

العدد الثامن والعشرون - الجزء الثاني - سبتمبر - 2026 - السنة السادسة مجلة علمية فصلية محكمة

المجلة الأمريكية الدولية للعلوم الإنسانية والاجتماعية

American International Journal of Humanities and Social Sciences

الالكتروني (3085 - 4806) (ISSN) / الورقي (3085 - 4830) (ISSN)

رقم الايداع القانوني في المكتبة الوطنية المغربية (2025 Pe00006)

رقم الايداع القانوني في دار الكتب والوثائق العراقية (2735)

تصدر عن الأكاديمية الأمريكية الدولية للتعليم العالي والتدريب

ISSUED BY AMERICAN INTERNATIONAL ACADEMY OF HIGHER EDUCATION AND TRAINING





الموقع الرسمي للمجلة / www.iajphss.us


بسم الله الرحمن الرحيم

رئيس التحرير-أ.د.نزهة إبراهيم الصبري – نائب رئيس الأكاديمية الأمريكية الدولية للتعليم العالي والتدريب- المملكة المغربية

نائب رئيس التحرير: أ.د. حاتم جاسم الحسون، رئيس الأكاديمية الأمريكية الدولية للتعليم العالي والتدريب.

مدير التحرير- أ.د. هند عباس على الحمادي-أستاذ بقسم اللغة العربية وعلومها-كلية التربية للبنات-جامعة بغداد، جمهورية العراق (مدقق اللغة العربية.)

https://orcid.org/my-orcid?orcid=0009-0003-0515-501X

سكرتارية التحرير

1. أ .م.د. محمد حسن أبو رحمة . وزارة التربية – فلسطين .
2. أ.سكينة إبراهيم الصبري. الشؤون الإدارية. الأكاديمية الأمريكية الدولية للتعليم العالي والتدريب.

أعضاء هيئة التحرير

1. أ.د. حسن يوسف – استاذ اللغة العربية آدابها – جامعة قناة السويس – مصر- المدقق العام.
2. أ.د. خالد ستار القيسي ،عميد كلية الإعلام ، الأكاديمية الأمريكية الدولية للتعليم العالي والتدريب.
3. أ. مجدي عبد الله الجايح، كلية اللغات والعلوم الإنسانية الأكاديمية الأمريكية الدولية للتعليم العالي والتدريب. (مدقق اللغة الإنكليزية)
4. المهندس اسماعيل المساق، كلية علوم التقنية ،جامعة محمد الخامس ،الرباط، المملكة المغربية. (التصميم)
5. أ.محمد تايه محمد - بك إدارة أعمال - كلية الإدارة والاقتصاد - جامعة الكوفة. (التنضيد) .
https://orcid.org/0009-0003-6945-2806

أعضاء الهيئة العلمية

1. Prof. Dr. Hanik Mahliatussikah – State University of Malang, Indonesia, Chairman of the Association of Arabic Language Teaching Departments in Indonesia.
2. Prof. Dr Shamnad N – University College, Thiruvananthapuram, Kerala, India.
3. Prof.Dr.Ali H. ABDUL RASOL – KDG College – Leerexpert -England.
4. Dr.MUSTAPHA ABDUL AZIZ AKANJI – Président-Fondateur des groupes scolaires et Universitaires AKANJI En Côte d'ivoire et Nigeria.

5. Dr.Nada Al-Abidi – Educational Sciences Teaching Curricula, Methods, and E-Learning – Sweden;

6. .أ.د. أبكر عبد البنات آدم. مدير جامعة القرآن الكريم وتأصيل العلوم. جمهورية السودان https://orcid.org/0009-0009-8298-4464.

7. أ.د. رانيا الصاوي عبده عبد القوي – قسم علم نفس تربوي – كلية التربية – جامعة 6 اكتوبر – مصر https://orcid.org/0000-0001-7436-2774 .

8. أ.د. آمال العرباوي مهدي – رئيس قسم التربية المقارنة بكلية التربية – مصر https/://orcid.org0009-0005-3260-820X .

9. أ.د. أمل مهدي جبر- رئيس قسم العلوم التربوية والنفسية. كلية التربية للبنات. جامعة البصرة، جمهورية العراق https://orcid.org/0000-0001-7463-9876 .

10. أ.د. ناهض فالح سليمان- كلية التربية للعلوم الإنسانية. قسم اللغة الإنجليزية. جامعة ديالى. جمهورية العراق https://orcid.org/0009-0009-7896-820X .

11. 1.أ. د نور الدين زين العابدين متولي أحمد – رئيس قسم اللغة العربية وآدابها بكلية العلوم الإنسانية بجامعة بيروت العربية – لبنان https://orcid.org/0009-0006-7020-7244 .

12. أ.د. نصيف جاسم أسود سالم الأحبابي. كلية التربية للعلوم الإنسانية. قسم الجغرافية. جامعة تكريت. جمهورية العراق https://orcid.org/0009-0002-6669-4706 .

13. أ.د. نورة محمد مستغفر. أستاذ التعليم العالي مؤهل، المركز الجهوي لمهن التربية والتكوين، المملكة المغربية https://orcid.org/0009-0001-4682-2005 .

14. أ.د. هاله خالد نجم- رئيس قسم الترجمة. كلية الآداب- جامعة الموصل – جمهورية العراق). https://orcid.org/0009-0004-3687-1788).

