER SEC. REV. 55, 14 (2014) [hereinafter Schmitt & Vihul, Proxy Wars].

80 Edwin Grohe, *The Cyber Dimensions of the Syrian Civil War: Implications for Future Conflict*, 34 COMPAR. STRATEGY 133, 142 (2015).

كما استخدمت محور المقاومة السيبراني لإحباط عمليات استخبارية غربية.[81] والقانون هنا أوضح، فالنظام السوري حكومة شرعية تستطيع دعوة إيران لمساعدتها، وقد دعتها عسكرياً بالفعل. لذا فالمساعدة السيبرانية الإيرانية لسوريا يمكن اعتبارها شرعية كونها تمت بموافقة حكومة ذات سيادة، خلافاً لدعم إيران لوكلاء غير دول. لذا فحالة سوريا مختلفة، إذ يمكن تكييف الدعم السيبراني الإيراني كدعم بطلب سيادي، وبالتالي غير مخالف للقانون الدولي بحد ذاته، وقد تجادل إيران بذلك لو طُرحت المسألة.

بيد أنّ على هذا التكييف تحفّظاً جوهرياً. فالرضا السيادي حتى مع التسليم بصدوره عن حكومةٍ تبسط سيطرةً فعليةً على الإقليم، لا يَنفي عدم المشروعية إلا في حدود ما تملك الدولةُ المُعطية أن تأذن به (المادة (20) من مشروع مسؤولية الدول 2001). ودمشق لا تملك أن تأذن بفعلٍ يمسّ حقوق دولٍ ثالثة، إذ ليست تلك الحقوق ممّا تختصّ بالتنازل عنه. ومن ثَمَّ فاستخدام الأراضي السورية منصّةً للإضرار بمصالح دولٍ ثالثة يُخرج النشاط من نطاق المساعدة المشروعة، إلى انتهاكٍ مستقلٍّ لسيادة تلك الدول، والتزام العناية الواجبة بعدم السماح باستخدام الإقليم إضراراً بالغير، بصرف النظر عن موافقة دمشق. وإذا أُريد الطعن في صحّة الرضا ذاته فذلك يتوقّف على معيار الفعالية، لا على شرعية المنشأ، وهو سندٌ احتياطيٌّ متنازَعٌ فيه يُستغنى عنه متى قام التحفّظ الأول.

2.9.4. العراق

لإيران نفوذ كبير في بعض فصائل الحشد الشعبي العراقي، وكما زودتها بالسلاح، دربت أفراداً منها على حرب المعلومات، إذ ظهرت مجموعات قرصنة موالية لإيران مثل (المنتقمون السيبرانيون CyberAv3ngers)، وقد صعّدت من الهجمات السيبرانية الإيرانية بعد اغتيال سليماني، كما حصلت هجمات اختراق لمواقع حكومية عراقية نفذتها ميليشيات موالية لإيران للضغط السياسي.[82] القانون هنا معقد، لأن العراق دولة ذات سيادة، وأي عملية قرصنة داخلية إما إجرامية أو بأمر حكومة. إيران قد لا تكون متورطة مباشرة، لكن ولاءها للميليشيات يعني وجود شُبهةٍ قويةٍ بأنّها تشجّعها. إن ثبت أنّها تأمرها، فهو تدخل إيراني ضد سيادة العراق.[83] ما حصل فعلياً أنّ الحكومة العراقية غضت الطرف خوفاً من اصطدام داخلي، وبقي الدور الإيراني غير خاضع للمساءلة.

2.9.5. اليمن

دعم إيران للحوثيين يشمل أيضاً الجوانب التقنية، فيُعتقد أنّ خبراء إيرانيين ساعدوهم في استهداف الأنظمة الحكومية والعسكرية وفي جمع المعلومات الاستخباراتية ضد قوات التحالف، كما تعاونوا في نشر دعاية مضادة للسعودية عبر منصات التواصل. في الواقع لم تظهر حوادث كبرى سيبرانية للحوثيين لقلة خبرتهم، لكن إن حصلت فإيران ستكون في قفص الاتهام كشريك.[84] وهذا مشابه لتكييف حزب اللّه، دعم جماعة متمردة ضد حكومة ودول أخرى انتهاك خطير وهو أساس قرار مجلس الأمن الذي حظر تسليح الحوثيين، والسيبراني ليس استثناء لتزويد الحوثيين بأدوات قرصنة يُعدّ مساهمة في اعتداءاتهم.[85]

3. التداعيات القانونية والاستراتيجية والدولية للدور السيبراني الإيراني

يستعرض المبحث الثالث التداعيات الأوسع للأنشطة السيبرانية الإيرانية على المستويين الإقليمي والدولي، ومدى اتساق الخطاب الرسمي الإيراني مع قواعد القانون الدولي من وجهة نظر المجتمع الدولي، وكذلك استجابات خصومها مقارنة بمواقفها. سنبحث كيف أدّت سلوكيات إيران إلى تطور تدريجي في ردود الفعل القانونية الدولية، من قبيل بلورة الأعراف وإصدار بيانات المواقف، وكيف اضطرت أطراف مختلفة إلى تعديل استراتيجياتها السيبرانية نتيجة لذلك.

