الحرب بين التحالف الأمريكي الإسرائيلي وإيران: تحوّل الحرب في عصر الذكاء الاصطناعي والقانون الدولي

محمد إسماعيلوف*

* جامعة أنقرة للعلوم الاجتماعية، تركيا.

ملخص: مع اندلاع الحرب بين الولايات المتحدة و«إسرائيل» من جهة وإيران من جهة في 28 فبراير 2026، استُخدِمت الأدوات السيبرانية المدعومة بالذكاء الاصطناعي في ساحة الحرب بالتزامن مع الهجمات الحركية. يتناول هذا التحليل، من منظور نقدي، مدى تجاوز الهجمات السيبرانية المدعومة بالذكاء الاصطناعي المذكورة حظرَ استخدام القوة المنصوص عليه في المادة2(4) من ميثاق الأمم المتحدة، وعتبة الهجوم المسلح المنصوص عليها في المادة51، ويتناول كذلك مسألة الإحالة في سياق المسؤولية الدولية للدولة، وحدود حق الدفاع عن النفس في هذا الإطار.

الكلمات المفتاحية: الذكاء الاصطناعي، القانون الدولي، إيران، الولايات المتحدة.

The U.S./Israel-Iran War: The Transformation of Warfare in the Age of AI & International Law

MAMMAD ISMAYILOV*

ORCID NO: 0000-0003-1278-663X memmedismayil93@gmail.com

* Social Sciences University of Ankara, Türkiye.

ABSTRACT: *With the outbreak of the US/Israel-Iran war on February 28, 2026, artificial intelligence (AI)-enabled cyber tools were deployed in the theater of war simultaneously with kinetic attacks. This analysis examines whether these AI-enabled cyberattacks violated the prohibition on the use of force under Article 2(4) and the threshold for an armed attack under Article 51, the issue of attribution in the context of state international responsibility, and the limits of the right to self-defense within this framework.*

Keywords: *Artificial Intelligence, International Law, Iran, United States.*

رؤيـــة تركيـــة
2026-(2/15)
87 - 104

Received Date: 07 / 05 / 2026 • Accepted Date: 19 / 06 / 2026
This work has been prepared in accordance with ethical principles

DOI:10.36360/1560-015-002-006

مقدمة

يصف هيرودوت، الذي يروي تقدّم الفَرَس إلى شبه جزيرة أتيكا في عام 490 قبل الميلاد، الحادثة المثيرة للجدل التي تفيد بإرسال إشارة إلى الفرس من خلال رفع درع بعد المعركة. يُظهر هذا المثال أن الحرب لا تقتصر على التصادم العسكري أو الصراع الحركي فحسب؛ بل إن المعلومات والتواصل وإدارة التصورات تؤدّي دورًا مهمًّا حتى في المراحل المبكرة من الصراع،[1] وقد أُعِيد تمثيل هذا المنطق القديم بشكل رقمي في الساعات المظلمة من يوم 28 فبراير 2026.

أدلى رئيس أركان الجيش الأمريكي الجنرال دان كين في مؤتمر صحفي عُقِد في 2 مارس 2026 بالتصريحات الآتية بشأن المرحلة الأولى من الهجمات: كانت القيادة السيبرانية الأمريكية والقيادة الفضائية الأمريكية «أول من بادر» بالعملية،[2] وقد أدّت الهجمات السيبرانية التي نُفِّذت قبل وصول الذخائر العسكرية الحركية الأولى إلى الأهداف- إلى تعطيل شبكات الاتصالات وأجهزة الاستشعار الإيرانية؛ وشلّ عمل رادارات الإنذار المبكر؛ وتعطيل البنية التحتية للقيادة والتحكم. وخلال هذه العملية، انخفضت حركة الإنترنت في إيران إلى أقل من 4% من مستواها الطبيعي خلال الساعات الأولى من الهجمات.[3]

تُظهِر العمليات التي أطلقت عليها «إسرائيل» اسم «الغضب الأسطوري» و«زئير الأسد» الدقّة العالية التي وصلت إليها الأنظمة السيبرانية والاستخباراتية المدعومة بالذكاء الاصطناعي في ساحة الحرب الحديثة. إن اختزال عمليات تحليل البيانات، التي قد تستغرق شهورًا باستخدام الأساليب التقليدية، إلى ثوانٍ معدودة، وإجراء تحديد الأهداف من خلال بيانات متعددة الطبقات مثل المراقبة البيومترية وتحليلات الكثافة السكانية، يزيدان بشكل كبير من الفعالية العملياتية تجاه الأهداف العالية القيمة. ويُظهر هذا التطور، عند تقييمه جنبًا إلى جنب مع أنظمة الاستهداف المدعومة بالذكاء الاصطناعي مثل «The Gospel» و «Lavender» و«Where is Your Daddy؟» المستخدمة في هجمات «إسرائيل» على غزة، أن هذه التقنيات قد نضجت بشكل تدريجي.[4]

ومع ذلك، يبرز عنصران أساسيان يميزان التوتر الحالي عن الفترات السابقة: الأول هو أن استخدام الذكاء الاصطناعي لم يعد عنصرًا تشغيليًّا خفيًّا، بل أصبح يُعبّر عنه صراحةً كبار المسؤولين العسكريين الأمريكيين بوصفه جزءًا من العقيدة العسكرية.

والثاني هو النقاشات حول المسؤولية الأخلاقية والقانونية التي تثيرها هذه التقنيات. ففي التصريحات الصادرة عن القيادة المركزية الأمريكية CENTCOM التي تُقِرّ باستخدام الذكاء الاصطناعي في العمليات، يُنظر إلى التأكيد على أن «القرار النهائي يتخذه الإنسان» على أنه محاولة لتحقيق توازن قانوني وسياسي في مواجهة الخسائر المدنية المتزايدة والانتقادات الدولية المتعلقة بمنظومة مسؤولية الأنظمة المستقلة.[5]

وفي هذا السياق، فإن دمج الأنظمة المدعومة بالذكاء الاصطناعي في عمليات الاستخبارات وتحديد الأهداف لا يشير إلى تفوق تقني فقط، بل يشير أيضًا إلى تشكل نموذج حربي جديد قائم على التفاعل بين الإنسان والآلة. إن الجمع بين تحليل البيانات الضخمة والاستخبارات الإشارية وخوارزميات التعلم الآلي يسرع عمليات اتخاذ القرارات العملياتية، ويقلل من هامش الخطأ في تحديد الأهداف. لكن هذا الوضع يؤدي إلى أن تصبح الحدود الفاصلة بين الفعالية العسكرية والمسؤولية القانونية موضع جدل متزايد، ويثير مسألة قابلية تطبيق قواعد القانون الدولي على هذه التقنيات الجديدة.