15. أ.د. محمد خضير عباس الجيلاوي – كلية الطوسي الجامعة – النجف الاشرف – العراق . https://orcid.org/0009-0001-9668-9329

16. أ.د. محمد نهان ابراهيم رحيم الهيتي – علوم اسلامية – جامعة الانبار – العراق. 0000-0003-6193-4092

17. أ. د. سميرة شمعاوي –استاذة باحثة بمركز التوجيه والتخطيط التربوي بالرباط – المغرب . https://orcid.org/0009-0008-2452-6011

18. أ.د. برزان ميسر حامد أحمد الحميد . كلية التربية للعلوم الإنسانية. جامعة الموصل . جمهورية العراق.(https://orcid.org/0009-0003-7795-3934)

19. .أ. د.محمد ازهري – جامعة السلطان مولاي سليمان – كلية الآداب والعلوم الإنسانية. بني ملال. المغرب.

20. أ.د. تارا عمر أحمد- كلية العلوم السياسية . جامعة السليمانية . جمهورية العراق https://orcid.org/my-orcid?orcid=0009-0003-9424-6211 .

21. أ.د.تحرير علي حسين علوان – كلية الفنون الجميلة – جامعة البصرة – جمهورية العراق. https://orcid.org/0009-0002-0076-0491

22. محمد لؤي محمد سليم البني معهد الحضارة للتأهيل والتدريب السياحي والفندقي | دمشق، سوريا. 0009-0008-2826-7088

23. أ. د. الشرقي عبد الحليم – كلية الآداب والعلوم الانسانية – سايس – جامعة – سيدي محمد بن عبد الله – فاس – المملكة المغربية https://orcid.org/0000-0002-6947-5712 .

24. أ.د. داود مراد حسين الداودي . دكتوراه العلوم السياسية . مدير وحدة البحوث والدراسات . جامعة القادسية . كلية القانون . جمهورية العراق https://orcid.org/0009-0000-3272-5899 .

25. أ.م.د. عزيز عبدالرحمن محمد الاديمي -جامعة تعز – مدير عام بحوث التنمية الادارية والتدريب – ديوان عام محافظة تعز – اليمن https://orcid.org/0009-0005-2702-0495 .

26. أ.م.د. علاء الدين محمد حسين عياش – رئيس قسم تكنولوجيا الاعلام -جامعة فلسطين التقنية – فلسطين https://orcid.org/0000-0001-8152-9261 .

27. أ.د. سندس عزيز فارس الفارس- خبير تربوي- عميد كلية الدراسات العليا والبحث العلمي في الاكاديمية الأمريكية . جمهورية العراق https://orcid.org/0009-0002-7185-1059.

28. أ.د.عدنان فرحان الجوراني . أستاذ الاقتصاد . جامعة البصرة . جمهورية العراق . https://orcid.org/0009-0006-6673-5714)

29. د. حلا عدنان نيربي – كلية الاقتصاد – قسم المحاسبة – جامعة حلب – سوريا https://orcid.org/0009-0006-5511-3266.

30. أ.د. ماجدولين محمد النهيبي- كلية علوم التربية . جامعة محمد الخامس . الرباط، المملكة المغربية Orcid id: 0009-0000-1125-8689.

31. د. ياسر حسن ناجي الصلوي – جامعة تعز – اليمن https://orcid.org/0009-0006-7335-3570 .

32. أ.د. ماهر مبدر عبد الكريم العباسي . نائب عميد كلية التربية للعلوم الإنسانية . جامعة ديالى . جمهورية العراق. 0009-0006-0681-1033

33. أ.د. حاكم موسى عبد الحسناوي – استاذ طرائق تدريس التأريخ – وزارة التربية – الكلية التربوية المفتوحة – جمهورية العراق https://orcid.org/0000-0002-3992-672X?lang=ar.

34. د. ليلى الادريسي – دكتوراه في القانون والعلوم السياسية – كلية العلوم القانونية والاقتصادية والاجتماعية – جامعة محمد الخامس – الراط – المغرب.
0009-0005-8175-7113

35. أ.م.د.آوان عبد الله محمود الفيضي . دكتوراه قانون خاص . كلية الحقوق . جامعة الموصل . جمهورية العراق https://orcid.org /0000-0001-8777-978x .

أعضاء الهيئة الاستشارية

1. أ.د.هالة مختار الوحش – استاذ اصول التربية الانسانية جامعة الازهر – مصر .
https://orcid.org/0009-0008-8680-0194

2. .أ.د. محمد علي عباس – علوم تربوية نفسية – الاكاديمية الامريكية الدولية للتعليم العالي والتدريب- أمريكا https://orcid.org/0009-0004-2576-8136 .

3. أ.د. حسن يوسف – استاذ اللغة العربية آدابها – جامعة قناة السويس – مصر.

4. د. عائشة الهوس – تخصص القانون العام والعلوم السياسية – المعهد المغربي للدراسات الاستراتيجية وإدارة الأزمات – المملكة المغربية https://orcid.org/0009-0000-4666-3086 .

5. أ.د. ناهض فالح سلمان – كلية التربية – جامعة ديالى – العراق https://orcid.org/0009-0009-7896-820X .

6. أ.د. رائد بني ياسين- عميد كلية الأعمال. قسم نظم المعلومات. الجامعة الأردنية- فرع العقبة . المملكة الأردنية الهاشمية (https://orcid.org/0009-0004-3687-1788) .

7. د. نادية فضيل – المركز الجهوي لمهن التربية والتكوين – بني ملال – المغرب.

