P-ISSN: 1680-9300
E-ISSN: 2790-2129
المجلد (26)، العدد (3)
ص.ص 32-39

الفضاء الالكتروني كأداة للنفوذ في السياسة الدولية: دراسة لحالة إيران و "إسرائيل"

زمن محمد جبار

رئاسة جامعة النهرين، بغداد، العراق.

المستخلص

أسفرت التطورات السريعة في التكنولوجيا الحديثة والاعتماد شبه الكامل من قبل معظم الدول على هذه التكنولوجيا عن إعادة تشكيل العلاقات الاقتصادية والسياسية والاجتماعية، وذلك بفضل الدور المركزي الذي تلعبه هذه التكنولوجيا في تسهيل الحركة والتواصل بين الدول، وتعزيز التعاون، والوصول إلى المعلومات الضرورية بسرعة، وزيادة كفاءة النشاط الاقتصادي الدولي إلى مستويات غير مسبوقة، يُعتبر الفضاء السيبراني البيئة التي تعيش فيها التكنولوجيا وتزدهر، فهو عالم فريد يختلف عن القواعد التقليدية للعالم الإنساني الذي نعرفه، وله قواعده الخاصة، فعلى سبيل المثال، في الطبيعة، القوة هي ضد الضعف، فكلما زادت قوة الفرد، قلّت نقاط ضعفه، وهذا ينطبق على عوالم الحيوان والنبات. أما في العالم السيبراني، فكلما تحسنت القدرات السيبرانية للدولة وتطورت حكومتها الرقمية، زادت نقاط ضعفها.

يعرض هذا التقدم التكنولوجي المحدث لعواقب وخيمة في حال استغلاله بشكل غير صحيح أو تحويله إلى أداة للصراع السياسي والعسكري بين الدول، وقد حدث هذا بالفعل على مدار العقدين الماضيين بين عدة دول، وخاصة بين إيران و"إسرائيل"، حيث يتصاعد الصراع بين هذين البلدين في الشرق الأوسط، إذ تعمل كل منهما على تطوير أدواتها السيبرانية الخاصة واستخدامها في صراعها ضد الأخرى.

الكلمات المفتاحية: الفضاء السيبراني، النفوذ الدولي، السياسة الدولية، إيران، "إسرائيل".

1. المقدمة

شهد النظام الدولي في العقود الأخيرة تحولات عميقة فرضتها الثورة الرقمية والتطور المتسارع في تكنولوجيا المعلومات والاتصالات، الأمر الذي أدى إلى إعادة تشكيل طبيعة العلاقات الدولية وأدوات القوة والنفوذ بين الدول. وفي هذا السياق، برز الفضاء السيبراني بوصفه أحد أهم المجالات الجديدة التي لم تعد تقتصر على بعدها التقني، بل أصبحت ساحة استراتيجية متكاملة تتقاطع فيها الأبعاد الأمنية والسياسية والاقتصادية والعسكرية، وتُمارس من خلالها الدول وغير الدول أنماطًا جديدة من الصراع والتأثير، وقد أسهمت خصائص الفضاء السيبراني، مثل اللامركزية، وصعوبة الإسناد، وتعدد الفاعلين، في تحويله إلى بيئة خصبة لإدارة الصراعات غير التقليدية.

حيث يمكن تحقيق أهداف استراتيجية بوسائل منخفضة التكلفة وذات تأثير واسع النطاق، هذا التحول جعل من الفضاء السيبراني عنصرًا مؤثرًا في إعادة تعريف مفاهيم القوة والردع والأمن القومي، بل وأصبح جزءًا لا يتجزأ من بنية النظام الدولي المعاصر، وفي هذا الإطار، يُعد الصراع الإيراني–"الإسرائيلي" من أبرز النماذج التي تعكس هذا التحول، إذ انتقل تدريجيًا من مواجهة عسكرية وأمنية تقليدية إلى صراع متعدد الأبعاد يشمل الفضاء السيبراني كجبهة موازية للصراع المباشر، فقد لجأ الطرفان إلى استخدام الهجمات السيبرانية والتجسس الرقمي والتخريب الإلكتروني كأدوات ضمن استراتيجياتها الأمنية.

ما جعل الفضاء السيبراني ساحة مواجهة دائمة تتداخل فيها العمليات العسكرية مع العمليات الرقمية، وكما يكتسب هذا الموضوع أهمية إضافية بالنظر إلى ارتباطه بتوازنات إقليمية ودولية أوسع، حيث لا يقتصر تأثير هذا الصراع على الطرفين فقط، بل يمتد ليشمل أطرافًا دولية كبرى ترتبط بشكل مباشر أو غير مباشر بمسار الأحداث، مما يعكس طبيعة الترابط المعقد في النظام الدولي الحالي. وبناءً على ذلك، تأتي هذه الدراسة لتحليل دور الفضاء السيبراني في إعادة تشكيل ديناميكيات الصراع الإيراني–"الإسرائيلي"، وفهم كيفية تحوله إلى أداة مركزية في إدارة النفوذ والصراع في

مجلة بحوث مستقبلية
المجلد 26، العدد 3 (2026).
أُستلم البحث في 21 نيسان 2026؛ قُبل في 5 تموز 2026
ورقة بحث منتظمة: نُشرت في 30 تموز 2026
البريد الإلكتروني للمؤلف المراسل: zaman.muhamad@nahrainuniv.edu.iq

DOI:10.61704/pr.657

السياسة الدولية المعاصرة.

2. منهجية الدراسة

1.2 أهمية الدراسة

تنبع أهمية الدراسة من كونها تتناول أحد أكثر الملفات حساسية في العلاقات الدولية المعاصرة، وهو توظيف الفضاء السيبراني في الصراعات الإقليمية، وبالأخص بين إيران و"إسرائيل"، كما تكمن أهميتها في تحليل الدور المتزايد للهجمات السيبرانية في إعادة تشكيل موازين القوة، وفهم كيفية تحول الفضاء الرقمي إلى أداة استراتيجية ذات تأثير مباشر على الأمن الإقليمي والدولي.