يبحث هذا التحليل في الهجمات السيبرانية المدعومة بالذكاء الاصطناعي التي تشنها الولايات المتحدة و«إسرائيل» في إطار المعايير الأساسية للقانون الدولي. وفي هذا السياق، يتم أولاً تناول قابلية تطبيق القانون الدولي على الفضاء السيبراني ومن ثَمّ على تقنيات الذكاء الاصطناعي؛ ثم يجري تقييم حظر استخدام القوة، وعتبة الهجوم المسلح، والمسؤولية الدولية للدولة، وحق الدفاع عن النفس من خلال الأبعاد الملموسة للحرب.

تطبيق القانون الدولي على الفضاء السيبراني والذكاء الاصطناعي!

من أجل تقييم الهجمات السيبرانية المدعومة بالذكاء الاصطناعي التي نُفِّذت في سياق الحرب بين التحالف الأمريكي الإسرائيلي وإيران في إطار القانون الدولي، تلزم أولاً الإجابة عن السؤال المتعلق بإمكانية تطبيق المعايير الحالية للقانون الدولي على الفضاء السيبراني والذكاء الاصطناعي اللذين يُوصَفان بـ«المجالات الافتراضية»؛ هذا السؤال هو: هل يمكن تطبيق قواعد القانون الدولي الحالية عليها أم لا؟

يختلف الفضاء السيبراني والذكاء الاصطناعي بشكل كبير عن مجالات سيادة الدولة البرية والبحرية والجوية. والسمة الأساسية التي تميّز هذين المجالين عن غيرهما هي أنهما من صنع الإنسان.[6] والمتحقّق أن الفضاء السيبراني والذكاء الاصطناعي، بحكم طبيعتهما

الاصطناعية –على عكس البر والبحر والجو– لا يقتصران على حدود جيوسياسية أو طبيعية.[7]

في أدبيات العلاقات الدولية، غالبًا ما يُوصَف الفضاء السيبراني بأنه «المجال الخامس» بالإضافة إلى مجالات السيادة التقليدية مثل البر والبحر والجو والفضاء الخارجي.[8] في المقابل، لا يُعَدّ الذكاء الاصطناعي مجالاً مستقلاً؛ لأنه يمثّل بنية مرتبطة بالفضاء السيبراني ومعتمدة عليه إلى حد كبير. إذا عددنا الفضاء السيبراني أو الذكاء الاصطناعي مجالاً خامسًا مستقلاً، فقد يصبح من الصعب نظريًّا تطبيق قواعد القانون الدولي الحالية بشكل مباشر على الأنشطة في هذين المجالين. ولهذا السبب، لا يُنظَر إلى تصنيف الفضاء السيبراني والذكاء الاصطناعي بهذه الطريقة على أنه نهج صائب.

يكفي النظر إلى الخصائص الأساسية للأرض والبحر والجو والفضاء الخارجي للوصول إلى هذه النتيجة. فالفضاء السيبراني والذكاء الاصطناعي، على عكس المجالات الأربعة الأخرى، ليسا وسيلة يمكن للناس الحضور فيها جسديًّا أو ممارسة أنشطتهم فيها شخصيًّا؛ لأنه لا يمكن «الذهاب» إلى هذه المجالات جسديًّا. في المقابل، يمكن للإنسان السفر جسديًّا بين المجالات الأربعة الأخرى، والوجود فيها. وحتى لو تطلّب الأمر معدات خاصة، فإن الذهاب إلى أعماق البحار أو الفضاء الخارجي أمر ممكن ماديًّا. وفي هذا السياق، يمكن على سبيل المثال لغواصة أن تطلق صاروخًا من تحت سطح البحر لاستهداف هدف على اليابسة أو في البحر أو الجو أو الفضاء. في حين أن إطلاق صاروخ مباشرة من تحت سطح البحر لاستهداف عنصر موجود في الفضاء السيبراني أو بيئة الذكاء الاصطناعي أمر مستحيل تقنيًّا.[9]

ومن ثَمّ، فإن الفضاء السيبراني والذكاء الاصطناعي هما أداة تُستخدَم للتأثير في الكائنات الموجودة في المجالات الأربعة الأخرى، بدلاً من كونهما مجالين مستقلين. تؤدي الأنشطة السيبرانية أو أنشطة الذكاء الاصطناعي في نهاية المطاف إلى نتائج ملموسة على الأرض وفي البحر والجو والفضاء الخارجي، ولهذا السبب تخضع لقواعد القانون الدولي المتعلقة بهذه المجالات. ومن هذا المنطلق، فإن التشكيك في قابلية تطبيق القانون الدولي بسبب الطبيعة الافتراضية للفضاء السيبراني والذكاء الاصطناعي أمر لا مسوّغ له.[10]

وإنّ الوثائق الأساسية للقانون الدولي، مثل ميثاق الأمم المتحدة عام 1945، على

الرغم من أنها وُضِعت قبل اختراع الفضاء السيبراني والذكاء الاصطناعي، فقد صُمِّمت بهدف تنظيم أنشطة الدول بشكل عام، لا تنظيم أنشطة الدول في تلك الفترة فقط. ولا توجد أي قيود تمنع تطبيق الوثائق الحالية على أنشطة الفضاء السيبراني والذكاء الاصطناعي. وفي هذا السياق، لا يمكن الادّعاء بأن ميثاق الأمم المتحدة واتفاقيات جنيف عام 1949 ومشروع مواد «المسؤولية الدولية للدولة عن الأفعال غير المشروعة» عام 2001 لا يمكن تطبيقها على البعد السيبراني للعمليات الحالية لمجرد أنها صيغت قبل العصر السيبراني.

> **أصبح من الضروري التركيز على النتيجة الإستراتيجية الناتجة، لا على الأداة المستخدمة فقط، لتحديد الوضع القانوني للهجمات السيبرانية المدعومة بالذكاء الاصطناعي**

وفي هذا الإطار، من الواضح أن قواعد القانون الدولي الحالية يمكن تطبيقها على الهجمات السيبرانية المدعومة بالذكاء الاصطناعي التي نُفِّذت في الحرب بين الولايات المتحدة و«إسرائيل»، وإيران. وبالفعل، فإن موقف المجتمع الدولي يتّجه في هذا الاتجاه: إذ أكد فريق الخبراء الحكوميين التابع للأمم المتحدة (GGE) في تقريريه عامي 2013 و2015 أن المعايير، مثل السيادة وحظر استخدام القوة وعدم التدخل في الشؤون الداخلية، تنطبق على الفضاء السيبراني أيضًا.