8. د. هشام الميموني، دكتور في القانون العام، جامعة الحسن الثاني – الدار البيضاء ، كلية الحقوق – المحمدية(المغرب 0000-0002-9569-3369

9. أ.م. د. سماح هادي محمد – كلية الحقوق – جامعة النهرين – جمهورية العراق https://orcid.org/0009-0006-9104-6347 .

10. أ.م.د.ايمان محمد مصطفى – كلية الدراسات العليا لتكنولوجيا النانو – مدير معمل الطاقة الشمسية – جامعة القاهرة – مصر. 0000-0001-6465-X575

11. م. د. حامد شمال مصحب – كلية الحكمة الجامعة تكنولوجيا المعلومات والاتصالات والذكاء الاصطناعي – العراق https://orcid.org/0000-0002-4382-0872 .

12. أ.د. ماهر جاسب حاتم الفهد – تحصص التاريخ الحديث والمعاصر – كلية الإمام الكاظم "ع" قسم التأريخ – العراق https://orcid.org/0000-0001-5708-2527 .

13. د. نجلاء حمدان رحمة الله جادين – جامعة جازان / كلية الفنون والعلوم الإنسانية المملكة العربية السعودية https://orcid.org/0009-0008-5146-475X .

14. أ.د.علي سموم الفرطوسي – الجامعة المستنصرية / كلية التربية البدنية وعلوم الرياضة – أستاذ القياس والتقويم – الإحصاء – كرة السلة

حكم ومراقب فني دولي بكرة السلة – العراق.
ORCID: https://orcid.org/0000-0002-8598-5149

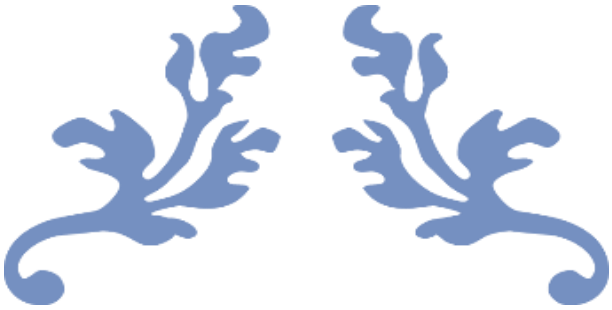
15. أ.د. مازن خلف ناصر.كلية القانون.جامعة المستنصرية . جمهورية العراق .
https://orcid.org/0000-0003-3754-4266

16. أ.م.د. محمد عبدالفتاح زهرى- رئيس قسم الدراسات الفندقية- كلية السياحة والفنادق – جامعة المنصورة- جمهورية مصر العربية(ORCID.org/0000-0002-8533-6552) .

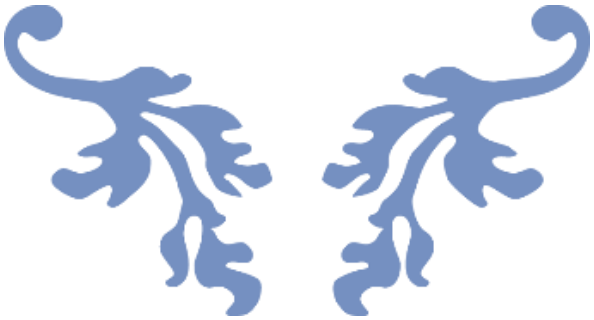
17. م.د. محمد مولود امنكور .كلية العلوم الإدارية والمالية والاقتصادية .الأكاديمية الأمريكية الدولية للتعليم العالي والتدريب https://orcid.org/0009-0000-8373-5528 .

18. أ.م.د. موسى إسماعيل صالح حسين – أستاذ مساعد الأدب والنقد العربي قسم اللغة العربية – جامعة جرش / الأردن https://orcid.org/0009-0007-7197-1954

19. أ.د. جاسم حسن سالم العطبي – طبيب عام – البصرة – العراق. 0009-0001-2819-1975



مقال العدد



بسم الله الرحمن الرحيم،

الحمد لله رب العالمين، والصلاة والسلام على خاتم الانبياء والمرسلين، وآله وصحبه أجمعين، أما بعد:

في المشهد المعرفي المتجدد، يطلّ علينا **العدد الثامن والعشرون (الجزء الثاني)** من **المجلة الأمريكية الدولية المحكمة للعلوم الإنسانية والاجتماعية**، ليحمل في طياته باقةً من الدراسات والبحوث المتميزة التي خطّتها أقلام نخبة من الباحثين والأكاديميين من المشاركين في اعمال المؤتمر العلمي الدولي الرابع والعشرون والمنعقد اون لاين للمدة 18 – 22 / 09 / 2026.

لقد حرصت هيئة التحرير في هذا العدد – كما دأبت دائماً – على ترجيح كفة **النوع والكيف** على الكمّ والعدد؛ فالغاية الأسمى لمجلتنا ليست تكديس الصفحات، بل إثراء المكتبة العربية والعالمية بالأفكار العلمية الأصيلة، والرؤى المنهجية الرصينة التي تمثل إضافة حقيقية للبحث العلمي الرصين.

وانطلاقاً من التزامنا الصارم بأعلى معايير النشر العالمي، فقد خضعت كافة البحوث الواردة إلى مسار تحكيمي دقيق وصارم، شأنها في ذلك شأن أعرق المجلات المحكمة في العالم؛ حيث تم عرض البحوث على محكمين أكفّاء ذوي مكانة علمية رفيعة ينتمون إلى مدارس وجامعات ومؤسسات أكاديمية متعددة الجنسيات، ما بين حكومية وخاصة، أثبتوا جدارة تامة في تقييم المادة العلمية والحكم على صلاحيتها للنشر بموضوعية وحياد.