2.2 مشكلة الدراسة

تتمحور إشكالية الدراسة حول السؤال الرئيس الآتي:

كيف أسهم الفضاء السيبراني في إعادة تشكيل ديناميكيات الصراع الإيراني–"الإسرائيلي"، وما مدى تأثيره في تحويل هذا الصراع من مواجهة تقليدية إلى صراع متعدد الأبعاد؟

ويتفرع عن هذه الإشكالية عدد من التساؤلات المتعلقة بطبيعة القدرات السيبرانية لدى الطرفين، وآليات استخدامها، وحدود تأثيرها على مسار الصراع.

3.2 فرضية الدراسة

تنطلق الدراسة من فرضية مفادها أن الفضاء السيبراني أصبح عنصرًا أساسيًا في إدارة الصراع الإيراني–"الإسرائيلي"، وأن تصاعد القدرات السيبرانية لدى الطرفين أدى إلى تعميق الصراع وتحويله إلى مواجهة مركبة تتداخل فيها الأدوات العسكرية التقليدية مع الأدوات الرقمية.

4.2 منهج الدراسة

اعتمدت الدراسة على المنهج الوصفي–التحليلي في وصف طبيعة الصراع الإيراني–"الإسرائيلي" في الفضاء السيبراني، وتحليل أنماط الهجمات السيبرانية المتبادلة، إضافة إلى المنهج الاستقرائي في تتبع تطور هذا الصراع عبر مراحل زمنية مختلفة، بهدف الوصول إلى استنتاجات تفسيرية حول دوره في العلاقات الدولية.

5.2 هيكلية الدراسة

تتكون الدراسة من ثلاثة مطالب رئيسية، تناول المطلب الأول مفهوم الفضاء السيبراني والمفاهيم المقاربة له، بينما بحث المطلب الثاني الفضاء السيبراني كأداة للقوة والنفوذ في السياسة الدولية، في حين خصص المطلب الثالث لتحليل الصراع الإيراني–"الإسرائيلي" في الفضاء السيبراني من حيث التطور، والهيكل التنظيمي، والتصعيد العسكري والسيبراني، وصولًا إلى تداعياته الإقليمية والدولية.

3. المطلب الأول (مفهوم الفضاء السيبراني والمفاهيم المقاربة)

1.3 مفهوم الفضاء السيبراني

يعيش عالمنا اليوم في عصر من الابتكارات والاكتشافات التي تكاد تكون محصورة على الدول الكبرى والعظمى، نظرًا لكثرتها وتقنياتها المتطورة، وهذا ما منحها ميزة خاصة في تفاعلها مع الآخرين على جميع الأصعدة. فالعلم والمعرفة في عصرنا الحالي لم يعودا مجرد ترف فكري أو استهلاكي، بل هما قوة، إذ أن من يمتلك العلم والمعرفة يتمتع بالقوة التي تمنحه القدرة الفائقة على التأثير في القضايا العالمية كافة.

إن الشخص الذي يمتلك القوة المكتسبة من العلم والمعرفة سيسعى إلى تمييز مصالحه واهتماماته ويضعها في المقام الأول، فالمعرفة ليست مجرد ابتكار عالمي جديد، بل هي عناصر قوة لمن يمتلكها. والفضاء السيبراني يعد أحد مخرجات المعلوماتية التي يتفاعل بها المجتمع الدولي بكثافة من خلال التطبيقات التي تُستخدم في العلاقات بين الدول. لذا، فإن فهم مفهوم المعلوماتية يشكل مدخلًا أساسيًا لفهم التأثير الذي يحدثه الفضاء السيبراني في اتخاذ القرارات السياسية، سواء في مواجهة الخصوم أو في الشؤون الداخلي (ذيب وفارس، 2021، ص 150).

يشير مفهوم الفضاء السيبراني إلى أنه عالم افتراضي متصل بشبكة عالمية يعتمد على الكمبيوتر، أي يتم الوصول إليه عبر الكمبيوتر، هو عالم مصنّع ومتعدد الأبعاد، وفي الاستخدام اليومي، يشمل مصطلح الفضاء الرقمي شبكة الإنترنت، والقوائم البريدية الإلكترونية، ومجموعات ومنتديات النقاش، وغرف الدردشة، والبريد الإلكتروني، بالإضافة إلى شبكات التواصل الاجتماعي، كلما زادت رقعة استخدام مواقع التواصل الاجتماعي وتحسنت نوعيتها، اتسعت دائرة الاتصال بالفضاء السيبراني، وزاد اهتمام الأفراد والدول بالفرص المتاحة وكذلك المخاطر المحتملة التي قد يسببها هذا التوسع، ولهذا ارتفع الاهتمام بالفضاء السيبراني إلى مراتب متقدمة في أولويات واضعي السياسات العامة (حميد، 2014، ص 3).

بينما وصف جوزيف ناي الفضاء السيبراني بشكل بسيط بأنه "مجال تشغيلي محكم يستخدم المعلومات عبر الأنظمة المتصلة والبنية التحتية المرتبطة بها"، وصوره كعدة طبقات تشكل نظامًا هجينًا فريدًا بخصائص مادية ورقمية. وملخصها في طبقتين: الطبقة المادية، التي تخضع للقوانين الاقتصادية والسياسية وتخضع للسلطة القضائية، وتتكون من الأنظمة والبنية التحتية المادية للفضاء السيبراني. والطبقة المعلوماتية أو الافتراضية، وهي ساحة الإنترنت والبرمجيات والمعلومات، التي يمكن السيطرة عليها قضائيًا. لذا، يمكن تنفيذ هجمات من الطبقة الافتراضية ذات التكلفة المنخفضة ضد الطبقة المادية التي تمتلك موارد شحيحة ومكلفة من المواد الضرورية للتحكم في الاتصالات والمعلومات والأجهزة الحاسوبية والشبكات والبرمجيات ومهارات المستخدمين. وهذا يشمل الأجهزة المتصلة بالإنترنت، ولكن أيضًا تشمل الشبكات الخلوية الداخلية وتقنيات الاتصالات الفضائية (Nye, 2010, p. 3).