حظر استخدام القوة

تحظر المادة 2(4) من ميثاق الأمم المتحدة، التي تشكل حجر الزاوية في القانون الدولي، بشكل قاطع تهديد الدول باستخدام القوة واستخدامها في علاقاتها الدولية على النحو الآتي:

«تمتنع جميع الدول الأعضاء، في علاقاتها الدولية، عن التهديد باستخدام القوة أو استخدامها، سواء ضد سلامة أراضي أي دولة أخرى، أم استقلالها السياسي، أم بأي شكل آخر لا يتوافق مع أهداف الأمم المتحدة».[11]

هذه الأحكام ليست مجرد قاعدة تعاقدية، بل هي في الوقت نفسه معيار ذو طابع jus cogens (قاعدة ملزمة) يربط جميع الدول. ومع ذلك، فإن التدخلات العسكرية الحديثة المستخدمة في الحرب بين التحالف الأمريكي الإسرائيلي وإيران تفتح الباب للنقاش حول كيفية قيام العناصر السيبرانية والأنظمة المدعومة بالذكاء الاصطناعي بتغيير عتبة استخدام القوة التقليدية. على الرغم من أن مفهوم «القوة» يُربَط تقليديّا بـ«القوة

المسلحة» بما يتوافق مع روح عام 1945، فإن قدرة الهجمات السيبرانية على شلّ دولة ذات سيادة دون انفجار رصاصة مادية تهزّ هذا التفسير الضيّق. لكي تشكل الهجمة السيبرانية استخدامًا للقوة، يُتوقَّع أن تسفر عن نتائج قابلة للمقارنة مع هجوم مادي من حيث نطاق العمل وتأثيراته، وفقًا لمبدأ «التكافؤ الحركي» المنصوص عليه في القاعدة 11 من دليل تالين، يُتوقّع أن تؤدي إلى نتائج قابلة للمقارنة مع هجوم مادي من حيث حجم العمل وتأثيراته. وفي هذا السياق، أصبح من الضروري التركيز على النتيجة الإستراتيجية الناتجة، لا على الأداة المستخدمة فقط، لتحديد الوضع القانوني للهجمات السيبرانية المدعومة بالذكاء الاصطناعي.[12]

تشكل «عملية التعمية»، وهي المرحلة الأولى من الهجمات التي شنتها الولايات المتحدة و«إسرائيل» التي شنتها الولايات المتحدة و«إسرائيل» ضد إيران، والتي تمثل المرحلة الأولى من «عملية التعمية»- تشكل الأساس الأكثر واقعية لهذا النقاش القانوني. إن قيام القيادة السيبرانية الأمريكية بتعطيل رادارات الإنذار المبكر وشبكات الاتصالات وأنظمة الاستشعار الإيرانية، قد يبدو للوهلة الأولى بمثابة عطل «مؤقت وقابل للإصلاح»، إلا أن النتائج الوظيفية التي تسببها هذه الأفعال ذات أهمية حيوية. تميل المناهج التقليدية إلى إبقاء التشويش على الترددات أو الاختراقات السيبرانية التي لا تسبب أضرارًا مادية دائمة تحت عتبة المادة 2(4)؛ لأنه لا يوجد مبنى مهدّم أو أرواح مفقودة. لكن هذا النهج السطحي يتجاهل الهدف الحقيقي للتدخل السيبراني المدعوم بالذكاء الاصطناعي، وهو تجريد الدولة الضحية من قدرتها الدفاعية تمامًا.[13] إذ أدى تجريد إيران من قدرتها على التنسيق إلى ضرب آلاف الأهداف وإضعاف القيادة الإستراتيجية، أي تمهيد الطريق لـ«الاستئصال الإستراتيجي». ومن ثَمّ فإن تقييم الهجوم السيبراني المدعوم بالذكاء الاصطناعي ليس بوصفه عطلاً منفصلاً ومستقلاً عن الهجوم الحركي، بل بوصفه خطوة تمهيدية ومكمّلة لا تنفصل عن العملية العسكرية الشاملة- هو مطلب من متطلبات الواقع القانوني.[14]

إن النظريات التقليدية المستخدمة في تحديد الطابع القانوني للهجمات السيبرانية المدعومة بالذكاء الاصطناعي تصبح غير كافية، وتفقد صلاحيتها في مواجهة عمليات متعددة المستويات ومتطورة، مثل «الغضب الملحمي». وفي هذا الإطار، فإن النهج القائم على الأدوات (instrument-based approach) ينطوي على خطر إقصاء التدخلات البرمجية المكونة من أكواد رقمية من نطاق التقييم القانوني؛ لأن هذا النهج

يحصر تفكيره في الطبيعة الحركية للأسلحة التقليدية فقط. في حين أن العنصر الذي يرفع أداة ما إلى مستوى «سلاح» هو الهدف الإستراتيجي الذي تستهدفه، والتأثير المدمّر الذي تكتسبه في يد الفاعل، لا هيكلها المعدني.[15]

وعلى الجانب الآخر من العملية، فإن النهج القائم على الهدف (target-based approach) يُظهر ردّ فعل «مفرط في شموليته» باعتباره أن أدنى تلامس إلكتروني مع البنى التحتية الحيوية الوطنية يُعَدّ استخدامًا للقوة؛ وهذا يخلق مناخًا خطيرًا من عدم اليقين قد يحوّل حتى أبسط نشاط استخباراتي إلى ذريعة للحرب.[16]

أما «النهج القائم على التأثير والوظيفة»، وهو الملاذ الأكثر عقلانية بين هذين القطبين، فيركز على مدى شلّ حقوق سيادة الدولة وقدرتها على المقاومة العسكرية، بدلاً من التركيز على الجوانب التقنية للتدخل السيبراني المدعوم بالذكاء الاصطناعي. وإذا وصلت هجمة إلكترونية مدعومة بالذكاء الاصطناعي إلى كثافة تشلّ حتى ردّ الفعل الدفاعي المشروع، وهو الحق الأساسي للدولة المستهدفة، فإن هذا العمل يُعَدّ استخدامًا للقوة بلا جدال، سواء كانت الأداة المستخدمة صاروخًا أم سطر برمجة.