وقد سلكت هيئة التحرير منهجاً مؤسسياً ثابتاً في آلية القبول والتحكيم؛ إذ يُعرض البحث على محكمين اثنين بالتوازي، فإن توافقا على الصلاحية، انتقل البحث فوراً إلى مرحلة التنضيد والإخراج الفني تمهيداً للنشر، شريطة استيفائه الكامل لتعليمات النشر الخاصة بالمجلة. أما في حال اختلاف التقييم بينهما، فيُحال البحث إلى محكم ثالث مرجعيّ، ليُصار إلى اعتماد رأيه حاسماً في قبول البحث أو استبعاده، صيانةً لجهود الباحثين وضماناً لأعلى درجات النزاهة الأكاديمية.

إنّ ما يميّز إصدارات مجلتنا هو حرصها الدائم على استيعاب التيارات الفكرية والموضوعات الإنسانية والاجتماعية المتنوعة ضمن إطار التخصص، مع ترك المساحة الرحبة للباحثين للتعبير عن رؤاهم ونظرياتهم العلمية دون تدخل في جوهر أفكارهم، شريطة التزامها بالمعايير الأخلاقية والعلمية التي تنأى عن الفوضى الفكرية أو التحريض بكل أشكاله، لتبقى منارةً للفكر الهادف والحوار البنّاء.

وختاماً.. لا يسعنا إلا أن نتقدم بخالص الشكر والتقدير وعظيم العرفان، مكللاً بأريج الود والامتنان، إلى كافة الجهود العلمية، والفنية، والإدارية المتضافرة التي أسهمت في إخراج هذا العدد إلى النور؛ من باحثين أفاضل، ومحكمين أطهار، وأسرة تحرير لا تلين عزيمتها.

والسلام عليكم ورحمة الله وبركاته.

تاريخ الإصدار: 30 سبتمبر 2026

المملكة المغربية

هيئة تحرير المجلة

الناشر:

الأكاديمية الأمريكية الدولية للتعليم العالي والتدريب – ولاية ديلاوير الامريكية.

فهرس الموضوعات

سيادة الدول في الفضاء السيبراني
أ.د. نعيمة عمر الغزير/أ.محمد إبراهيم أبوقرين.....12

نشأة وتطور المجالس التشريعية والنيابية تاريخياً
سليمان بن خلف بن زاهر الريامي 49

أثر أنموذج هوني ـ مومفورد في تحصيل طلبة قسم معلم الصفوف الأولى في كليات التربية الأساسية في مقرر علم النفس النمو.
أ. م. د. سرمد محمد داود الخفاجي.....65

حماية المشرع والقاضي الدستوري للحق في الخصوصية
الاستاذ الدكتور حيدر وهاب عبود.....82

الوعي بالذات وعلاقته بالطموح والتحصيل اللغوي لدى متعلمي اللغة العربية
أ.م.د. آلاء فيصل عيسى/.د. عبد الباقي حسين الزعيل العبد..... 98

الصحة النفسية بين الارث التشخيصي والتدخلات المعاصرة: فعالية العلاج بالتقبل والالتزام في خفض القلق لدى الافراد الذين يعانون من اضطراب استخدام القنب
الباحث: أشرف فتح الله /الدكتورة منار بن البوعزاوي /الأستاذة نجاة بلعربي.....130

سيادة الدول في الفضاء السيبراني

أ.د. نعيمة عمر الغزير
قسم القانون العام/ مدرسة العلوم القانونية /الأكاديمية الليبية للدراسات العليا: طرابلس/ليبيا
Naema.Alghazir@academy.edu.ly
00218913775445

أ.محمد إبراهيم أبوقرين
قسم القانون العام/ مدرسة العلوم القانونية /الأكاديمية الليبية للدراسات العليا: طرابلس/ليبيا
mohamedabogharen@gmail.com
00218913218329

الملخص:

نظراً لأن المادة 2، الفقرة 4 من ميثاق الأمم المتحدة تحظر استخدام القوة في العلاقات الدولية إذ تعتبر قاعدة أمرة، واستنادًا لوثائق الأمم المتحدة الأخرى بما فيها اعلان مبادئ القانون الدولي المتعلقة بالعلاقات الودية والتعاون بين الدول وفقًا لميثاق الأمم المتحدة، وميثاق الحقوق والواجبات الاقتصادية للدول، يمكن توصيف الهجمات على البنية التحتية الحيوية للدولة باستخدام الوسائل الإلكترونية على أنها نوع أخر من تدابير الإكراه التي تمارسها دولة ما على دولة أخرى

بهذا تشكل الهجمات السيبرانية تهديدات جديدة لسيادة الدول، وهذا الموضوع يكتسب أهمية متزايدة في ضوء تطورات أحكام سيادة الدول بمفهومها التقليدي

بناءً عليه؛ فإن هذه الدراسة التي تناولت مسألة سيادة الدول في الفضاء السيبراني تتبنى البحث في نهج الاعتداء على الشخصية القانونية للدولة في الفضاء السيبراني من خلال اتجاهين: الأول منهما؛ الطابع الإقليمي للفضاء السيبراني؛ والاتجاه الثاني: تأثير الهجمات السيبرانية على سيادة الدول في الفضاء السيبراني

الكلمات المفتاحية: الإقليم، الهجمات السيبرانية، التدخل السيبراني، التكنولوجيا، الإلكتروني

State Sovereignty in Cyberspace

Prof. NAEMA OMAR ALGHAZIR

Mr. MOHAMED IBRAHIM ABUGREN

Department of Public Law / Faculty of Legal Sciences/ Libyan Academy for Graduate Studies: Tripoli, Libya

Abstract:

Since Article 2, Paragraph 4 of the United Nations Charter prohibits the use of force in international relations—as it is considered a peremptory norm— and based on other United Nations documents, including the Declaration on Principles of International Law Concerning Friendly Relations and Cooperation Among States in Accordance with the Charter of the United Nations and the Charter on the Economic Rights and Duties of States, attacks on a state's critical infrastructure using electronic means can be characterized as another form of coercive measures exercised by one state against another.