3.1. تناقض المواقف الإيرانية المُعلنة والممارسة العملية – الميزان القانوني الدولي

وفقاً لما ورد في المباحث السابقة، نلاحظ وجود فجوة واضحة بين مواقف إيران المُعلنة في المنتديات الدولية التي تؤكد احترامها للمبادئ القانونية من سيادة وعدم تدخل وغيرها، وتدعو لاستخدام سلمي للفضاء السيبراني وسلوكها السيبراني الإقليمي الفعلي الذي يشمل اختراقات وتخريب ودعم عمليات عدائية. وهذا التناقض لم يخفَ على المجتمع الدولي. في البداية، احتفت بعض الدول بإعلان إيران لعام 2020 واعتبرته مؤشراً إيجابياً على التزامها بالقانون الدولي.[86] لكن سرعان ما لوحظت انتهاكات إيران لنفس المعايير التي أعلنتها مثال: بعد أسابيع من إعلان احترام عدم التدخل، تدخلت إيران سيبرانياً في انتخابات الولايات المتحدة 2020 بإرسال رسائل تهديد جماعية للناخبين، وهو ما اعتُبر مخالفاً حتى لمعاييرها الذاتية.[87] هذا جعل الدول الغربية تشكك في نوايا إيران الحقيقية، إذ رأت أنّ بيانها قد لا يعدو كونه أداةً للعلاقات العامة لكسب الدعم السياسي والدبلوماسي، وليس التزاماً صادقاً.[88]

وإزاء ترسّخ هذه القناعة لدى عواصم القرار، بدأ خطاب دولي مضاد لمزاعم إيران القانونية يبرز تدريجياً. فعلى سبيل المثال، أثناء المناقشات الأممية في مجموعات الخبراء مفتوحة العضوية، أشارت دول غربية إلى ازدواجية بعض الدول التي تدعو للقانون الدولي علناً بينما تمارس هجمات سراً وكانت إيران ضمنياً من المعنيين.[89] وبالمثل، تبنّى حلفاء الولايات المتحدة، من بينهم إسرائيل والدول الأوروبية، نهجاً حذراً في الاستجابة لإعلان إيران، لم يرحبوا به بحماس، بل أصدروا بياناتهم الخاصة التي قدمت رؤية بديلة. إسرائيل في بيان نائب المستشار القانوني لوزارة الخارجية الدكتور روي شورندورف أواخر 2020 قدّمت منظوراً حذراً وبديلاً حول كيفية تطبيق القانون الدولي في الفضاء السيبراني، متجنبة الاعتراف الصريح بأنّ كل اختراق هو انتهاك للسيادة،

81 Michael Eisenstadt, *Iran's Lengthening Cyber Shadow*, WASH. INST. 7, 7 (2016), https://www.washingtoninstitute.org/policy-analysis/irans-lengthening-cyber-shadow.

82 Ranj Alaaldin, *The Popular Mobilization Force Is Turning Iraq into an Iranian Client State* (Feb. 2, 2024), https://policycommons.net/artifacts/11371460/the-popular-mobilization-force-is-turning-iraq-into-an-iranian-client-state/12260780/.

83 Moynihan, *supra* note 9, at 16.

84 Seth G. Jones et al., *The Iranian and Houthi War against Saudi Arabia*, CTR. FOR STRATEGIC & INT'L STUD. (2021), https://www.csis.org/analysis/iranian-and-houthi-war-against-saudi-arabia.

85 Schmitt & Vihul, Proxy Wars, *supra* note 79, at 14, 19.

86 Roguski, *supra* note 35.

87 FBI, *Iranian Interference in 2020 U.S. Elections* (2020), https://www.fbi.gov/wanted/cyber/iranian-interference-in-2020-us-elections.

88 إبراهيم السيد رمضان، مرجع سابق، ص 1831.

89 Nanette S. Levinson, *Idea Entrepreneurs: The United Nations Open-Ended Working Group & Cybersecurity*, 45 TELECOMM. POL'Y 1, 1 (2021) [hereinafter Levinson, Idea Entrepreneurs].

ومؤكدة على عتبة عالية لاستخدام القوة.[90] ومن هذا المنطلق فُسر بيان إسرائيل كرد غير مباشر على بيان إيران وقدّم بديلاً إقليمياً له في تفسير القانون خاصة لدول الخليج وغيرها بمعنى أنّ النهج القانوني الإيراني ليس الوحيد.

وفي حين عبّرت الدول الكبرى عن مواقفها خطابياً، سلكت دول الخليج مساراً مغايراً. إذ لم تصدر بيانات رسمية مفصلة عن رفض السلوك الإيراني، فدول الخليج رغم ضعف قدراتها القانونية المستقلة في تقديم مواقف عامة، سعت عملياً لتوحيد جهودها مع القوى الكبرى لمواجهة إيران. ورحبت بالحضور التقني الأمريكي والأوروبي في المنطقة للتدريب والتأمين السيبراني، وانخرطت في مبادرات مثل "مبادرة الشرق الأوسط للأمن السيبراني" بالشراكة مع الولايات المتحدة.[91] ولقد فتح التقارب من بعض الدول الخليجية مع إسرائيل بعد التوقيع على اتفاقيات إبراهام عام 2020، الباب أيضاً لتعزيز التعاون السيبراني الدفاعي بينها ضد التهديدات الإيرانية.[92]

وإذا تجاوزنا المستوى الإقليمي إلى السياق الدولي الأوسع، فإنّ السلوكيات الإيرانية كشفت ثغرات في النظام، إذ لا توجد معاهدات ملزمة صريحة تنظم السلوك السيبراني، والأمر يعتمد على تكييف القواعد العامة. فما كان من إيران إلا استغلال هذه الثغرات من خلال المناورة الانتقائية: تلتزم متى وافق ذلك مصالحها فإدانة الاختراقات ضدها، وتتجاهل عندما تريد فإنكار تورطها في هجمات. ولقد دفع هذا السلوك عدة دول بما في ذلك دول أوروبية والصين وروسيا للدعوة لتطوير قواعد السلوك المسؤول للدول في الفضاء السيبراني.[93] كما أنّ منصات مثل الأمم المتحدة، عبر فريق الخبراء الحكومي وأعمال الجمعية العامة، أصبحت أيضاً نشطة لتعزيز الوعي والاتفاق حول تطبيق القانون الدولي. في هذه المناقشات، تبرز مواقف متعارضة: الغرب عموماً يركز على محاسبة دول مثل إيران وروسيا على الهجمات ويؤكد على مبادئ المسؤولية، بينما إيران ومعسكرها يدفعان نحو إطار فضفاض يسمح بمجال للمناورة ويؤكد على سيادة الدولة على فضائها بما يشمل الرقابة الداخلية. حتى الآن، يبقى التوافق صعباً، لكن الضغط الدولي على إيران ازداد، وتبنّت الجمعية العامة بدعم غربي قرارات تدين جرائم المعلومات، وأنشأت أيضاً فريق عمل مفتوح العضوية لمناقشة أمن المعلومات، تشارك فيه إيران لكن بفعالية محدودة.[94]