بانها مجموعة من أنظمة التحويل ذات الطابع المالي، تسهل عمليات التبادل المالي بين

DOI:10.61704/pr.657

أما الاتحاد الدولي للاتصالات "ITU " فقد عرف الفضاء السيبراني بأنه "المجال المادي والمعنوي الذي يتضمن تكاملاً متزايدًا لتكنولوجيا المعلومات والاتصالات مع الأشياء التي كانت تعمل دونها سابقًا، مثل السيارات والعبارات وأنظمة التحكم لشبكات الطاقة والنقل الضخمة، وإمدادات الكهرباء، وأنظمة النقل والخدمات العسكرية (Touré, 2011, p. 9).

يمكن القول إن الفضاء السيبراني أصبح أداة محورية في تعزيز القوة والتأثير في العلاقات الدولية في ظل التطور التكنولوجي المتسارع، كما يمثل في الوقت ذاته مجالًا حيويًا يتيح فرصًا واسعة للتفاعل، لكنه ينطوي على تحديات ومخاطر أمنية متزايدة.

2.3 المفاهيم المقاربة للفضاء الالكتروني

شهد مفهوم الأمن السيبراني نمواً ملحوظاً نتيجة للتقدم السريع في التكنولوجيا الحديثة، ومع انتهاء الحرب الباردة في أوائل التسعينيات، ظهرت مجموعة من المفاهيم المرتبطة به، التي تتداخل معه في المعنى وتختلف في بعض الجوانب.

1.2.3الفضاء السيبراني

هناك جانبين، الأول هو الواقع الافتراضي - بيئة مكانية إلكترونية ثلاثية الأبعاد يمكن للناس "دخولها" و"التنقل خلالها"، والتفاعل مع كل من الحاسوب والبشر الآخرين، من ناحية أخرى، يوجد عالم أقل تشويقًا، لكنه أكثر فائدة، وهو عالم الشبكات الحاسوبية المتصلة عبر الكابلات وأجهزة التوجيه "مثل اتصالات الهاتف"، والتي تتيح لنا التواصل وتخزين المعلومات واسترجاعها، يُعتبر الإنترنت، بلا منازع، أكبر هذه الشبكات وأكثرها شهرة، حيث تم استخدامه في البداية للبريد الإلكتروني، وبروتوكول نقل الملفات " FTP، ولوحات الإعلانات، ومجموعات الأخبار، وبروتوكول Telnet للوصول عن بُعد إلى الحواسيب"، وأصبح الآن اسمًا مألوفًا بشكل واسع بفضل شبكة الويب العالمية، التي توفر استخدامًا سهلاً. ويُعد الفضاء السيبراني مجموعة ديناميكية من أنظمة المعلومات المترابطة والمستخدمين الذين يتفاعلون مع هذه الأنظمة (Choudhury & Malik, 2019, p. 170).

2.2.3 الارهاب السيبراني

يمثل الإرهاب السيبراني فاعلاً مهماً في الفضاء السيبراني، حيث إن هدفه سياسي وإيديولوجي في المقام الأول يسعى إلى نشر الخوف، من الضروري توفر أربعة عناصر لنستطيع القول بأنه إرهاب سيبراني، وهي: استخدام جهاز كمبيوتر، دافع سياسي، الإكراه النفسي، وإمكانية العنف الجسدي، كما يجب أن يكون الهدف من الإرهاب السيبراني سياسياً أو دينياً أو اجتماعياً، وهذه الشروط تساعد في التمييز بين الإرهاب السيبراني وبقية الأنشطة المشابهة مثل الجرائم السيبرانية والحروب السيبرانية وغيرها (حارك، 2024، ص 41).

3.2.3 المجال الرقمي

المجال الرقمي يُشير إلى "البيئة التي يتم فيها معالجة وتبادل المعلومات عبر التقنيات الرقمية، بما في ذلك الشبكات، والبرمجيات، والبيانات، والتطبيقات المتنوعة". ويعتبر مفهومًا قريبًا من الفضاء السيبراني مع تركيزه على الجانب التقني للمعلومات وتحويلها إلى صيغ رقمية قابلة للتخزين والمعالجة والتداول، (OECD, 2019) كما أنه يشمل مجموعة من الأساليب والأنشطة الرقمية الجديدة التي تمكّننا من إنتاج ونشر المحتوى الإعلامي وتلقيه بمختلف أشكاله عبر الأجهزة الإلكترونية "سواء كانت متصلة أو غير متصلة بالإنترنت في عملية تفاعلية بين المرسل والمستقبل" (منصور، 2022، ص 89).

يمكن القول، بناءً على ما سبق، إن المفاهيم المرتبطة بالفضاء السيبراني تعكس تطور البيئة الرقمية وتوسع استخداماتها، حيث تتداخل بين البعد التقني مثل المجال الرقمي، والبعد التفاعلي مثل الفضاء السيبراني، وصولًا إلى البعد الأمني والتهديدي كما في الإرهاب السيبراني، مما يُبرز شمولية الفضاء السيبراني وتنوع أبعاده.

4. المطلب الثاني (الفضاء السيبراني كأداة للقوة والنفوذ في السياسة الدولية)

أصبح الفضاء السيبراني نتيجة للاعتماد المتزايد على التكنولوجيا الرقمية ساحة رئيسية للتنافس الجيوسياسي، حيث أصبحت القدرات السيبرانية تؤثر في موازين القوى العالمية، الدول المتقدمة في المجال الرقمي تمتلك قدرة أكبر على حماية مصالحها وتنفيذ عمليات تأثير ضد خصومها، بينما تظل الدول الضعيفة أكثر عرضة للاستهداف، لم يعد النفوذ السيبراني مقصورًا على الهجمات المباشرة، بل يتضمن التأثير على الرأي العام والتلاعب في المجالات السياسية والاقتصادية، مما جعل الأمن السيبراني جزءًا أساسيًا من الأمن القومي، ودفع الدول لتطوير استراتيجيات دفاعية وهجومية لمواجهة هذه التهديدات المتزايدة.