Thus, cyberattacks pose new threats to state sovereignty, and this issue is gaining increasing importance in light of developments in the provisions governing state sovereignty in its traditional sense

Accordingly, this study, which addresses the issue of state sovereignty in cyberspace, examines the concept of an attack on the legal personality of a state in cyberspace from two perspectives: first, the territorial nature of cyberspace; and second, the impact of cyberattacks on state sovereignty in cyberspace

Keywords: *territory, cyberattacks, electronic, cyber interference, technology*

المقدمة

أهمية سيادة الدول في الفضاء السيبراني تتسم بالغموض؛ بالنظر لما تشكله الاختراقات الرقمية من تحدي للمفهوم القانوني والسياسي التقليدي للسيادة؛ على أن للدول السلطة الحصرية على حدودها المادية وأنظمة المعلومات وبنيتها التحتية؛ تعيد طرح الأسئلة بشأن السيادة الإقليمية للدول في الفضاء السيبراني؛ من حيث مدى استيفاؤها لتوصيف إقليم الدولة في العالم المادي ؛ وما هي الاعتبارات الأولية للتحقق من دور مبدأ سيادة الدول في الفضاء السيبراني؛ إذ يُعرَّف الفضاء السيبراني بأنه منطقة افتراضية غير ملموسة بلا حدود، لكونه نظام اتصالات ونقل بيانات سريع وغريب عن العالم الخارجي؛ إلا أنه مع تطور الدراسات القانونية في هذا الشأن تأكد بوجود ثمة اتفاق على أن السيادة ليست مجرد مصطلح أو مفهوم أساسي في القانون الدولي، بل هي ، أيضا على الأقل في صورة المساواة السيادية بين الدول، مبدأ من مبادئ القانون الدولي حتى في نطاق الفضاء السيبراني، والدلالة على ذلك سلطة تلك الدول الحصرية على إقليمها، وما اشتمل عليه من شبكات الويب والأنظمة المعلوماتية. الذي يتجلى بوضوح في ممارستها لولايتها القضائية على البنية التحتية لتكنولوجيا المعلومات والاتصالات الموجودة في نطاق إقليمها ؛ كما تسري هذه الولاية على الأنشطة السيبرانية سواء انطلقت من داخل أراضيها أو تلك التي توجه لها؛ الأمر الذي يؤكد لنا من خلال الصياغات العامة أن السيادة الإقليمية تمتد إلى البنية التحتية الإلكترونية وبيئة المعلومات وهو ما يشكل كيفية تنظيم الدول واستجابتها للأنشطة الإلكترونية التي تُنفذ من أراضيها أو تُوجه ضدها كاستخدام للقوة، فضلاً عن الرد على العمليات السيبرانية حتى في مواجهة جهات غير حكومية.

أهداف البحث:

يهدف هذا البحث إلى التقصي عن الأسانيد القانونية بشأن نطاق سريان سيادة الدولة في الفضاء السيبراني وتحدياتها؛ من خلال البحث في ممارسات الدول والتشريعات التي تتبناها في إطاره؛ بالإضافة إلى تتبع دراسات قانونية متخصصة حول تطبيق السيادة في الفضاء السيبراني؛ بقصد الوصول إلى رؤية واستنتاجات ذات قيمة علمية وقانونية بشأن الإشكاليات المتعلقة بإعمال مبدأ سيادة الدول في هذا المجال.

مشكلة البحث:

الاختصاصات المتعددة والطبيعة المعقدة والغير معروفة الحدود لهذا الفضاء تثير إشكاليات كثيرة؛ من حيث صعوبة تحديد التصرفات التي تشتبك في نطاقه؛ لذا تتمثل الإشكالية المنهجية الرئيسية للبحث في صعوبة إسقاط المفاهيم التقليدية للسيادة والإقليم والاختصاص على فضاء يتميز بطبيعته غير الإقليمية، وبقدرته على تجاوز الحدود السياسية والجغرافية للدول في ضوء تساؤل عام؛ هل يمكن للفضاء السيبراني في حد ذاته أن يكون كيانًا ذا سيادة؟، ويتفرع عن هذا السؤال تساؤلات عديدة منها: متى تُعتبر الأنشطة السيبرانية تدخلاً محظورًا في سيادة الدول؟، وما الذي يُعتبر سلوكًا قسريا في غياب الضرر المادي؟

المنهجية:

حتى نجيب عن هذه الأسئلة الواردة في مشكلة البحث؛ فإنه من حيث الأهمية العلمية وخصوصية النتائج؛ دراسة هذا الموضوع وفق المنهج التحليلي؛ بهدف تتبع القواعد التي تحكم ممارسة الدولة لاختصاصها في الفضاء السيبراني، ومدى إمكانية اعتبار انتهاك سيادة الدولة قاعدة قانونية مستقلة في مواجهة العمليات والهجمات السيبرانية، والتمييز بين مجرد التدخل في المجال السيبراني للدولة وبين سلوك قد يرقى إلى انتهاك قواعد أخرى من قواعد القانون الدولي.