وتبلغ الفجوة بين الخطاب الإيراني المُعلَن والممارسة الفعلية حدّاً يُرتّب أثراً قانونياً لا سياسياً فحسب. فالدولة التي تُعلن قناعةً قانونيةً (opinio juris) في تفسير عتبتَي استخدام القوة والتدخّل، تُقيِّد بها في مقام الاحتجاج، إذ لا يستقيم أن تطالب غيرها بالتقيّد بتفسيرٍ ترفض هي الالتزام بمقتضاه، وهو ما يقترب في أثره من منطق الإغلاق (estoppel) وإن لم تكتمل شروطه التقنية من اعتمادٍ وضرر. ويضع هذا إيران أمام معضلةٍ مزدوجة: فإمّا أن تُؤخذ بتفسيرها المُعلَن فيخرج جزءٌ معتبرٌ من عملياتها عن نطاق المشروعية، وإمّا أن تتنصّل منه فتفقد رصيدها وحجتها أمام المجتمع الدولي. ومن ثَمَّ فالإعلان الإيراني (2020) لا يُقرأ التزاماً صادقاً بالقاعدة، بقدر ما يُقرأ موقفاً تفسيرياً انتقائياً يسعى إلى احتكار صفة الضحيّة في الفضاء السيبراني، دون تحمّل أعباء المشروعية.

3.2. المقارنة بين الاستراتيجية السيبرانية الإيرانية واستراتيجيات خصومها الإقليميين

من المفيد في ختام التحليل المقارن إبراز الاختلافات الجوهرية بين النهج السيبراني الإيراني ونهج خصومها الإقليميين البارزين، وخاصة إسرائيل ودول الخليج، سواء من ناحية الاستراتيجية أو المنظور القانوني:

إسرائيل: تمتلك قدرات سيبرانية متقدمة هجومية ودفاعية. تتبع نهجاً حذراً تجاه القانون الدولي، حيث لا تعلن عن هجماتها لكنّها تنفذها، كستاكسنت وهجمات الموانئ. استراتيجياً، تعتمد على الهجومية الدفاعية: ضربات محدودة استباقية أو انتقامية، مع تبنّي عقيدة الغموض الاستراتيجي المقصود لتعطيل قواعد الإسناد وإبقاء خيار الردّ مفتوحاً لدى الخصم دون نفي صريح أو إقرار، بالمقابل أصدرت أواخر 2020 بياناً رسمياً اعتُبر الأكثر تفصيلاً بعد بيان إيران، احتوى على تفسير محافظ للغاية للقانون: إسرائيل لم تؤكد صراحة وجود قاعدة سيادة ملزمة في الفضاء السيبراني، إذ تركت الأمر غامضاً مما يعني ضمناً أنّها لا تعتبر كل اختراق انتهاكاً.[95]

دول الخليج: قدراتها الهجومية أقل، وتركز على الدفاع والتحصين، مع تعزيز البنية التحتية السيبرانية الوطنية والتعاون مع حلفاء أقوى. تعتمد على الرد الدبلوماسي والقانوني أكثر من الهجوم المباشر، مع التنسيق تدريجياً مع إسرائيل والولايات المتحدة في التهديدات الإيرانية.

تلاقي المصالح: من المثير للاهتمام أنّ التهديد السيبراني الإيراني المشترك أدى إلى تلاقٍ غير مسبوق في المصالح بين إسرائيل ودول خليجية مثل الإمارات والبحرين. فبعد توقيع على اتفاقيات إبراهام في عام 2020، تحول التعاون الأمني السري إلى شراكات علنية، حيث مهدت الاتفاقيات الطريق لتعاون غير مسبوق في مجالات الأمن والاستخبارات والتكنولوجيا، والخليج فتح أسواقه للتكنولوجيا الإسرائيلية المتقدمة واستفاد منها.[96] من الجانب الآخر، إيران تقف وحدها تقريباً في المنطقة في تبنّي الهجمات السيبرانية الهجومية كأداة سياسة خارجية رئيسية. وبالتالي أصبحت إيران معزولة إقليمياً في هذا النهج، مما سهل على خصومها تصويرها كعنصر شاذ وخطير، وهو ما تفعله إسرائيل دبلوماسياً بنجاح نسبي، حاشدة الدعم بزعم التهديد السيبراني الإيراني للاستقرار الإقليمي.[97]

قانونياً، يبرز نموذجان متعارضان: النموذج الإيراني الذي يوسع نظرياً نطاق عدم الشرعية لكنّه يضيقه عملياً لنفسه، والنموذج الإسرائيلي الغربي الذي يضيق نظرياً نطاق عدم الشرعية لكنّه يسعى جوهريا لتشكيل قواعد عرفية تجرم سلوكيات مثل إيران.