أضاف استخدام أدوات الذكاء الاصطناعي في دور الاستهداف النشط في الهجمات التي شنتها الولايات المتحدة و«إسرائيل» ضد إيران طبقة جديدة من التعقيد إلى النقاشات المتعلقة بعتبة استخدام القوة. إن قيام الأنظمة الموجهة بالذكاء الاصطناعي بتحسين اختيار الأهداف وتحديد مسارات الهجوم بشكل مستقلّ يجعل من الصعب تحديد «لحظة بدء» استخدام القوة. إنّ آلاف عمليات الاختراق والتعطيل التي تنفّذها برمجيات مستقلّة في غضون أجزاء من الثانية تشير إلى عملية أسرع وأكثر تدميرًا بكثير من أي هجوم يخضع للسيطرة البشرية. وفي هذه المرحلة، فإن تراجع الرقابة البشرية على قرارات الذكاء الاصطناعي لا يلغي المسؤولية الدولية للدول؛ بل على العكس، يتطلب ذلك تحميل الدول التي تستخدم هذه التقنيّات المسؤولية المباشرة عن النتائج التي ستترتب على هذه الأنظمة. تثبت الحرب بين الولايات المتحدة و«إسرائيل» من جهة وإيران من جهة أخرى أن الذكاء الاصطناعي ليس مجرد أداة للكفاءة، بل هو عامل أساسي يرفع حجم الهجوم وشدته إلى مستوى القوة بموجب المادة 2(4).

وكما هو معروف، فإن المادة 2(4) من ميثاق الأمم المتحدة تحظر بشكل قاطع التهديد باستخدام القوة أو استخدامها ضد الاستقلال السياسي للدول. وقد ركزت الهجمات

الحركية المدعومة بالذكاء الاصطناعي التي شنتها الولايات المتحدة و«إسرائيل» في 28 فبراير 2026 على تحييد المرشد الأعلى الإيراني آية الله علي خامنئي، وشكلت في هذا الصدّد استخدامًا صريحًا للقوة ضد استقلال إيران السياسي.

ونتيجة لذلك، فإن أدوات أو عمليات الذكاء الاصطناعي في حرب الولايات المتحدة و«إسرائيل» ضد إيران، متكاملة مع العمليات الحركية، وقد تبنتها الدولة علنًا؛ وقد وصلت إلى عتبة الضرر المادي مع وفاة خامنئي وغيره من كبار المسؤولين، وشكلت تدخلاً جسيمًا في استقلال إيران السياسي وسلامتها العسكرية، ومن ثَمّ أصبحت انتهاكًا مباشرًا لحظر استخدام القوة.

الهجوم المسلّح

يُعَدّ حقّ الدفاع عن النفس أحد أهمّ الاستثناءات في القانون الدولي، ولا ينشأ إلا عند وقوع «هجوم مسلّح» وفقًا للمادة 51 من ميثاق الأمم المتحدة. وقد وضعت محكمة العدل الدولية، في قرارها التاريخي في قضية نيكاراغوا، عتبة بين هذين المفهومين، مؤكّدة أن كلّ استخدام للقوة لا يشكل هجومًا مسلحًا، وأن الهجوم المسلح هو «أشد أشكال» استخدام القوة. وقد اعتمدت المحكمة معيار «الحجم والتأثير» للتمييز بينهما.[17] يقع البعد السيبراني والذكاء الاصطناعي لهجمات الولايات المتحدة و«إسرائيل» في قلب هذه المنطقة الرمادية القانونية بالذات. يزعم مصممو الهجوم أن التشويش الراديوي والتعطيلات السيبرانية لا تسبب أضرارًا دائمة في الأجهزة، ومن ثَمّ فهي «مؤقتة وقابلة للعكس»، وهو ما يجعل هذه الأعمال تقع تحت عتبة الهجوم المسلح. ومع ذلك، فإن ما يجعل أداة ما سلاحًا ليس طبيعتها المادية، بل الغرض من استخدامها والتأثير الملموس الذي تحدثه.[18] إذا كان التدخل السيبراني المدعوم بالذكاء الاصطناعي يسبّب دمارًا أو خسائر في الأرواح أو شللاً استراتيجيًّا يعادل تأثيرات هجوم حركي، فإن تقييم الرمز الرقمي المستخدم بنفس الوضع القانوني للصاروخ التقليدي يعد أمرًا ضروريًّا.

قد تبدو أنشطة «التعطيل السيبراني» التي نُفِّذت في إطار هجمات الولايات المتحدة و«إسرائيل»، عند النظر إليها بمعزل عن العمليات الحركية، كأنها لا تتجاوز عتبة «الهجوم المسلح». وحقًّا، فإن أعمال التشويش على الترددات اللاسلكية وقطع الإشارات، على الرغم من تقييمها تقليديًّا على أنها انتهاك للسيادة أو استخدام للقوة، نادرًا ما صُنِّفت على أنها هجوم مسلّح. ومع ذلك، فإن مبدأ «تكامل الأحداث» الذي أشارت إليه محكمة

الجنايات الدولية في قضية منصّات النفط، يثبت أن الهجوم السيبراني جزء لا يتجزأ من الهجوم الحركي.[19] وقد أدّى تدمير قدرات إيران الدفاعية والاتصالات إلى تمهيد الطريق لدمار واسع النطاق تلا ذلك، وأسفر عن ضرب أكثر من 1000 هدف. وفي هذا السياق، فإنّ النظر إلى الهجمات السيبرانية المدعومة بالذكاء الاصطناعي على أنها «أعطال تقنية» منفصلة ومستقلّة عن الهجوم الحركي سيشكل عمىً قانونيًّا. إن خفض سعة البنية التحتية للإنترنت في إيران إلى 4 في المئة وإبقاءها عند هذا المستوى مدة 27 يومًا، يخرج المسألة من كونها «عملاً مزعجًا» إلى مستوى هجوم منهجي يستهدف وجود الدولة.