في القرن الحادي والعشرين، أصبح الفضاء السيبراني مجالًا استراتيجيًا مركزيًا في بنية العلاقات الدولية، حيث تجاوز كونه مجرد فضاء تقني ليصبح أداة فعالة لإعادة تشكيل أنماط القوة والنفوذ بين الدول، يستند هذا التحول إلى خصائصه البنيوية مثل اللا إقليمية النسبية، وتعدد الفاعلين، وصعوبة الإسناد، وهي عناصر ساهمت في تقويض المفاهيم التقليدية المرتبطة باحتكار الدولة للعنف الشرعي وضبط المجال الإقليمي، في هذا السياق، أصبحت الدول الأكثر تقدمًا تقنيًا تستخدم الفضاء السيبراني كوسيلة لتعزيز نفوذها عبر أدوات هجومية ودفاعية غير تقليدية، تشمل التأثير في الرأي العام وإدارة الصراعات وتوجيه التفاعلات السياسية والاقتصادية. من ناحية أخرى، أدى انفتاح هذا المجال أمام فاعلين غير دوليين إلى تعقيد البيئة الدولية وزيادة مستويات عدم اليقين، بسبب صعوبة إسناد الهجمات وتحديد المسؤولية عنها، مما أضعف آليات المساءلة التقليدية، وبالتالي يمكن القول إن الفضاء السيبراني أصبح يشكل بنية قوة جديدة تعيد تعريف مفهوم النفوذ في السياسة الدولية، وتفرض تحديات نظرية وعملية على مقاربات العلاقات الدولية الكلاسيكية (عمران، 2024، ص 13).

يشكل الفضاء السيبراني في العلاقات الدولية تحولًا مهمًا في بنية النظام الدولي، إذ لم يعد مجرد مجال تقني، بل أصبح عنصرًا مؤثرًا في إعادة تشكيل تفاعلات الدول

DOI:10.61704/pr.657

وأنماط القوة والنفوذ. وقد أثار هذا التحول جدلًا نظريًا حول طبيعته: هل هو مجال مستقل ضمن مجالات السياسة الدولية أم عامل بنيوي مُعدِّل داخل النظام الدولي. تتوزع المقاربات حوله إلى ثلاث اتجاهات رئيسية (Foulon & Meibauer, 2024, p. 433):

1. يرى أنه أحدث تحولًا جذريًا في مفاهيم الحرب والردع وأدوات القوة.
2. يعتبر تأثيره محدودًا ولا يتجاوز كونه امتدادًا للأدوات التقليدية.
3. ينظر إليه كعامل بنيوي يؤثر في سلوك جميع الفاعلين ويعيد تشكيل التفاعل الدولي بشكل غير مباشر.

وفي هذا السياق، يُطرح مفهوم "المُعدِّل البنيوي" الذي يدمج الفضاء السيبراني ضمن بنية العلاقات الدولية دون إلغائها، بل من خلال إعادة تشكيل كيفية عملها عبر التأثير في توزيع القوة ومستويات عدم اليقين. وبالتالي، لا يُحدث الفضاء السيبراني تغييرًا جذريًا في النظام الدولي، لكنه يعيد تنظيم آليات عمله ويزيد من تعقيد التفاعلات بين الفاعلين.

يمكن اعتبار الفضاء السيبراني كعامل مُعدل بنيوي في النظام الدولي، إذ لا يقتصر تأثيره على كونه مجالًا تقنيًا تمارس فيه الدول أنشطتها، بل يمتد ليعيد تشكيل كيفية إدراك الفاعلين لتأثيرات بنية العلاقات الدولية. إن انتشار الفضاء السيبراني يؤثر على مستوى النظام الدولي بشكل عام، من خلال زيادة كثافة وسرعة التفاعلات وتوسيع نطاقها بين الدول والفاعلين غير الدوليين، مما يؤدي إلى إنشاء أنماط أكثر تعقيدًا في العلاقات الدولية. كما يساهم الفضاء السيبراني في إعادة توزيع مظاهر القوة والنفوذ، ليس فقط من خلال تعزيز القدرات التقنية للدول، بل أيضًا عبر تغيير طبيعة التهديدات وأساليب التأثير، بما في ذلك التأثير المباشر على الرأي العام وتوظيف أدوات غير تقليدية في إدارة الصراع. كما يسهم في تقليص الفجوة بين الفاعلين الدوليين وغير الدوليين، مما يمنح بعض الدول الأصغر قدرة نسبية على التأثير في بيئة دولية تتسم بعدم التماثل في القوة التقليدية. ومع ذلك، فإن الفضاء السيبراني لا يلغي البنية التقليدية للنظام الدولي القائم على الفوضى وتوزيع القوة، بل يعيد تشكيل كيفية تفاعل الدول معها وإدراكها لها، وبالتالي فإنه يعمل كعامل تعديلي يغير شروط ممارسة القوة دون أن يغير قواعد النظام الدولي بشكل جذري، مما يجعله عنصرًا أساسيًا لفهم التحولات الحالية في بنية النفوذ في السياسة الدولية (Cyberspace Reading, 2025).

يمكن اعتبار البعد الأمني كأحد أكثر الجوانب تأثرًا بظاهرة الرقمنة في العلاقات الدولية، إذ إن الخصائص البنيوية للفضاء السيبراني، مثل الشفافية النسبية واللامركزية وقابلية الاختراق، جعلته بيئة معقدة أمنيًا. وفي هذا السياق، اتسع مفهوم الأمن السيبراني ليشمل مجموعة واسعة من التهديدات، بدءًا من النزاعات والهجمات السيبرانية، مرورًا بالتجسس والمراقبة الرقمية، وصولًا إلى الحروب الهجينة والإرهاب السيبراني. وقد أسهم هذا التحول في إعادة صياغة مفهوم الأمن نفسه في العلاقات الدولية، بحيث لم يعد محصورًا في الإطار التقليدي المرتبط بالدولة فقط، بل أصبح سؤال "أمن من؟" محورًا رئيسيًا في النقاشات الراهنة. كما أدى تطور الفضاء السيبراني إلى توسيع نطاق الفاعلين والقطاعات الأمنية، وتعميق الترابط بين مستويات الأمن المختلفة، مما يجعل أمن أي فاعل مرتبطًا مباشرة بأمن الآخرين داخل الشبكة السيبرانية العالمية. وبالتالي، لا يقتصر الأمن السيبراني على حماية الدولة ومؤسساتها، بل يمتد ليشمل أمن الأفراد، مما يتماشى مع مقاربة الأمن الإنساني التي تنظر إلى الأمن كمنظومة متعددة الأبعاد تتداخل فيها الجوانب السياسية والاقتصادية والصحية والغذائية والبيئية والاجتماعية، مما يجعل الأمن السيبراني أحد المكونات الأساسية للأمن الشامل في البيئة الدولية المعاصرة (Akyeşilmen, 2024, pp. 504–505).