ويلتقي النموذجان على تعارضهما الظاهر، لا في تماثل القدر الذي يبتعد به كلٌّ منهما عن القانون، بل في بنيتهما الحجية ذاتها: فصلُ الخطاب القانونيّ المُعلَن عن السلوك الفعليّ للدولة. فالنموذج الإيرانيّ يستثمر في توسيع القاعدة لتحصين بيئته الداخلية، وتجريم خصومه توسيعاً يقع خارج التفسير المعقول لقاعدة السيادة، والنموذج الإسرائيليّ الغربيّ يستثمر في تضييق العتبة لتحرير هامش عملياته، مع الاحتفاظ بحقّ الإدانة الخطابية وإن ظلّ تضييقه في حدوده الدنيا، داخل نطاقٍ تفسيريٍّ متنازَعٍ فيه. وما يسدّ الفجوة بينهما نموذجٌ ثالثٌ قوامه الاتّساق بين التفسير المُعلَن للقاعدة،

90 Roy Schöndorf, *Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations*, 97 INT'L L. STUD. 423, 423 (2021) [hereinafter Schöndorf].

91 Nima Khorrami, *Israel's Cybersecurity Cooperation with the GCC States*, MIDDLE EAST INST. 1, 1 (2021).

92 Marwa Fatafta, *Normalizing the Surveillance State—Cybersecurity Cooperation and the Abraham Accords*, MERIP (Sept. 27, 2023), https://merip.org/2023/09/normalizing-the-surveillance-state-cybersecurity-cooperation-and-the-abraham-accords/.

93 Duncan B. Hollis, *A Brief Primer on International Law and Cyberspace*, CARNEGIE ENDOWMENT FOR INT'L PEACE 1, 1 (2021).

94 Levinson, Idea Entrepreneurs, *supra* note 89, at 5.

95 Schöndorf, *supra* note 90, at 423.

96 Islam Alhalwany, *Israel Is Becoming a Cybersecurity Guarantor in the Middle East. Here's How.*, ATL. COUNCIL (Nov. 18, 2021), https://www.atlanticcouncil.org/blogs/menasource/israel-is-becoming-a-cybersecurity-guarantor-in-the-middle-east-heres-how/.

97 Monika Stachoń, *Iranian Cyber Capabilities as a Tool of Domestic and Foreign Policy*, 2 ZESZYTY NAUKOWE SGSP 267, 267 (2024).

والسلوك الفعليّ على نهج التفسير بحُسن النية المكرَّس في المادة (31) من اتفاقية فيينا لقانون المعاهدات، وهو ما تقترب منه دولٌ متوسّطةٌ حين تُفصح عن مواقفها الوطنية كفرنسا وهولندا، على تباينٍ بيّنٍ في مضمون موقفيهما.

وفي الموقف الخليجيّ تحديداً فالاكتفاء بالدفاع التقنيّ وتعزيز البنية التحتية دون بلورة موقفٍ قانونيٍّ مُعلَن، يترك التفسير المعياريّ للأفعال السيبرانية حكراً على الفاعلين الكبار. ومن هنا تَلزم بلورةُ موقفٍ خليجيٍّ مُفصِح إعلاناً موحّداً إن أمكن توافقه، أو حدّاً أدنى من المبادئ المشتركة تُصدره الدول منفردةً، مع تنسيقٍ في الجوهر يُرسّخ مصالح المنطقة، ويسدّ الفجوة بين موقفَي إيران وإسرائيل.

3.3. تطـور الأعـراف والسياسـات الدوليـة نتيجـة الأنشـطة السيبرانية الإيرانية

لقد كانت الأنشطة الإيرانية عمداً أو غير عمد من بين العوامل المحفزة لتطوير النقاشات العالمية حول القانون والسياسات السيبرانية. نلخص بعض هذه التأثيرات:

الدفع نحو الإعلانات الوطنية: بإطلاق إعلانها لعام 2020، دفعت إيران دولاً أخرى لتحذو حذوها حتى لا تترك لها السبق. إسرائيل أصدرت بياناً، فرنسا وهولندا وألمانيا وأخريات أصدرن مواقف قبل ذلك بقليل أو بعده، وبالتالي هناك الآن مجموعة محترمة من البيانات الرسمية حول تطبيق القانون الدولي في الفضاء السيبراني. هذه البيانات رغم تباينها ساهمت في تعزيز وضوح نسبي للمواقف وتضييق فجوة الخلاف، على سبيل المثال، الجميع تقريباً، بما في ذلك إيران وإسرائيل، يتفقون على انطباق حظر القوة وعدم شرعية التدخل، لكنّهم يختلفون في التفاصيل والعتبات. مجرد وجود هذه النقاشات العلنية خطوة نحو إرساء العرف لأن ما تقوله الدول عنصر من عناصر تكوين العرف الدولي.

وقد أدّت الهجمات الإيرانية الكبرى خاصة الهجوم على ألبانيا، إلى تعزيز غير مسبوق في التعاون الدولي ضد طهران. فعلى إثر الهجوم، أصدر حلف الناتو بياناً قوياً أدان فيه الأنشطة السيبرانية الخبيثة المنسوبة إلى إيران، مؤكداً أنّ الحلفاء يدعمون ألبانيا في تعزيز قدراتها للدفاع السيبراني لصد مثل هذه الهجمات مستقبلاً.[98] وعلى المستوى العملي، قدّمت الولايات المتحدة وحلفاء آخرون مساعدة فنية مباشرة للسلطات الألبانية، بينما قام الاتحاد الأوروبي بتفعيل "فريق الاستجابة السيبرانية السريع" لمساعدة تيرانا، ورغم ذلك، لم يقم الاتحاد الأوروبي بتفعيل نظام عقوباته السيبرانية رداً على هذا الهجوم تحديداً.[99] ولقد أثارت هذه الحادثة نقاشاً جاداً حول المادة الخامسة من ميثاق الناتو المتعلقة بالدفاع الجماعي، فرغم أنّ ألبانيا لم تطلب تفعيلها رسمياً، إلا أنّ الهجوم سلط الضوء على سياسة الناتو القائمة منذ 2014 بأنّ هجوماً سيبرانياً خطيراً يمكن أن يؤدي إلى تفعيل المادة الخامسة، مع الحفاظ على غموض استراتيجي مقصود حول العتبة الدقيقة لذلك، مما يشكل بحد ذاته رادعاً مهماً.[100]