تُعرّف المادة 3(ب)، فعل الهجوم في إطار واسع بحيث يشمل «استخدام أي سلاح ضد أراضي دولة ما». والرأي السائد في أدبيات القانون الدولي هو أن عبارة «أي سلاح» الواردة في هذه المادة لا تشمل الوسائل الحركية فحسب، بل تشمل أيضًا الوسائل السيبرانية التي تؤدي، من حيث نطاقها وتأثيرها، إلى دمار مادي أو شلل إستراتيجي.[20] وعند تقييم معيار «الوزن الكافي» المنصوص عليه في المادة 2 من القرار[21] في سياق هجمات الولايات المتحدة و«إسرائيل»، يتبين أن الأثر الإجمالي للهجمات المذكورة يفي بهذا الوزن بأكثر من اللازم. فهذه العملية، التي نُفِّذت بالتزامن مع الهجمات الحركية وأسفرت عن مقتل مسؤولين رفيعي المستوى، منهم المرشد الأعلى علي خامنئي، تتوافق مع أشد أشكال استخدام القوة المنصوص عليها في قضية نيكاراغوا. من ناحية أخرى، فإن عناصر الحرب النفسية التي شكّلت جزءًا من الهجمات، مثل الاستيلاء على التلفزيون الحكومي أو التلاعب بتطبيقات الصلاة، لا تشكّل في حدّ ذاتها هجمات مسلّحة، ولكن يجب قراءتها بوصفها عناصر تزيد من خطورة الهجوم في إطار النطاق العام للعملية وتأثيرها. والأمر الحاسم هنا ليس التدمير المادي فقط، بل كسر ردود فعل الدولة الدفاعية، والتصفية المنهجية لسلامة سيادتها باستخدام الذكاء الاصطناعي والأدوات السيبرانية.

إن إدراج أدوات الذكاء الاصطناعي في عملية الاستهداف يجعل تحديد عنصر «النية الخاصة» (animus aggressionis) في تصنيف الهجوم المسلح أكثر تعقيدًا. يبحث القانون الدولي عن إرادة واعية تهدف إلى إلحاق الضرر بدولة معينة حتى يمكن عدّ الفعل هجومًا مسلحًا.[22] في سيناريو تعمل فيه الأنظمة المستقلة المدعومة بالذكاء الاصطناعي على تحسين اختيار الأهداف وتوسيع نطاق الهجمات بشكل مستقل، من أين تأتي النية؟ لا يكفي «دليل تالين» والمعايير الحالية لوضع هذه الاستقلالية التكنولوجية في إطار

قانوني لـ«النية».[23] ومع ذلك، في سياق هجمات الولايات المتحدة و«إسرائيل»، أدّى اعتراف الجنرال كين علنًا بهذه الهجمات[24] ومشاركته الأهداف الإستراتيجية للعملية مع الرأي العام العالمي إلى إزالة الغموض حول النية. تثبت هذه الهجمات، التي تبنّاها كبار المسؤولين العسكريين في الولايات المتحدة، أن الذكاء الاصطناعي هو مجرّد أداة تقنية، وأن النية الإستراتيجية تعود إلى الإرادة السياسية للدولة. ومن ثَمّ، فإن استخدام الذكاء الاصطناعي لم يكتفِ بإخفاء المسؤولية فحسب، بل زاد من حساسية الهجوم وتدميره، وهذا جعله عنصرًا يسهّل استيفاء معيار «الوزن الكافي».

اكتسب الجدل حول كون الهجمات السيبرانية المدعومة بالذكاء الاصطناعي يشكل هجومًا مسلحًا أم لا بعدًا جديدًا في سياق هجمات الولايات المتحدة و«إسرائيل». إن النهج التقليدي المتمثل في فرضية «لا يوجد هجوم مسلح إذا لم يكن هناك ضرر مادي» أصبح غير كافٍ بشكل متزايد في مواجهة قدرة الذكاء الاصطناعي على شلّ دولة ما. لذلك، يمكن القول: إن الهجمات السيبرانية التي تسبّب «تأثيرًا مدمرًا»، بغضّ النظر عن طبيعة الهدف، يجب تقييمها في إطار «الهجوم المسلح» باعتبارها معادلة للقصف من حيث النتائج. في هذه المرحلة، من المهمّ توضيح مفهوم «التأثير المدمر».

تجب الإشارة أولاً إلى أنه لا يوجد تعريف ملزم ومقبول عمومًا للهجمات السيبرانية المدعومة بالذكاء الاصطناعي التي تسبّب «تأثيرًا مدمرًا».[25] ومع ذلك، توجد تعريفات متنوعة تسهم في إدراك المفهوم. على سبيل المثال، تُعرّف المبادرة الوطنية لمهن ودراسات الأمن السيبراني (NICCS) التأثير التدميري بأنه حدث يؤدي إلى انقطاع غير متوقع للعمليات أو الوظائف لفترة طويلة بشكل غير مقبول.[26] أما إستراتيجية ميشيغان للاستجابة للاضطرابات السيبرانية (Michigan Cyber Disruption Response Strategy) فتشرح هذا المفهوم على أنه حدث يؤدي إلى الإضرار بالوظائف والخدمات الحيوية في القطاعين العام والخاص، أو يحتمل أن يؤدي إلى ذلك، نتيجة انتهاك سرية أو سلامة أو إمكانية الوصول إلى المعلومات الإلكترونية أو أنظمة المعلومات أو الخدمات أو الشبكات؛ وهو حدث يمكن أن يهدّد الأمن العام، أو يزعزع ثقة الجمهور، أو يؤثر سلبًا في اقتصاد البلاد، أو يضعف أمن الدولة.[27] ووفقًا لنهج آخر، فإن التأثير المدمر يشير إلى الأعمال التي تؤدي إلى تعطيل تدفق المعلومات أو تشغيل أنظمة المعلومات دون التسبب في أضرار مادية أو إصابات.[28]

في هذا الإطار، تتمثل السمة الأساسية للهجمات السيبرانية المدعومة بالذكاء الاصطناعي التي تسبب تأثيرًا مدمرًا في أن الضرر الناجم عنها يكون ذا طابع تعطيلي. بعبارة أخرى، تؤدي هذه الهجمات إلى تعطل خدمات أو أنشطة أو وظائف معينة. وقد يتجلى هذا الوضع في أشكال مختلفة، مثل منع الوصول إلى أنظمة المعلومات الحيوية، أو انقطاع الاتصال بالإنترنت، أو عدم القدرة على الوصول إلى شبكات معينة، أو تعطل أنظمة التشغيل. علاوة على ذلك، لا تقتصر هذه الآثار على النتائج المباشرة فحسب، بل قد تؤدّي أيضًا إلى نتائج من الدرجة الثانية وحتى الثالثة.

إلى جانب ذلك، يجب أن تصل الآثار المسببة للتعطيل المذكورة إلى مستوى معين من الخطورة والجدية. إذ إنّ بعض الآثار المدمرة تؤدي إلى نتائج أشد بكثير مقارنة بغيرها. على سبيل المثال، يؤدي تعطيل مواقع الإنترنت التابعة للمؤسسات الحكومية الحيوية إلى نتائج أكثر خطورة بكثير مقارنة بإغلاق مواقع للتجارة الإلكترونية.