بناءً عليه؛ تتطلب المنهجية العلمية لهذه الدراسة أن تكون خطة البحث على النحو التالي:

المبحث الأول: الطابع الإقليمي للفضاء السيبراني؛ **المطلب الأول منه يتعلق بدراسة** الفضاء السيبراني بوصفه نطاق السيادة السيبرانية للدول؛ في حين يناقش **المطلب الثاني:** السيادة السيبرانية مبدأ قانوني يُنتج التزامات قانونية. كما جاء **المبحث الثاني في مطلبين تحت عنوان** تأثير الهجمات السيبرانية على سيادة الدولة بموجب ميثاق الأمم المتحدة؛ الأول منهما يبحث في التدخل السيبراني المحظور؛ كما اختص **المطلب الثاني بدراسة** نماذج للتدخلات السيبرانية المحظورة ؛ **أما الخاتمة فقد تضمنت نتائج البحث وتوصياته**

المبحث الأول

الطابع الإقليمي للفضاء السيبراني

يستقي الطابع الإقليمي للفضاء السيبراني معناه من حيث أن الإقليم أو الفضاء الجغرافي أيًا كان مسماه ليس مجرد نطاق مادي أو مساحة أرضية محايدة تحدث فيها السياسة، بل هو بنية سياسية واجتماعية يتم تشكيلها عمداً؛ والدلالة على ذلك امتداد سيادة الدولة إلى الفضاء السيبراني ؛ فـقد أقرت الجمعية العامة للأمم المتحدة من خلال فريق الخبراء الحكوميين (GGE أن مبادئ القانون الدولي، وعلى رأسها ميثاق الأمم المتحدة، تنطبق بالكامل على الفضاء السيبراني. مما يعني أن لكل دولة الحق السيادي في إدارة البنية التحتية المعلوماتية والشبكات الموجودة في نطاق إقليمها؛ وإقليمية الفضاء السيبراني لا يُقصد منها إعادة رسم للخرائط، بل هو إعادة تنظيم لممارسة الدول وتوزيع السلطة عبر هذا الفضاء شأنه شأن الفضاءات الأخرى للدولة.

بناءً عليه: سنناقش في المطلب الأول: الفضاء السيبراني بوصفه نطاق السيادة السيبرانية للدول؛ ومن ثم نعرض إلى السيادة السيبرانية مبدأ قانوني يُنتج التزامات قانونية؛ وذلك على النحو التالي.

المطلب الأول

الفضاء السيبراني بوصفه نطاق السيادة السيبرانية للدول

يُعرَّف الفضاء الإلكتروني في الغالب بأنه منطقة بلا حدود، ونظام اتصالات ونقل بيانات سريع وغريب عن العالم الخارجي hab&

UKSW Łukasz Kułaga(2024), ؛ وبالتالي الحدود الإقليمية للدولة في الفضاء السيبراني تتحدى في مفهومها القانون التقليدي لكونه؛ مساحة محددة بشاشات وكلمات مرور بدلًا من علامات مادية، وفقًا لذلك أساليب فهم تعريفات الفضاء السيبراني تتقرر في فهم مكوناته؛ وهي: أولًا: البنية التحتية: وتشمل مكونات الأجهزة كالدوائر المتكاملة ومعدات تخزين البيانات وكابلات الألياف الضوئية؛ ثانيًا: برامج الحاسوب؛ ثالثًا: البيانات التي تنشؤها وتخزنها تلك المعدات(2023)Rohit Bokil

وقد تم تطوير مفهوم الفضاء السيبراني، الذي صاغه ويليام غيبسون قبل نحو أكثر من 40 عامًا https://en.wikipedia.org/wiki/Neuromancer ، بحيث يمكن فهمه على أنه يشمل جميع الكيانات التي يجب أن تكون متصلة رقميًا أو قد تصبح كذلك Ducheine, B. et al.(2021) ؛ وبالتالي يُعد الفضاء السيبراني بيئة مفاهيمية تشمل شبكة الإنترنت إلى جانب الحواسيب وشبكات الاتصالات الأخرى Lasky, Jack(2022)& Mhajne, .Anwar(2024,

كما أنه في بدايات ظهور الفضاء السيبراني، اقترح عدد من الباحثين **Johnson, D& Post,D (1996,p1402)**ما يُعرف بـ (أطروحة عدم السيادة) محناوي، محمد (2026) ، والتي تستند إلى مفهوم (الاستثنائية السيبرانية) وهي قراءة إقليمية تقليدية لمفهوم السيادة&Pierucci, F(2025) كامش طيب (2025) ، حيث ذهبوا إلى أن غياب الحدود في الفضاء السيبراني يُفقد الدول القدرة على ممارسة سلطتها على أشخاص وأقاليم محددة، ويضعف الطابع الشرعي المستمد من الرضا **Johnson, D& Post,D (1996, p1367)**

هذه الفرضية، مؤكداً أنه لا يوجد ما هو استثنائي في الفضاء السيبراني، إذ إن قيام الدول بفرض سلطتها Goldsmithوقد انتقد Goldsmith, على الأشخاص والأشياء (بما في ذلك مواطنيها في الخارج) يُعد ممارسة طبيعية للسيادة على أنشطة الفضاء السيبراني J) (1998,p1199,)& Ashkan (2025)

وبذلك نتبين بأن مجرد تجسيد الدولة لسلطتها—مثل تنظيم الفضاء السيبراني على المستوى الوطني بما يحقق الأمن السيبراني أو مكافحة الجرائم السيبرانية— يكفي لدمج (الفضاء السيبراني ضمن نطاق السيادة).