ضغط لتدويل قواعد السلوك: رأت الدول المتضررة من إيران أنّه من الضروري ملء الفراغ القانوني بمعاهدات أو أعراف. فالولايات المتحدة وأوروبا تدفعان باتجاه معايير السلوك المسؤول المستوحاة من توصيات مجموعات الخبراء.[101] فعلى سبيل المثال، قاعدة عدم استهداف البنية التحتية المدنية الحيوية في زمن السلم هذه جاءت كتوصية في تقرير الأمم المتحدة 2015، لكن بعد حادثة ألبانيا، بدأت أمريكا وحلفاؤها يستشهدون بها كقاعدة ملزمة لتأكيد استعدادهم لفرض عواقب على المنتهكين، كما فعلوا مع إيران.[102]

إشراك فاعلين جدد: من بين التأثيرات أيضاً دخول القطاع الخاص والكيانات غير الحكومية كلاعبين في المناقشات. الكثير من الأدلة على هجمات إيران قدّمتها شركات الأمن السيبراني، كمايكروسوفت ومانديانت في حالة ألبانيا.[103] هذا خلق نموذج تعاون بين الدول والشركات في مواجهة وكشف الهجمات. بالمثل، مراكز البحث، كمركز الدراسات الاستراتيجية والدولية (CSIS)، بدأت توثق تاريخ الهجمات الإيرانية وتأثيرها، مكوّنة أرشيف معرفة يساعد المشرعين. على سبيل المثال، مركز ناتو السيبراني أنشأ منصة للحوادث السيبرانية ووثق حادثة ألبانيا كنموذج، مبرزاً جانبها القانوني. هذه التوثيقات تراكم خبرة قانونية ستكون مفيدة لأي محكمة دولية أو جهة تحقيق مستقبلية.[104]

الاقتراب من معاهدات دولية؟ على مستوى آخر، الفوضى الحالية دفعت دولاً كبرى للتفكير في أطر معاهدات. فلقد اقترحت روسيا منذ مدة معاهدة معلومات تركّز على مكافحة جرائم المعلومات، وهو مسار تدعمه إيران، بينما الأمريكيون وحلفاؤهم يفضلون الالتزام بالقانون الدولي الحالي دون معاهدة جديدة خوفاً من تقييد حريتهم.

ويتبيّن، في خاتمة المطاف أنّ تطوّر الأعراف السيبرانية في ضوء الأنشطة المنسوبة لإيران، يكشف عن مفارقةٍ في بنية تكوين العرف المعاصر: فمَوضِع التكوين لم يَعُد الفعل المخالف وحده، بل ردودُ الفعل عليه، وهي ردودٌ متى ضعُف اتّساقها أجهضت بلورة القاعدة بدلاً من ترسّيخها. وعلى خلاف ما قد يوحي به العرض الوصفيّ المتقدّم، فلم تبلغ ردود الفعل الدولية على حادثة ألبانيا عتبة الممارسة العامة المقبولة بمثابة القانون الذي تشترطه المادة 38(1)(ب) من النظام الأساسيّ لمحكمة العدل الدولية، وذلك لسببين متضافرين. أولهما أنّ إدانات الناتو والاتحاد الأوروبيّ بقيت سياسيةً خطابيةً، دون التحول لممارسةٍ جزائيةٍ متّسقة، بدليل أنّ الاتحاد لم يُفعّل نظام عقوباته السيبرانية ردّاً على الهجوم. وثانيهما أنّ هذه الإدانات خلَت من ادّعاءٍ قانونيٍّ صريحٍ بانتهاك التزامٍ دوليٍّ بعينه، فبقي العنصر المعنويّ (opinio juris) في دائرة الغموض. ومن ثَمَّ يظلّ الحديث عن بلورة أعرافٍ سيبرانية سابقاً لأوانه.

والأكثر فعالية لسدّ هذه الفجوة المعيارية أن يكون هناك مسارٌ متدرّجٌ، يبدأ بإعلاناتٍ وطنيةٍ وإقليميةٍ مُفصِحة تُراكم opinio juris صريحاً، تمهيداً لإطارٍ معاهديٍّ للسلوك السيبرانيّ يُحدّد عتبات الانتهاك بدقّة، وهو طريقٌ

98 NATO, *NATO Reaffirms Support for Albania Following Cyber Attacks*, https://www.nato.int/en/news-and-events/articles/news/2022/09/22/nato-reaffirms-support-for-albania-following-cyber-attacks (last visited 23 February 2026).

99 Gerta Zaimi, *Iran's Balkan Front: The Roots and Consequences of Iranian Cyberattacks against Albania*, MIDDLE EAST INST., https://www.mei.edu/publication/irans-balkan-front-roots-and-consequences-iranian-cyberattacks-against-albania/ (last visited 17 February 2026).

100 Michaela Prucková, *Cyber Attacks and Article 5—A Note on a Blurry but Consistent Position of NATO*, NATO COOP. CYBER DEF. CTR. OF EXCELLENCE, https://ccdcoe.org/library/publications/cyber-attacks-and-article-5-a-note-on-a-blurry-but-consistent-position-of-nato/ (last visited 2 February 2026).

101 Bart Hogeveen, *The U.N. Norms of Responsible State Behaviour in Cyberspace* 8, 8 (2022).

102 *2015 U.N. GGE Report: Major Players Recommending Norms of Behaviour, Highlighting Aspects of International Law*, NATO COOP. CYBER DEF. CTR. OF EXCELLENCE, https://ccdcoe.org/incyder-articles/2015-un-gge-report-major-players-recommending-norms-of-behaviour-highlighting-aspects-of-international-law/ (last visited 3 March 2026).