في ضوء ما سبق، يتضح أن الفضاء السيبراني أصبح عنصرًا بنيويًا فاعلًا في إعادة تشكيل العلاقات الدولية من خلال تأثيره على توزيع القوة وأنماط التفاعل بين الفاعلين، وهو لا يلغي البنية التقليدية للنظام الدولي، بل يعمل كمُعدل بنيوي يعيد تشكيل كيفية إدراكها والتفاعل معها، مما يزيد من تعقيد التفاعلات ويعلي من مستويات عدم اليقين، وفي هذا السياق أصبح الأمن السيبراني جزءًا أساسيًا من الأمن الشامل والأمن الإنساني في البيئة الدولية المعاصرة.

5. المطلب الثالث (إيران و "إسرائيل" في التنافس السيبراني)

شهد الصراع الإيراني "الإسرائيلي" في يونيو 2025 تصعيدًا عسكريًا بعد ضربات "إسرائيلية" استهدفت منشآت نووية إيرانية، وقد دفع هذا التصعيد نحو احتمالات أكبر لانتقال المواجهة إلى الفضاء السيبراني كأداة رد غير مباشر، ورغم تاريخ الطرفين في الهجمات السيبرانية، فإن التوتر الجديد يعزز من دور الفضاء الرقمي كساحة صراع موازية، ويُتوقع أن يشهد الفضاء السيبراني نشاطًا متزايدًا بين الجانبين في إطار هذا التصعيد.

1.5 الهيكل التنظيمي لجهاز الأمن السيبراني الإيراني و"الاسرائيلي"

تُنفَّذ الأنشطة السيبرانية الإيرانية من قِبَل عدة هيئات ومجالس مترابطة، تتبع لجهات حكومية مختلفة، بما في ذلك الرئيس والمرشد الأعلى وأمين المجلس الأعلى للأمن القومي، ومن أبرز هذه الهيئات وزارة الاستخبارات والأمن والحرس الثوري الإسلامي، الاول هو الجهاز المسؤول عن جمع المعلومات الاستخباراتية محلياً ودولياً، ومكافحة التجسس، ومراقبة المعارضين المحليين، ومن أبرز الجماعات المرتبطة بها والتي تُعنى بالتهديدات السيبرانية (SecAlliance, 2025):

1. Muddy Water: تركز على التجسس الإلكتروني، بشكل أساسي في الشرق الأوسط وأفريقيا، ولكن تم ربطها بنشر برامج الفدية من قبل الحكومة "الإسرائيلية".

DOI:10.61704/pr.657

2. APT34: معروفة باستخدامها لبرامج مسح البيانات المدمرة.

3. أغريوس: معروفة بنشر برامج الفدية وبرامج مسح البيانات، وخاصة ضد "اسرائيل".

4. Void Manticore: غالبًا ما تتنكر هذه الجماعات في صورة مجموعات ناشطة في مجال القرصنة، وقد استهدفت "اسرائيل" ببرامج خبيثة مدمرة وساهمت في تضخيم روايات الهجوم.

اما الثاني فهو الحرس الثوري الإسلامي اذ يتولى مهمة واسعة النطاق تتمثل في الدفاع عن الثورة ضد التهديدات الخارجية والداخلية، ويشارك في كثير من الأحيان في عمليات ذات نطاق عالمي أوسع من تلك التي تقوم بها الجهات المرتبطة بوزارة الاستخبارات الإيرانية، ومن أبرز أقسامه الإلكترونية ما يلي (SecAlliance, 2025):

1. APT35، APT42: تتخصص في جمع المعلومات الاستخباراتية على المدى الطويل وحملات التصيد الاحتيالي المستهدفة، على التوالي.

2. APT33: تشارك في حملات التجسس الإلكتروني ضد البنية التحتية الحيوية، وهي في وضع يسمح لها بتنفيذ حملات التأثير المتعلقة بالانتخابات.

3. فوكس كيتن: اشتهرت بالتجسس، ومخططات القرصنة والتسريب، ونشر برامج الفدية.

4. Storm-0784 "CyberAv3ngers/Soldiers of Solomon": جهات فاعلة تتنكر في زي ناشطين إلكترونيين، وقد تم ربطها بهجمات تخريبية وهجمات على أنظمة التكنولوجيا التشغيلية (OT).

اما الهيكل التنظيمي للأمن السيبراني في "إسرائيل" يقوم على نموذج مركزي–شبكي يجمع بين القيادة الحكومية والتنسيق مع المؤسسات الأمنية والقطاع الخاص، ويمكن توضيحه كالتالي (Cyber-Reports, 2020, pp. 5–11):

- المستوى القيادي الأعلى: تتولى المديرية الوطنية السيبرانية (INCD) الإشراف العام، وهي جهة مركزية ترتبط مباشرة بمكتب رئيس الوزراء، وتضطلع بوضع الاستراتيجيات والسياسات الوطنية للأمن السيبراني.

- المستوى الأمني والعسكري: تشارك الأجهزة الأمنية في تنفيذ العمليات، مثل الجيش "خصوصًا الوحدات السيبرانية العسكرية"، وجهاز الأمن الداخلي "الشاباك"، وجهاز الاستخبارات الخارجية "الموساد"، حيث تتولى هذه الجهات مهام الدفاع والهجوم السيبراني وجمع المعلومات.

- المستوى المدني–الوطني: تتولى هيئات مدنية مسؤولية حماية البنية التحتية الحيوية، والتنسيق مع الوزارات والمؤسسات الحكومية، إضافة إلى إدارة الاستجابة للحوادث السيبرانية.