في حين ذهب بعض الفقه إلى أن المشاعات العالمية تشمل المياه الدولية والفضاء الجوي والفضاء الخارجي وأيضًا الفضاء السيبراني مما يجعله غير قابل للتملك (وزارة الدفاع الأمريكية،2005). وهذا ليس بالأمر الغريب فهو استنتاج قانوني متعارف عليه منذ القدم؛ تاريخياً، فقد اعتبر الفقه الروماني(2023)Ferrándiz, Emilia أن البحر والهواء غير قابلين للتملك وغير خاضعين للحكم.

وبعد سقوط الإمبراطورية الرومانية، حاولت دول وقوى مختلفة فرض سيطرتها على البحار بدوافع تجارية وأمنية ومالية، مما أدى إلى قرون من الجدل الفقهي بين مبدأ البحر المغلق ومبدأ البحر المفتوح.

وفي نهاية المطاف انتهى الأمر إلى استقرار أغلب الفقه على أن للدول حق تنظيم الأنشطة في البحار القريبة من سواحلها، خصوصاً ضمن نطاق تأثير المدفع الساحلي (عبد الجليل (2026)). وقد انعكس هذا المفهوم في المادة 2 من اتفاقية جنيف لأعالي البحار لعام 1958، وكذلك في المواد 87 و89 و139 من اتفاقية الأمم المتحدة لقانون البحار (UNCLOS) غير أن أنظمة المشاعات العالمية الحديثة لا تقوم على استحالة ممارسة السيطرة، بل على خيار قانوني—سياسي تتخلى بموجبه الدول عن ادعاء الملكية الحصرية، وتوافق على ممارسة سلطتها بشكل متزامن مع غيرها ((Vattel (1777,p125)).

وبالتالي، فإن مفهوم المشاعات العالمية ليس مفهوماً معادياً للسيادة، بل هو بناء قانوني—سياسي قائم على التعاون بين الدول والرضا المتبادل[1]. وهكذا باعتبار أن مبدأ التقييد الذاتي يُعد تعبيراً عن السيادة

Tsagourias,N & Buchan, R (2021, p. 30)

لذا فإن الدول قد تتفق في نهاية مواقفها القانونية على اعتبار الفضاء السيبراني "مشاعاً عالميًا" ومع ذلك، في المرحلة الراهنة نستبعد ذلك، إذ لا يوجد دافع سياسي أو قانوني للاعتراف بذلك؛ وبالتالي؛ السؤال الجوهري في هذا الصدد والذي يتطلب إجابة يتقرر فيما إذا كان الفضاء السيبراني ,Hardin,G(1968,p48) يُظهر فعلاً الخصائص التقليدية للمشاعات العالمية (الغزير، 2025)

ثمة اختلاف رئيسي بشأن المشاعات العالمية؛ في أن أعالي البحار والفضاء الخارجي والقارة القطبية الجنوبية، بخلاف الفضاء السيبراني، تمتلك جميعها بعداً مادياً يمكن استغلاله لاستخراج الموارد الطبيعية، في حين أن الموارد السيبرانية هي كيانات من صنع الإنسان لا توجد طبيعياً ولا يمكن استخراجها إلا تقنياً؛ **هذا أولًا**.

ثانيًا: الطبقات الاجتماعية والمادية للفضاء السيبراني تقع بالضرورة داخل حدود الدول، وبالتالي ضمن سلطتها، وهو ما يستلزم استبعاداً جزئياً لهذه السلطة,(2021) Tsagourias, N . باعتبار أن الفضاء السيبراني لا يوجد بشكل مستقل عن العالم المادي، بل هو متجذر فيه,**Buchan, R(2019)** .

ثالثاً، بينما تتسم المشاعات العالمية بأنها غير قابلة للاستبعاد، بمعنى أنه لا يمكن منع الآخرين من استخدامها، فإن كون البنية التحتية السيبرانية مملوكة للدول أو كيانات خاصة يجعل من الممكن عملياً استبعاد الآخرين منها.**Buchan, R(2019)**

[1] صدر حكم المحكمة الدائمة للعدل الدولية في قضية السفينة "ويمبلدون" (بريطانيا وفرنسا وإيطاليا واليابان ضد ألمانيا) في 17 أغسطس 1923، وقررت المحكمة أن رفض ألمانيا مرور السفينة المحملة بمعدات عسكرية إلى بولندا عبر قناة كيل يمثل انتهاكاً لمعاهدة فرساي، مؤكدة أن المعاهدات الدولية تعلو على قوانين الحياد الوطنية. وقد أرست المحكمة مبدأً قانونيًا عندما اعتبرت أن قبول الدولة بالالتزامات عبر المعاهدات الدولية لا يمثل تقييداً غير مقبول لسيادتها بل هو مظهر من مظاهر السيادة نفسها. https://www.scribd.com/document/247836020/Case-of-the-Ss-Wimbledon-Ft

رابعاً؛ الطبقة المادية للفضاء السيبراني مملوكة في الغالب للقطاع الخاص، وبالتالي يتطلب نزع الملكية عنه محمود، (2026)، وهو ما يمثل إشكالاً يتجاوز الإطار القانوني وحده.