انظر أيضاً: غسان صبري كاطع البيضاني، "دور القانون الدولي الإنساني في التصدي للحرب السيبرانية"، **مجلة الميزان للدراسات الإسلامية والقانونية**، المجلد 10، العدد 1، مارس 2023، ص 46. سارة العنبورية، مرجع سابق، ص 110.

103 Microsoft Threat Intelligence, *Microsoft Investigates Iranian Attacks against the Albanian Government* (2022), https://www.microsoft.com/en-us/security/blog/2022/09/08/microsoft-investigates-iranian-attacks-against-the-albanian-government/ [hereinafter Microsoft, Albania Investigation].

104 Ctr. for Strategic & Int'l Stud., *Significant Cyber Incidents*, https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents (last visited 16 March 2026).

وعزّ تشهد على وعورته تعثّراتٌ مساري الأمم المتحدة القائمين، غير أنّ بطأه المنضبط أحرى من انتظار عرفٍ قد تُفرغه الانتهاكات المتكرّرة من مضمونه قبل أن يستقرّ.

3.4. المشهد المستقبلي – نحو تقنين عالمي للسلوك السيبراني

يعتقد العديد من المراقبين أنّه مع استمرار الضغط الدولي والهجمات السيبرانية البارزة المتكررة، نتجه نحو إطار دولي أكثر صرامة فيما يتعلق بالفضاء السيبراني.[105] فسلوكيات إيران ودول أخرى مثل روسيا وكوريا الشمالية عجلت هذا الاتجاه، لأنّها دقت أجراس الإنذار للقوى الكبرى بوجود حاجة لقواعد اشتباك واضحة. والسيناريو المحتمل في المستقبل القريب يشمل:

- تفاهمات ثنائية/إقليمية: قد نشهد اتفاقيات غير رسمية بين كتل دولية، كاتفاق ضمني بين الناتو وروسيا/الصين على عدم استهداف مرافق معينة. اقترحت كل من فرنسا وأمريكا بالفعل مبادرات للاستقرار السيبراني والنظام القائم على القواعد في الفضاء السيبراني، وإذا استمر الزخم، قد تتطور هذه إلى اتفاقيات إقليمية ملزمة، ثم تتوسع عالمياً.[106]
- تطوير مؤسسي: قد تتطور المؤسسات الدولية لتشمل آليات سيبرانية متخصصة: ربما محاكم سيبرانية تحت رعاية الأمم المتحدة، أو قوات حفظ سلام سيبرانية، أو حتى ناتو سيبراني للدفاع الجماعي. هذه ليست أفكاراً بعيدة المنال نظراً لسرعة التطور التكنولوجي وتصاعد الحوادث. تقنين القواعد العرفية بدون معاهدات رسمية، الممارسة المتكررة للدول في إدانة سلوكيات معينة، كما في حالة إيران، وفرض عواقب قد تؤدي لبلورة قواعد عرفية ملزمة.

ومن الممكن القول إنّ التجربة السيبرانية الإيرانية ساهمت في رفع الوعي الدولي حول مخاطر الفضاء السيبراني وضرورة تنظيمه، بما في ذلك منع استهداف البنية التحتية المدنية وتحميل الدولة المسؤولية عن أفعال وكلائها. حوادث مثل هجوم ألبانيا دفعت الدول المتضررة لتنسيق جهودها سياسياً ودبلوماسياً، ما قد يؤدي مستقبلاً إلى اتفاقيات دولية أو أعراف ملزمة تنظم السلوك السيبراني وتحدد عواقب الانتهاكات، ما يضطر دولاً مثل إيران لمواءمة سلوكها لتجنب تكاليف أكبر.

4. خاتمة

تكشف الدراسة أنّ الفضاء السيبراني لم يعد مجالاً تقنياً منفصلاً عن النظام القانوني الدولي، بل أصبح ساحة من ساحات التنافس الجيوسياسي التي تختبر قدرة قواعد القانون الدولي التقليدية على استيعاب أنماط جديدة من السلوك العدائي بين الدول. وفي هذا السياق فقد مثّل السلوك السيبراني الإيراني نموذجاً دالاً على كيفية توظيف القدرات الرقمية لتحقيق أغراض سياسية وأمنية تتجاوز الحدود الإقليمية، ولا سيما في بيئة الشرق الأوسط التي تتداخل فيها النزاعات المسلحة، وحروب الوكالة، والتنافس على النفوذ الإقليمي.

وقد بيّنت الدراسة أنّ القواعد العامة للقانون الدولي، وفي مقدمتها مبدأ المساواة في السيادة، وحظر التدخل في الشؤون الداخلية للدول، وحظر التهديد باستخدام القوة أو استخدامها، لا تفقد قابليتها للتطبيق لمجرد انتقال الفعل غير المشروع إلى البيئة السيبرانية. فميثاق الأمم المتحدة يقرر التزام الدول بالامتناع عن التهديد باستعمال القوة أو استعمالها ضد السلامة الإقليمية أو الاستقلال السياسي لأي دولة، كما يؤكد عدم جواز التدخل في المسائل الداخلة في الاختصاص الداخلي للدول.

ويعزز هذا الاتجاه ما استقر في تقارير الأمم المتحدة المعنية بسلوك الدول في استخدام تكنولوجيا المعلومات والاتصالات من تأكيد انطباق القانون الدولي، بما في ذلك ميثاق الأمم المتحدة على الفضاء السيبراني.