إن تداخل العناصر السيبرانية والكيميائية في هجمات الولايات المتحدة و«إسرائيل»

يفرض إعادة تقييم الطبيعة القانونية للأنشطة السيبرانية المدعومة بالذكاء الاصطناعي، التي تسبّب في تأثيرات مدمرة بشكل خاص. فحتى لو لم تسبّب هذه الهجمات أضرارًا مادية، فإنها، من خلال تعطيل البنية التحتية الحيوية، وزعزعة النظام العام بشكل خطير، وتعريض حياة البشر للخطر بشكل غير مباشر، قد تؤدي إلى آثار مشابهة لتلك التي تنتج عن الهجمات المسلحة التقليدية. ولذلك، فإن العامل الحاسم هو خطورة الأثر الناتج، لا طبيعة الوسيلة المستخدمة. وإذا تسبب هجوم إلكتروني مدعوم بالذكاء الاصطناعي في انقطاعات واسعة النطاق وعميقة وخطيرة، وأدّى إلى شلّ الوظائف الأساسية للدولة، فيجب في هذه الحالة الاعتراف بأن الفعل المعني قد تسبب في تأثير مدمر. وفي هذه الحالة، يكتسب النهج الذي يرى أنه يجب تقييم الفعل المعني على أنه هجوم مسلح من منظور القانون الدولي قوة أكبر. ويظهر هذا التفسير في الوقت نفسه أن القانون الدولي لا يمثل بنية ثابتة، بل بنية ديناميكية قادرة على التكيف مع التطورات التكنولوجية .

مسؤولية الدولة

تشير مسؤولية الدولة في القانون الدولي إلى العلاقة القانونية التي تنشأ عندما تلحق دولة ما ضررًا بشخص قانوني آخر بفعل غير قانوني. وقد حُدِّد الإطار الأساسي لهذه المسؤولية في وثيقة «المواد التمهيدية المتعلقة بمسؤولية الدولة الدولية الناشئة عن الأفعال غير المشروعة الدولية» الصادرة عام 2001. وبموجب المادة 2 من هذه الوثيقة، يتعين توفر شرطين أساسيين في آن واحد لكي يُحمّل الدولة المسؤولية: (1) أن يُنسب الفعل (سواء كان فعلاً إيجابيًّا أو إهمالاً) إلى الدولة وفقًا للقانون الدولي، (2) أن يشكّل هذا الفعل انتهاكًا لالتزام دولي من جانب الدولة.[29]

ولا يترك موقع الهياكل التي تشكل الخلفية التقنية للهجمات، مثل القيادة السيبرانية الأمريكية ووحدة 8200 الإسرائيلية، أيَّ مجال رمادي من منظور قانون المسؤولية الدولية. ووفقًا للمادة 4 من الوثيقة الصادرة عام 2001، يُعَدّ فعل أي شخص أو وحدة تمارس وظائف التشريع أو التنفيذ أو القضاء في دولة ما فعلاً لتلك الدولة.

والنقطة الحاسمة هنا هي: نظرًا لأن هذه الوحدات تُعرَّف رسميًّا في القانون الداخلي للدول المعنية بوصفها جهازًا حكوميًّا (de jure organ)، فإن كل تحركاتها في الفضاء السيبراني تُنسب مباشرة إلى شخصية الدولة. وفي هذا السياق، تحولت مسألة تحديد الجهة التي تشن الهجمات السيبرانية المدعومة بالذكاء الاصطناعي، على عكس الحالات

التي يظل فيها الجاني مجهولاً، إلى يقين قانوني «قابل للنسب» مع التدخل الصريح للمؤسسات الحكومية الرسمية. تُحمّل المادة 4 من الوثيقة الصادرة عام 2001 المسؤولية مباشرةً على الدولة في مثل هذه التدخلات المؤسسية دون الحاجة إلى اختبارات أكثر تعقيدًا مثل «السيطرة الفعلية».

حق الدفاع عن النفس

يخضع حق الدفاع عن النفس، المكفول بموجب المادة 51 من ميثاق الأمم المتحدة، يشهد تحولاً جذريًّا في ظل الطبيعة المجهولة والهجينة للذكاء الاصطناعي والفضاء السيبراني. تبرر الولايات المتحدة و«إسرائيل» عملياتهما العسكرية في إطار حقّ الدفاع عن النفس ضد تهديد أمني مرتبط بالهجمات المنهجية التي تواصل إيران شنها منذ فترة طويلة عبر جماعات وكيلة مثل حماس وحزب الله والحوثيين. وتستند هذه الحجة إلى معيار «التورط بشكل كبير» الذي حددته محكمة العدل الدولية في قضية نيكاراغوا.[30] تبرر حكومتا واشنطن وتل أبيب العملية الشاملة التي وقعت في عام 2026 في إطار حق الدفاع عن النفس، مدّعيتين أن الدعم الإستراتيجي واللوجستي الذي تقدمه طهران للجماعات الوكيلة مرتبط بالهجمات الموجهة ضدّ «إسرائيل». لكن هذا النهج مثير للجدل في أدبيات القانون الدولي. بالإضافة إلى ذلك، أدّى استخدام الهجمات السيبرانية المدعومة بالذكاء الاصطناعي –تمهيدًا لهذه العمليات الحركية– إلى إثارة نقاش قانوني جديد يتجاوز الحدود التقليدية للدفاع عن النفس.

تتمثل العتبة الأكثر أهمية في تقييم الهجمات السيبرانية المدعومة بالذكاء الاصطناعي في إطار الدفاع عن النفس في مدى توافق هذه الهجمات مع مبدأي: «الضرورة» و«التناسب». وقد سعت القيادة السيبرانية الأمريكية إلى تكوين درع حماية قانوني من خلال تعريف التدخلات السيبرانية على أنها «عناصر داعمة تقع تحت العتبة الحركية».[31] لكن الهجوم السيبراني المدعوم بالذكاء الاصطناعي الذي يشل الوظائف الأساسية للدولة، ويجعل شبكات القيادة والسيطرة العسكرية غير قادرة على العمل، ويقضي على القدرة الدفاعية، يمكن عدّه معادلاً للهجوم المسلح حتى لو لم يتسبب في دمار مادي. إن ضرب أكثر من 1000 هدف بعد تعطيل ردود الفعل الدفاعية الإيرانية بواسطة أدوات إلكترونية مدعومة بالذكاء الاصطناعي، يجعل من المستحيل إخضاع الهجمات الإلكترونية والكيماوية لاختبار التناسب بشكل مستقل عن بعضهما. ويشير هذا الوضع

إلى أن الهجمات السيبرانية المدعومة بالذكاء الاصطناعي يجب ألا تخضع للتحليل التناسبي بمفردها، بل من خلال النتائج الإستراتيجية التي تترتب عليها.