- القطاع الخاص والشراكات: يعتمد النظام بشكل كبير على التعاون مع الشركات التكنولوجية والقطاع الخاص، وكذلك على شراكات دولية "خصوصًا مع الولايات المتحدة"، لتعزيز القدرات التقنية والابتكار.

أذ أن الهيكل ليس هرميًا تقليديًا فقط، بل هو منظومة متكاملة متعددة الفاعلين، تقودها مهمة مركزية، وتُنفذها شبكة من المؤسسات الأمنية والعسكرية والمدنية، مع دعم قوي من القطاع الخاص.

تعتبر "إسرائيل" إيران تحديًا أمنيًا رئيسيًا في ظلّ سعي إيران لتطوير برنامجها النووي وبناء نفوذها على المستوى الإقليمي، لإيران أيضًا موقف مختلف تجاه القضية الفلسطينية، فدعمها لاستقلال فلسطين وإقامة دولتها الفلسطينية كان حاسمًا لأمن "إسرائيل" وباعتبارها أحد اللاعبين الرئيسيين في الشرق الأوسط، تُمثّل إيران التحدي الأبرز لأمن "إسرائيل"، علاوة على ذلك ترى إيران في "إسرائيل" تهديدًا، لا سيما لسيادتها الوطنية ووكلائها في منطقة الشرق الأوسط" وقد دفع قلق "إسرائيل" وإيران الأمني كلتيهما إلى تعزيز قدراتهما العسكرية، وتلعب العمليات السيبرانية دورًا رئيسيًا في الصراع "الإسرائيلي" الإيراني، وقد استخدم الطرفان العمليات السيبرانية لإضعاف أمن كل منهما في الشرق الأوسط (Amaliya, 2025, pp. 50–54).

2.5 التصعيد العسكري والسيبراني في الصراع الإيراني "الإسرائيلي"

بدأت المواجهة السيبرانية بين "إسرائيل" وإيران تتصاعد بالتوازي مع التوترات العسكرية، حيث بادرت "إسرائيل" في مراحل مبكرة إلى تنفيذ هجمات سيبرانية استهدفت منشآت إيرانية حساسة ضمن سياق الضغط الأمني والتقني، وقد شكّل فيروس ستوكسنت "2010" أبرز مثال على ذلك ، اذ تم بالتعاون التقني العالي بين الولايات المتحدة و"إسرائيل" من حيث استهداف البنية النووية الإيرانية وألحق بها أضرارًا مادية مباشرة، وفي المقابل طوّرت إيران قدراتها السيبرانية وردّت عبر هجمات مضادة استهدفت البنية التحتية الإسرائيلية، بما في ذلك أنظمة المياه والنقل والمواقع الحكومية، إضافة إلى عمليات اختراق وتخريب رقمية، ومع استمرار هذا التصعيد، أصبحت الهجمات السيبرانية المتبادلة جزءًا ثابتًا من نمط الصراع، حيث انتقلت المبادرة بين الطرفين بشكل متبادل وفقًا لظروف التوتر السياسي والعسكري، ما جعل الفضاء السيبراني ساحة مواجهة ديناميكية ومتغيرة في العلاقات بينهما (Umar, 2025, p. 2040).

نفذت "اسرائيل" في حزيران 2025، عملية عسكرية واسعة ضد إيران استهدفت منشآت نووية ومواقع عسكرية، تلاها رد إيراني عبر إطلاق صواريخ، بالتوازي مع نشاط سيبراني متبادل بين الطرفين، شمل هجومًا إلكترونيًا نفذته مجموعة

DOI:10.61704/pr.657

قرصنة موالية "لإسرائيل" تُعرف باسم "العصفور المفترس" استهدف بنك سباه الإيراني، ما يعكس انتقال جزء من المواجهة إلى الفضاء الرقمي، ووفقًا لتقارير مختبر NSFOCUS Fuying، فقد شهد عام 2025 موجات متصاعدة من الهجمات السيبرانية المتبادلة بين الجانبين، إذ بلغت الهجمات الموجهة ضد إيران ذروتها في 10 حزيران، أي قبل الضربة العسكرية الإسرائيلية بثلاثة أيام، واستهدفت قطاعات حيوية مثل الخدمات المالية والإعلام والاتصالات والبنية التحتية الرقمية، بما يشير إلى وجود استعدادات وتنسيق مسبق ضمن سياق تصعيد أوسع، وفي المقابل تصاعدت الهجمات السيبرانية الايرانية ضد "إسرائيل" في 16 حزيران، عقب الضربات العسكرية "الإسرائيلية" مباشرة، واستهدفت هذه الهجمات مؤسسات حكومية وقطاعات الدفاع والطيران والتعليم وغيرها، ويُظهر تزامن هذه الهجمات مع التطورات العسكرية أن الفضاء السيبراني أصبح جزءًا مكمّلًا للصراع التقليدي، وأداة متبادلة في إطار "الهجوم المضاد" بين الطرفين (NSFOCUS Fuying Lab, 2025).

وعندما شنت الولايات المتحدة و"إسرائيل" عملية "الغضب الملحمي" في 28 شباط 2026، لم تكن الخطوات الأولى قاذفات بي-2 أو صواريخ توماهوك، بل كانت ضربة خفية حددت ملامح المرحلة التالية من الصراع ، اذ لعبت طائرة الحرب الإلكترونيةEA-18G Growler، التابعة للبحرية الأمريكية، دورًا محوريًا في قمع رادارات الدفاع الجوي الإيراني وأنظمة الاتصالات في الساعات الأولى من تلك العملية، اذ نشرت الولايات المتحدة طائرات شبحية من بينها قاذفة القنابل B-2 Spirit ومقاتلات35-F، إلى جانب طائرة EA-18G Growler، التي تتمثل وظيفتها الأساسية في التشويش على أنظمة الرادار والاتصالات المعادية، ووفرت الأصول الفضائية، بما في ذلك كوكبة الأقمار الصناعية التابعة لقوة الفضاء الأمريكية، دعمًا استخباراتيًا وإنذارًا صاروخيًا فوريًا، حيث كان التسلسل العملياتي واضحًا: القمع، ثم التشويش، ثم الضرب، وفي غضون ساعات من الضربات، تضررت اتصالات إيران بشدة وانخفضت سرعة الإنترنت في إيران إلى حوالي 4% من مستوياتها الطبيعية، وتعطلت الخدمات الحكومية، وتم اختراق بث قنوات التلفزيون الحكومية الفضائية لبث رسائل مؤيدة لتغيير النظام (ORF Geotech, 2026).