وقد خلصت الدراسة إلى أنّ الإشكالية القانونية في العمليات السيبرانية لا تكمن في غياب القانون كلياً، بل في صعوبة تكييف الفعل السيبراني، وإثبات نسبته إلى الدولة، وتحديد العتبة التي ينتقل عندها من مجرد عمل عدائي أو تدخلي إلى استخدام غير مشروع للقوة. وهذه الصعوبة لا ينبغي أن تتحول إلى ذريعة للإفلات من المسؤولية، لأن قواعد مسؤولية الدولة تقرر أنّ الدولة تُسأل عن أفعال أجهزتها، وعن أفعال الأشخاص أو الكيانات التي تعمل بناءً على تعليماتها أو تحت توجيهها أو سيطرتها.

4.1. النتائج

توصلت الدراسة إلى عدد من النتائج، لعل أهمها:

1) تبنّت إيران في المجال السيبراني استراتيجية غير متماثلة تستهدف تعويض القيود التي تواجهها في القوة التقليدية، وذلك من خلال استخدام أدوات رقمية منخفضة التكلفة نسبياً وعالية الأثر السياسي.

2) لم تكن العمليات السيبرانية المنسوبة إلى إيران مجرد حوادث تقنية متفرقة، بل بدت في كثير من الحالات جزءاً من تصور أوسع لإدارة الصراع الإقليمي عبر الضغط، والردع، وجمع المعلومات، وتعطيل الخصوم، والتأثير في بيئاتهم الداخلية.

3) يثير السلوك السيبراني الإيراني إشكالات قانونية متكررة تتصل بثلاث قواعد مركزية في القانون الدولي: السيادة، وعدم التدخل، وحظر استخدام القوة. فإذا استهدفت العملية السيبرانية بنية تحتية حكومية أو مدنية، أو أدّت إلى تعطيل خدمات عامة أساسية، أو ترتب عليها إتلاف واسع للبيانات أو الأنظمة، فإنّها لا تبقى في نطاق المنافسة السياسية المشروعة، بل قد تشكل فعلاً غير مشروع دولياً بحسب طبيعة الأثر، وجسامة الضرر، وصلته بوظائف الدولة المستهدفة.

4) تقدم حالة الهجوم السيبراني الإيراني على ألبانيا عام 2022 نموذجاً واضحاً لأهمية الإسناد القانوني والسياسي في المجال السيبراني. فقد أدانت منظمة حلف شمال الأطلسي الهجمات السيبرانية التي استهدفت البنية المعلوماتية الوطنية الألبانية، وأشارت ألبانيا وحلفائها في بياناتهم بالمسؤولية إلى حكومة إيران، واعتبرت تلك الأنشطة مصممة لزعزعة أمن دولة حليفة، وتعطيل الحياة اليومية للمواطنين، وتؤكد هذه الحالة أنّ الإسناد لم يعد مسألة تقنية محضة، بل أصبح عملية مركبة تتداخل فيها الأدلة الرقمية، والموقف السياسي، والقواعد القانونية الناظمة للمسؤولية الدولية.

5) أظهرت الهجمات من قبيل "شمعون" ضد شركة أرامكو السعودية عام 2012 خطورة انتقال الهجمات السيبرانية من مجال التجسس أو جمع المعلومات، إلى مجال التدمير وتعطيل المرافق الاقتصادية الحيوية. فقد أشارت مصادر متخصصة إلى أنّ الهجوم أدى إلى مسح بيانات عشرات الآلاف من أجهزة شركة أرامكو، ونُسب من قبل مصادر استخباراتية أمريكية إلى إيران، كما عُدّ مؤشراً على تنامي قدرات إيران السيبرانية، واستعدادها لاستخدامها في صراعات النفوذ الإقليمي، ورغم ذلك فالإسناد في مثل هذه الحالات قد يظل محل نقاش، رغم الأثر العملي للهجوم الذي يبرهن على أنّ الضرر السيبراني قد يبلغ مستوى يهدد الاستقرار الاقتصادي والأمني لدول المنطقة.

6) توظيف إيران لجماعات أو شبكات مرتبطة بها أو متعاطفة معها، لا يعفيها عند توافر شروط التوجيه أو السيطرة أو الدعم الفعال من المسؤولية الدولية. فالقانون الدولي لا يكتفي بالنظر إلى الفاعل المباشر،

105 Kubo Mačák, *From Cyber Norms to Cyber Rules: Re–Engaging States as Law–Makers*, 30 LEIDEN J. INT'L L. 877, 877 (2017).

106 Jeremy Julian Sarkin & Saba Sotoudehfar, *Artificial Intelligence and Arms Races in the Middle East: The Evolution of Technology and Its Implications for Regional and International Security*, DEF. & SEC. ANALYSIS 10, 10 (2024).

بل يبحث في علاقة هذا الفاعل بالدولة، ومدى خضوعه لتعليماتها أو سيطرتها أو استفادته من دعمها. وبذلك فنمط "الإنكار القابل للتصديق" الذي يميز بعض العمليات السيبرانية، لا يلغي المسؤولية متى أمكن إثبات الصلة القانونية بين الدولة والفعل.

7) استمرار الغموض في بعض قواعد القانون الدولي السيبراني لا يعني وجود فراغ قانوني كامل، وإنّما يعني وجود حاجة إلى مزيد من التحديد والتقنين. فالقواعد القائمة توفر أساساً كافياً لتقييم كثير من الأفعال السيبرانية، لكنّها تحتاج إلى تطوير معايير أكثر دقة بشأن عتبة استخدام القوة، وحماية البنى التحتية المدنية، وقواعد الإسناد، وواجبات العناية الواجبة، والتعاون في التحقيقات العابرة للحدود.

8) رغم أنّ السلوك السيبراني الإيراني حقق بعض المكاسب التكتيكية قصيرة المدى، إلا أنّه أسهم في المقابل في تعزيز التنسيق الدفاعي والسياسي بين خصومها الإقليميين والدوليين. أي أنّ الاستخدام المتكرر للأدوات السيبرانية الهجومية قد يؤدي على المدى البعيد إلى نتائج عكسية، تتمثل في زيادة عزلة إيران، وتوسيع نطاق العقوبات، وتعزيز قدرات الردع الجماعي ضد الدولة المنسوب إليها السلوك العدائي.