أحد الجوانب الأكثر لفتًا للانتباه في هجمات الولايات المتحدة و«إسرائيل» هو تحول البنى التحتية الرقمية المملوكة للقطاع الخاص إلى أهداف عسكرية. وحتى لو لم يكن هدف الهجوم السيبراني المدعوم بالذكاء الاصطناعي منشأة عسكرية مباشرة، فإن التدخلات التي تستهدف الأنظمة المدنية، مثل تعطيل شبكة مستشفيات ضخمة أو مركز بيانات عالمي مثل غوغل، يمكن تصنيفها على أنها هجوم مسلح بسبب الآثار المدمرة التي تسببها. إن كون الجزء الأكبر من البنية التحتية الوطنية الحيوية في الدول الحديثة في أيدي شركات خاصة، ينقل هذه المؤسسات إلى «خط الجبهة الرقمي».

تُظهر الحرب بين الولايات المتحدة و«إسرائيل» من جهة وإيران من جهة أخرى ضرورة إعادة تفسير حق الدفاع عن النفس وفقًا للواقع التكنولوجي للقرن الحادي والعشرين. ورغم أن الهجمات الإلكترونية المدعومة بالذكاء الاصطناعي أهدأ من الرصاص التقليدي، إلا أنها أكثر فعالية بكثير من حيث قدرتها على ترك أمة ما دون حماية. وإذا كان هجوم إلكتروني مدعوم بالذكاء الاصطناعي يمنع الحكومة من أداء مهامها الأساسية، ويجعل نشر القوات المسلحة مستحيلاً، فإن هذا الهجوم يُعَدّ هجومًا بالمعنى المقصود في المادة 51. لكن في هذه المرحلة، يجب على الدول أن تحرص على ألا تتجاوز الإستراتيجيات العدوانية التي تنفذها تحت مسمّى «الدفاع» مبدأ الضرورة. إن التصريحات العدوانية، مثل خطاب الرئيس الأمريكي دونالد ترامب بشأن «تفجير» البنية التحتية الإيرانية،[32] تنطوي على خطر التحول إلى تصعيد في استخدام القوة يهدد السلام الدولي بتجاوزه حدود حق الدفاع المشروع.

خاتمة

سُجِّلت الهجمات الأمريكية- الإسرائيلية التي بدأت في 28 فبراير 2026 بوصفها نقطة تحول تاريخية خضعت فيها المعايير الأساسية للقانون الدولي، مثل حظر استخدام القوة، وعتبة الهجوم المسلح، ومسؤولية الدولة، وحق الدفاع المشروع، لاختبار شامل للغاية. على الرغم من انتهاء المرحلة الساخنة من الحرب مع إعلان الهدنة في 7 أبريل 2026، إلا أن الحجم الذي وصلت إليه الهجمات السيبرانية والدور العميق الذي أدّاه الذكاء الاصطناعي خلال هذه العملية قد أظهرا بوضوح عدم كفاية النموذج القانوني الحالي.

تظهر الاستنتاجات الأساسية التي تُوصِّل إليها في ضوء جميع البيانات التي جرى تحليلها خلال الحرب، تُظهر أن الذكاء الاصطناعي والفضاء السيبراني لم يعودا مجرد مجال تقني، بل أصبحا في الوقت نفسه مجالاً لتطبيق القانون الدولي بشكل مباشر، وأنه من الضروري على وجه السرعة تدوين المناطق الرمادية في هذا المجال.

النتيجة الأساسية الأولى المستخلصة من هذا التحليل هي أن الهجمات السيبرانية المدعومة بالذكاء الاصطناعي التي تبنتها الولايات المتحدة رسميًّا قد وصلت فعليًّا إلى عتبة استخدام القوة بموجب المادة 2(4) من ميثاق الأمم المتحدة. إن تنفيذ التدخلات السيبرانية المدعومة بالذكاء الاصطناعي بشكل متكامل تمامًا مع العمليات الحركية يظهر أن هذه الأعمال ليست مجرد أعطال تقنية، بل هي هجوم مباشر على سيادة الدولة المستهدفة. ويُعَدّ تدمير البنية التحتية للإنترنت في إيران فعليًّا إلى الصفر تقريبًا وشل قدرتها الدفاعية خلال الحرب- الدليل الأكثر واقعية على أن الهجمات السيبرانية المدعومة بالذكاء الاصطناعي تحمل طابع الهجوم المسلح من حيث الحجم والتأثير. وقد أدى هذا الوضع إلى بدء حقبة تُعَدّ فيها الهجمات السيبرانية المدعومة بالذكاء الاصطناعي معادلة لأدوات الحرب التقليدية من حيث النتائج الإستراتيجية، حتى لو لم تسبب دمارًا ماديًّا.

ومن منظور مسؤولية الدولة ومسألة الإسناد، توفر الحرب بين التحالف الأمريكي الإسرائيلي وإيران أرضية أكثر وضوحًا، ولا جدال فيها مقارنة بالنزاعات السيبرانية السابقة. إذ أدى إعلان كل من الولايات المتحدة و«إسرائيل» مسؤوليتهما عن الهجمات على المستوى الرسمي إلى إزالة ستار «الإنكار المعقول» -وهو عنصر لا غنى عنه في الحروب السيبرانية التقليدية- بشكل كامل هذه المرة.

وعلى الرغم من كل هذه التحديات الناشئة والفجوات المعيارية التي ولّدها الفضاء السيبراني، فإن القانون الدولي الحالي ليس عاجزًا تمامًا أو صامتًا في مواجهة هذه الحقيقة الجديدة. بل على العكس، تتمتع الأعراف الراسخة والمبادئ الأساسية بمرونة وقدرة على الصمود عميقتي الجذور، بحيث يمكنهما ترويض الطبيعة الفوضوية للفضاء السيبراني والذكاء الاصطناعي من خلال القانون الدولي. في هذه العملية، يستمر القانون الدولي في الوجود بوصفه هيكلاً معياريًّا ديناميكيًّا لا يتراجع أمام التكنولوجيا، بل يتحول معها ليصبح الدرع الرقمي لحقوق السيادة.