كان رد إيران على الحرب الإلكترونية محدودًا، لكنه لم يكن ضئيلاً، وقد تحقق نجاحها الأكبر ليس في الجو، بل في البحر، فقد شهد مضيق هرمز وهو ممر مائي حيوي يبلغ عرضه 39 كيلومترًا، ويمر عبره نحو 20% من نفط العالم، تشويشًا إلكترونيًا متطورًا أثر على الملاحة العسكرية والتجارية منذ شباط 2026، ففي غضون 24 ساعة من أولى الضربات الأمريكية "الإسرائيلية"، أبلغت أكثر من 1100 سفينة تجارية في مياه الإمارات وقطر وعُمان وإيران عن أعطال في الملاحة، وقد رصدت أنظمة تحديد المواقع العالمية "GPS" على متن السفن مواقع في المطارات ومحطات الطاقة النووية ومواقع داخلية، وهي سمة مميزة للتشويش الإلكتروني النشط، وبحلول نهاية الأسبوع الأول، سجل 1735 حالة تشويش أثرت على 655 سفينة، مع تضاعف الحوادث اليومية تقريبًا (ORF Geotech, 2026).

وأن التصعيد في الصراع الإيراني–الإسرائيلي لا يقتصر على البعد الإقليمي، بل يمتد إلى تداعيات عالمية تعيد تشكيل موازين القوى الدولية. إذ تستغل روسيا انشغال الولايات المتحدة في الشرق الأوسط لتخفيف الضغط عن أوكرانيا وتعزيز اقتصادها من خلال ارتفاع أسعار الطاقة، مع احتمال توظيف الصراع عبر دعم غير مباشر لإيران، بما في ذلك الهجمات السيبرانية والمعلوماتية. في المقابل، تواصل الصين دعم إيران اقتصاديًا وعسكريًا باعتبارها شريكًا استراتيجيًا ومصدرًا رئيسيًا للطاقة، مستفيدة من انشغال واشنطن لتوسيع نفوذها في آسيا. كما يؤدي هذا الانخراط الأمريكي المتزايد في الشرق الأوسط إلى إضعاف تركيزها على منطقة المحيطين الهندي والهادئ، ما يمنح الصين هامشًا أوسع في ملف تايوان. وبذلك، يعكس الصراع تحوّلًا في النظام الدولي نحو ترابط الأزمات وتعدد ساحات التنافس بين القوى الكبرى (Hamdach, 2026).

ويمكن القول إن الصراع الإيراني–الإسرائيلي تطور من مواجهة عسكرية تقليدية إلى صراع متعدد الأبعاد يشمل الفضاء السيبراني، حيث أصبحت الهجمات السيبرانية جزءًا ثابتًا من أدوات الصراع بين الطرفين، ويعكس ذلك امتلاك كل من إيران وإسرائيل هياكل تنظيمية متقدمة للأمن السيبراني وقدرات هجومية ودفاعية متبادلة، تطورت منذ هجوم ستوكسنت وصولًا إلى تصعيدات 2025، كما أظهر التصعيد في 2026 دخول أطراف دولية كبرى في هذا المجال، مما وسّع نطاق الصراع ليشمل أبعادًا إقليمية ودولية. وبذلك لم يعد الفضاء السيبراني مجرد ساحة مساندة، بل أصبح عنصرًا أساسيًا في إعادة تشكيل ديناميكيات القوة والنفوذ في هذا الصراع.

6. الخاتمة

يمثل الصراع بين إيران و"إسرائيل" نموذجًا متقدمًا لتحول طبيعة النزاعات في النظام الدولي الحديث، حيث لم يعد هذا الصراع مقتصرًا على الإطار العسكري التقليدي، بل تطور ليصبح ذا طابع معقد تتداخل فيه الجوانب العسكرية والسياسية والأمنية والسيبرانية. لقد أصبح الفضاء السيبراني عنصرًا جوهريًا في هذا الصراع، وليس مجرد أداة مساعدة، إذ يتم استخدامه كوسيلة للردع والهجوم واستنزاف الموارد بين الطرفين.

كما أن تطور القدرات السيبرانية لدى كل من إيران و"إسرائيل" ساهم في إعادة تشكيل أساليب إدارة النزاع، حيث انتقلت المواجهة من ساحات القتال المباشرة إلى فضاء رقمي أكثر مرونة وأقل تكلفة وأكثر تعقيدًا في الدعم. هذا التحول قد زاد من ديناميكية الصراع وجعله أكثر تعقيدًا وصعوبة في التنبؤ، خاصة مع تداخل الفعل السيبراني مع العمليات العسكرية التقليدية كما شهدنا في تصعيدات عامي 2025 و2026.

ومن ناحية أخرى، فإن توسع نطاق هذا الصراع ليشمل دولًا كبرى مثل الولايات المتحدة وارتباطه غير المباشر بتوازنات روسيا والصين يؤكد أن تداعياته لم تعد محصورة إقليميًا، بل أصبحت جزءًا من إعادة تشكيل موازين القوى العالمية. وهذا يعكس بوضوح أن الفضاء السيبراني لم يعد مجرد مجال تقني، بل تحول إلى ساحة استراتيجية تُعاد فيها صياغة مفاهيم القوة والنفوذ والردع في العلاقات الدولية.

DOI:10.61704/pr.657

وبناءً على ذلك، فإن هذا الصراع يبرز اتجاهًا عالميًا متصاعدًا نحو "رقمنة" النزاعات الدولية، حيث تتداخل الحرب التقليدية مع الحرب السيبرانية ضمن منظومة واحدة، ما يجعل إدارة الصراعات المستقبلية أكثر تعقيدًا، ويؤكد الحاجة إلى فهم أعمق لدور الفضاء السيبراني في تشكيل النظام الدولي المعاصر.