4.2. التوصيات

تطرح الدراسة عدداً من التوصيات، يمكن استعراضها على النحو التالي:

1) عمل المجتمع الدولي على بلورة اتفاق دولي خاص بالسلوك السيبراني للدول، أو على الأقل بروتوكول تفسيري ملحق بميثاق الأمم المتحدة، يحدد بصورة أوضح متى ترقى العملية السيبرانية إلى تدخل غير مشروع، أو استخدام للقوة، أو هجوم مسلح. ولا ينبغي أن يكون الهدف من هذا التقنين إنشاء قانون جديد بالكامل، بل توضيح كيفية تطبيق القواعد القائمة على الأفعال السيبرانية الحديثة.

2) تطوير معيار دولي أكثر انضباطاً للإسناد السيبراني، يجمع بين الأدلة التقنية، والسياق السياسي، ونمط السلوك السابق، ومؤشرات السيطرة أو التوجيه. فضعف الإسناد يظل أحد أهم أسباب الإفلات من المسؤولية في الفضاء السيبراني، ولذلك فوضع معايير إجرائية مشتركة للتحقيق وتبادل الأدلة من شأنه أن يعزز الثقة في الاتهامات الدولية، ويقلل من مخاطر التسييس.

3) تجريم الهجمات السيبرانية التي تستهدف البنى التحتية المدنية والخدمات العامة الأساسية، مثل الطاقة، والمياه، والصحة، والمصارف، والاتصالات، والأنظمة الحكومية الرقمية. وينبغي التعامل مع هذه القطاعات باعتبارها محلاً لحماية خاصة في زمن السلم كما في زمن النزاع، لأن تعطيلها قد يؤدي إلى أضرار إنسانية واقتصادية تتجاوز بكثير نطاق الفعل التقني ذاته.

4) إنشاء آلية إقليمية في منطقة الخليج والشرق الأوسط للإنذار المبكر وتبادل المعلومات بشأن التهديدات السيبرانية، على أن تجمع هذه الآلية بين البعدين التقني القانوني. فالاستجابة للهجمات السيبرانية لا تكتمل بتقوية الدفاعات الرقمية فقط، بل تتطلب أيضاً فرقاً قانونية قادرة على توثيق الضرر، وحفظ الأدلة، وبناء ملف قانوني صالح للاستخدام في المحافل الدولية.

5) اعتماد دول مجلس التعاون الخليجي مقاربة موحدة في التعامل مع التهديدات السيبرانية ذات الطابع الإقليمي، وربط استراتيجيات الأمن السيبراني الوطنية بالرؤى التنموية الخليجية، فالأمن السيبراني لم يعد قطاعاً فنياً مساعداً، بل أصبح شرطاً لازماً لحماية التحول الرقمي، والاقتصاد المعرفي، والخدمات الحكومية الذكية.

6) تفعيل مبدأ العناية الواجبة السيبرانية، بحيث تلتزم الدول بعدم السماح باستخدام إقليمها أو بنيتها الرقمية لشن عمليات تضر بدول أخرى، والتعاون بحسن نية في التحقيقات وطلبات المساعدة القانونية. ويكتسب هذا الالتزام أهمية خاصة في الحالات التي تعمل فيها جماعات غير حكومية، أو وكلاء رقميون من داخل إقليم دولة معينة أو عبر بنيتها المعلوماتية.

7) عدم الاكتفاء بالردود السياسية أو التقنية على الهجمات السيبرانية، وضرورة بناء مسار قانوني متكامل يشمل التوثيق، والإسناد، والاحتجاج الدبلوماسي، وطلب التعويض عند الاقتضاء، واللجوء إلى المنظمات الدولية المختصة. فالرد القانوني المنهجي لا يقل أهمية عن الرد التقني، لأنّه يحول الضرر السيبراني من واقعة عابرة إلى ملف مسؤولية دولية قابل للمساءلة.

4.3. الخلاصة

تؤكد تجربة إيران السيبرانية أنّ الفضاء الرقمي ليس منطقة خارجة عن حكم القانون، وأنّ الغموض النسبي في بعض القواعد لا يبرر تحويله إلى مجال للفوضى أو الإنكار أو تصفية الحسابات السياسية. وتؤكد الدراسة أنّ القانون الدولي يملك أدوات مهمة لمواجهة السلوك السيبراني العدائي، متى توافرت الإرادة السياسية، والأدلة التقنية، والصياغة القانونية المحكمة، ولكنّها بلا شك أدوات بحاجة إلى تطوير وتدقيق. ومن ثم فالتحدي الحقيقي لا يتمثل في السؤال عما إذا كان القانون الدولي ينطبق على الفضاء السيبراني أم لا؟ وإنّما في كيفية جعله أكثر فعالية في ردع الانتهاكات، وحماية البنى التحتية المدنية، وضمان عدم تحول الثورة الرقمية إلى وسيلة جديدة لتقويض سيادة الدول واستقرار النظام الدولي.

الإفصاح عن استخدام الذكاء الاصطناعي

يقر المؤلفان بأنّه تم استخدام برنامج (Deepl) للترجمة والتحرير اللغوي بهدف تحسين سهولة قراءة المقالة البحثية وأسلوبها اللغوي. وبعد استخدام هذا البرنامج، قاما بمراجعة المحتوى وتحريره حسب الحاجة. كما يتحمل المؤلفان المسؤولية الكاملة عن محتوى المقالة.

الإفصاح عن تضارب المصالح

يقر المؤلفان بعدم وجود أي تضارب مصالح نتيجة لعلاقات تنافسية أو تعاونية أو غيرها للإفصاح عنها.