الهوامش والمراجع:

1. Herodot, Herodot Tarihi, çev. Müntekim Ökmen, (Türkiye İş Bankası Kültür Yayınları, İstanbul: 2019), VI. 115, VI. 124.
2. Dan Caine, “Pentagon Press Briefing on Operation Epic Fury”, US CENTCOM, 2 Mart 2026, https://www.centcom.mil/Media/Press-Briefings, (Erişim tarihi: 6 Nisan 2026); Evan Grey, “The Iran Precedent: Operation Epic Fury and the Law of Armed Conflict in Space”, SatNews, 4 Mart 2026, https://satnews.com/2026/03/04/the-iran-precedent-operation-epic-fury-and-the-law-of-armed-conflict-in-space, (Erişim tarihi: 6 Nisan 2026).
3. “Iran-Israel Cyber War Dashboard”, SOCRadar, 28 Şubat 2026, https://socradar.io/iran-israil-cyber-conflict-dashboard, (Erişim tarihi: 6 Nisan 2026); “Threat Brief: March 2026 Escalation of Cyber Risk Related to Iran (Updated March 26)”, Palo Alto Networks Unit 42, 26 Mart 2026, https://unit42.paloaltonetworks.com/iranian-cyberattacks-2026, (Erişim tarihi: 6 Nisan 2026).
4. Erman Akıllı, “ABD/İsrail-İran Savaşında İkinci Haftanın Ardından YZ Bilançosu”, SETA, 18 Mart 2026, https://www.setav.org/abdisrail-iran-savasinda-ikinci-haftanin-ardindan-yz-bilancosu, (Erişim tarihi: 10 Nisan 2026).
5. Akıllı, “ABD/İsrail-İran Savaşında İkinci Haftanın Ardından YZ Bilançosu.”
6. Mammad Ismayilov, Siber Uzayda Yeni Devlet Dışı Aktörlerin Uluslararası Sorumluluğu: Atıf, Özen Yükümlülüğü ve Doğrudan Sorumluluk, (Yetkin Yayınları, Ankara: 2026), s. 35.
7. Nils Melzer, “Cyberwarfare and International Law”, UNIDIR Resources, (2011), s. 5, https://unidir.org/files/publication/pdfs/cyberwarfare-and-international-law-382.pdf, (Erişim tarihi: 6 Nisan 2026).
8. W. J. Lynn III, “Defending a New Domain: The Pentagon’s Cyberstrategy”, Foreign Affairs, Cilt: 89, Sayı: 5, (2010), s. 97-108.
9. Christian Czosseck ve Kenneth Geers, The Virtual Battlefield: Perspectives on Cyber Warfare, (IOS Press, Amsterdam: 2009), s. 132-142.
10. Ismayilov, Siber Uzayda Yeni Devlet Dışı Aktörlerin Uluslararası Sorumluluğu, s. 37.
11. “Birleşmiş Milletler Şartı”, BM, 26 Haziran 1945, https://www.un.org/en/about-us/un-charter/full-text, (Erişim tarihi: 8 Nisan 2026).
12. Michael N. Schmitt, “Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework”, Columbia Journal of Transnational Law, Sayı: 37, (1999), s. 890-895.
13. Michael N. Schmitt, “The Law of Cyber Warfare: Quo Vadis?”, Stanford Law & Policy Review, Sayı: 25, (2014), s. 280-285.
14. Francois Delerue, Cyber Operations and International Law, (Cambridge University Press, Cambridge: 2020), s. 294-298.

15. Schmitt, “Computer Network Attack and the Use of Force in International Law”, s. 890-915.
16. Russell Buchan ve Nicholas Tsagourias, Regulating Cyber Operations: State Responsibility and the Use of Force, (Edward Elgar Publishing, Cheltenham: 2020), s. 158-162.
17. Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Merits, Judgment, International Court of Justice Reports 1986, s. 14; 1986 I.C.J. 14 (27 Haziran 1986).
18. Karl Zemanek, “Armed Attack”, Max Planck Encyclopedia of Public International Law, Sayı: 1, (2012), s. 599.
19. Oil Platforms (Islamic Republic of Iran v. United States of America), Judgment of 6 November 2003, I.C.J. Reports 2003, s. 161, para. 64, https://www.icj-cij.org/en/case/90, (Erişim tarihi: 8 Nisan 2026).
20. UN General Assembly, Resolution 3314 (XXIX), Definition of Aggression, 14 December 1974, Article 3(b), https://digitallibrary.un.org/record/201407, (Erişim tarihi: 8 Nisan 2026).
21. UN General Assembly, Resolution 3314 (XXIX), Definition of Aggression, 14 December 1974, Article 2, https://digitallibrary.un.org/record/201407, (Erişim tarihi: 8 Nisan 2026).
22. Michael N. Schmitt, “Autonomous Weapon Systems and International Humanitarian Law: A Reply to the Critics”, Harvard National Security Journal, (2013).
23. Schmitt, “The Law of Cyber Warfare: Quo Vadis?”, s. 269-299.
24. Akıllı, “ABD/İsrail-İran Savaşında İkinci Haftanın Ardından YZ Bilançosu”.
25. David Sanger ve John Markoff, “Obama Outlines Coordinated Cyber-Security Plan”, The New York Times, 29 Mayıs 2009.
26. “Explore Terms: A Glossary of Common Cybersecurity Terminology”, National Initiative for Cybersecurity Careers and Studies (NICCS), 10 Şubat 2015, https://definedterm.com/a/download/document/11128, (Erişim tarihi: 23 Nisan 2026).
27. “State of Michigan Cyber Disruption Response Plan”, State of Michigan Executive Office, 12 Kasım 2023, https://www.michigan.gov/dtmb/-/media/Project/Websites/dtmb/Services/Cybersecurity/Cyber-Disruption-Response-Plan.pdf, (Erişim tarihi: 23 Nisan 2026).
28. Ido Kilovaty, “Virtual Violence - Disruptive Cyberspace Operations as ‘Attacks’ under International Humanitarian Law”, Michigan Telecommunications and Technology Law Review, Cilt: 23, Sayı: 1, (2016), s. 123-124.
29. Enver Bozkurt, Yasin Poyraz-Selcan Erdal, Devletler Hukuku, 11. Baskı, (Yetkin Yayınları, Ankara: 2021), s. 273.

30. Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Merits, Judgment, I.C.J. Reports 1986, p. 14, para. 195.

31. Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command, US Cyber Command, 23 Mart 2018, https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010, (Erişim tarihi: 8 Nisan 2026).

32. "Trump Warns a 'Whole Civilization will Die Tonight' if a Deal with Iran isn't Reached", PBS NewsHour, 7 Nisan 2026, https://www.pbs.org/newshour/amp/world/trump-warns-a-whole-civilization-will-die-tonight-if-a-deal-with-iran-isnt-reached, (Erişim tarihi: 21 Nisan 2026).