المصادر:

المصادر العربية

حارك، ف. (2025). الفضاء السيبراني والتحول في مفهوم الأمن في الولايات المتحدة الأمريكية [أطروحة دكتوراه، جامعة قسنطينة 3]. https://doi.org/10.13140/RG.2.2.33456.47365

السعدون، ح. ح. (2014). استخدام الفضاء الإلكتروني وتأثيره في العلاقات الدولية: الشرق الأوسط أنموذجًا. مجلة دراسات دولية، (59)، 1–22.

ذيب، م.، & فارس، ف. (2021). الفضاء الإلكتروني: مفاهيم ودلالات: رؤية سوسيولوجية تحليلية. مجلة التميز الفكري للعلوم الاجتماعية والإنسانية، 3(1)، 149–157.

عمران، ط. ع. (2024، 11 مايو). الفضاء السيبراني: إطار مفاهيمي في ضوء نظريات العلاقات الدولية. المركز الديمقراطي العربي. https://democraticac.de/?p=96508

منصور، ح. (2022). الإعلام الرقمي: مفهومه، وسائله، ونظرياته. مجلة بحوث ودراسات في الميديا الجديدة، 3(2)، 87–104.

المصادر الاجنبية

Akyeşilmen, N. (2024). Geopolitical implications of cyberspace on international relations: An in-depth analysis. In A. N. Yurdusev & M. Doğrul (Eds.), Global transformations and Türkiye (pp. 501–518). Turkish Academy of Sciences. https://doi.org/10.53478/TUBA.978-625-6110-04-5.ch36

Amaliya, L. R. (2025). A cyber war of Iran-Israel: A geopolitical rivalry. In I. K. Rohman et al. (Eds.), Proceedings of the International Conference on Strategic and Global Studies (ICSGS 2024) (pp. 45–56). Atlantis Press. https://doi.org/10.2991/978-94-6463-646-8_4

Awasthi, S. (2026, March 24). Signals before strikes: Electronic warfare in the Iran war. Observer Research Foundation. https://www.orfonline.org/expert-speak/signals-before-strikes-electronic-warfare-in-the-iran-war

Foulon, M., & Meibauer, G. (2024). How cyberspace affects international relations: The promise of structural modifiers. Contemporary Security Policy, 45(3), 426–458. https://doi.org/10.1080/13523260.2024.2365062

Frei, J. (2020). Israel's national cybersecurity and cyberdefense posture: Policy and organisations. Center for Security Studies, ETH Zürich. https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2020-09-Israel.pdf

Hamdach, W. (2026, March 26). The war against Iran and global risks: "Tell me how this ends." Georgetown Journal of International Affairs. https://gjia.georgetown.edu/conflict-security/the-war-against-iran-and-global-risks-tell-me-how-this-ends/

Malik, J. K., & Choudhury, S. (2019). Cyber space—Evolution and growth. East African Scholars Journal of Education, Humanities and Literature, 2(3), 170–190. https://doi.org/10.36349/easjehl.2019.v02i03.005

McLeod, R. K. (2025, June 13). Iran's cyber strategy and the Israel-Iran conflict. SecAlliance. https://www.secalliance.com/blog/irans-cyber-strategy-and-the-israel-iran-conflict

NSFOCUS Fuying Lab. (2025, June 26). The hacktivist cyber attacks in the Iran-Israel conflict. NSFOCUS. https://nsfocusglobal.com/the-hacktivist-cyber-attacks-in-the-iran-israel-conflict/

Nye, J. S., Jr. (2010). Cyber power. Belfer Center for Science and International Affairs, Harvard Kennedy School. https://www.belfercenter.org/publication/cyber-power

Saaid, Z. (2025). Cyberspace reading through the prism of international relations theories: Morocco as a practical case. European Journal of Law and Political Science, 4(3), 1–9. https://doi.org/10.24018/ejpolitics.2025.4.3.172

Touré, H. I., & Permanent Monitoring Panel on Information Security of the World Federation of Scientists. (Eds.). (2011). The quest for cyber peace. International Telecommunication Union. https://www.itu.int/pub/S-GEN-WFS.01-1-2011

Umar, M. (2025). Iran and Israel cyber warfare and interference of US. Social Science Review Archives, 3(2), 2040–2048. https://doi.org/10.70670/sra.v3i2.824

DOI:10.61704/pr.657

Cyberspace as a Tool of Influence in International Politics: A Case Study of Iran and "Israel"

P-ISSN: 1680-9300
E-ISSN: 2790-2129
Vol. (26), No. (3)
pp. 32-39

Zaman M. Jabbar

Presidency of Al-Nahrain University, Baghdad, Iraq.

Abstract:

The rapid advancements in modern technology and the near-total reliance of most countries on it have reshaped economic, political, and social relations. This is due to the central role technology plays in facilitating movement and communication between nations, enhancing cooperation, enabling rapid access to essential information, and increasing the efficiency of international economic activity to unprecedented levels. Cyberspace is the environment in which technology thrives and flourishes; it is a unique world, distinct from the traditional rules of the human world as we know it, and it has its own set of rules. For example, in nature, strength is the opposite of weakness; the stronger an individual is, the fewer their weaknesses. This applies to the animal and plant kingdoms. However, in the cyber world, the more advanced a nation's cyber capabilities and digital government become, the greater its vulnerabilities.

This technological advancement presents dire consequences if it is misused or turned into a tool for political and military conflict between countries, this has already happened over the past two decades between several countries, especially between Iran and Israel, as the conflict between these two countries in the Middle East escalates, with each developing its own cyber tools and using them in its conflict against the other.

Keywords: Cyberspace, International Influence, International Politics, Iran, Israel.

How to Cite: Jabbar, Z. M. (2026). Cyberspace as a Tool of Influence in International Politics: A Case Study of Iran and "Israel". PROSPECTIVE RESEARCHES, 26(3), 31–39. https://doi.org/10.61704/pr.657

DOI:10.61704/pr.657