من جهة أخرى يرى بعض الفقهاء، انطلاقاً من البعد الافتراضي للفضاء السيبراني، أن الدول غالباً لا تمتلك القدرة الكاملة على السيطرة على حدودها السيبرانية أو تحديد الفاعلين بدقة، وبالتالي—وبالاستلهام من مبدأ حرية البحار—ينبغي أن يبقى الفضاء السيبراني؛ من حيث أنه بيئة اصطناعية في مفهومه، وإن كان يتسم بعدم التحديد المكاني والانتشار وإمكانية إخفاء الهوية، فإن ذلك لا ينفي أنه يظل انعكاساً لكيانات وأشخاص ماديين يمكن التحكم بهم. ومن ثم، فإنه أقرب إلى مشاع غير مكتمل2 أكثر من كونه مشاعاً عالمياً كاملاً.

بناءً عليه؛ إقليم الفضاء السيبراني للدولة معترف به؛ ويظهر من خلال سلطة الدولة في نطاقه التي تُقرها القرارات والمواثيق الدولية؛ باعتبار

أن: "الإقليم هو أحد أوجه السيادة، وهو محمي بها، لكنه ليس مرادفاً لها. وبذلك "الفضاء السيبراني وعاء للسيادة، إذ أن السيادة في نطاقه بوصفها سلطة وقدرة يمكن أن تمتد خارج حدود الإقليم.(2015) Tsaugourias, N

في أكثر استخداماته شيوعاً، يشير مصطلح (السيادة) بمعناه الشامل إلى مجموعة الحقوق التي تمتلكها الدولة، بما يشمل قدرتها ككيان مخول بممارسة السيطرة على مجتمعها الإقليمي ,James Crawford (2019)، بما في ذلك قدرتها على تنظيم حركة العبور عبر الحدود – على المجتمع الإقليمي –؛ Krasner (2010 وكذلك قدرتها بالتصرف على الصعيد الدولي وتمثيل ذلك الإقليم وسكانه ,James Crawford (2019)

لذا يُقر البعض بأن السيادة تعني "الاستقلال"؛ استقلال خارجي فيما يتعلق بحرية التصرف خارج الحدود، واستقلال داخلي فيما يتعلق بحرية تصرف الدولة داخل حدودها، مؤكداً بذلك البعد الإقليمي القوي للسيادة في القانون الدولي **حمد قدوره (2020)**،

ومع ذلك، فإن هذه الحدود ليست مجرد بناء جغرافي أو مادي، بل هي بناء قانوني وسياسي: يتعلق بتنظيم الفضاءات لأغراض سياسية وقانونية ,Tsagourias, N(2021) ، أو بصياغة أخرى يتعلق الأمر بطريقة تنظيم سلطة الدولة[3]؛ كما الحال بشأن السيادة الخارجية؛ إذ تعني عدم الخضوع لسلطة خارجية؛ وهي أحد الأركان الأساسية لمفهوم السيادة، لكنها في الوقت نفسه ليست ادعاءً بالحرية المطلقة في التصرف تجاه الآخرين.

---

2 مصطلح استخدمه جولد سميت مستقبل القوة، The Future of Power Author(s): Joseph S. Nye, Jr. and Jack Landman Goldsmith ، Bulletin of the American Academy of Arts and Sciences, Vol. 64, No. 3 (SPRING 2011), pp. 45-52 (8 pages) ، https://www.jstor.org/stable/41149419?seq=1

[3] يشير TUOMAS FORSBERG و John Ruggie إلى أن الإقليمية ليست مجرد مساحة بل طريقة لتنظيم السلطة السياسية الحديثة عبر الفضاءات الإقليمية

بمعنٍ واسع، تُعد السيادة شرطاً مسبقاً لقيام الدولة ,ha Łukasz Kułaga(2024)، ونقطةً محورية في البناء القانوني الدستوري للدول،

كما أنها تُعد عنصراً مُكوِّناً للقانون الدولي ذاته، إذ توفّر في الوقت ذاته مبدأً تنظيمياً لما هو داخلي بالنسبة للدول وما هو خارجي بالنسبة لها.

ومع ذلك، فإن التوسع التنظيمي المتزايد للقانون الدولي، والذي يتجلى في التطور المتزامن لحماية حقوق الإنسان، يؤدي بشكل موضوعي إلى إخراج بعض الأنشطة من نطاق المجال المحجوز للدولة ,SCHRIJVE, NICO(2000) ، وبذلك مصطلح السيادة ذو طابع وصفي، يشير بمعنى شامل إلى مجموعة الحقوق التي تتمتع بها الدولة حتى في الفضاء السيبراني.

المطلب الثاني

السيادة السيبرانية مبدأ قانوني يُنتج التزامات قانونية

العديد من الإعلانات الصادرة عن الاتحاد الأوروبي[4]، والاتحاد الإفريقي[5]، وحلف الناتو[6]، ومنظمة الأمن والتعاون في أوروبا[7]، رفضت بشكل قاطع أي أطروحة تنكر السيادة في الفضاء السيبراني، مؤكدة أنه : لا توجد دولة تملك حرية مطلقة في الفضاء السيبراني[8] ، فقد جاء في تقرير فريق الخبراء الحكوميين لعام 2015 أن : "سيادة الدولة والمعايير والمبادئ الدولية الناشئة عن السيادة

---

[4] اعتمد مجلس الاتحاد الأوروبي في 20 نوفمبر 2017 استنتاجات بشأن البلاغ المشترك "المرونة والردع والدفاع: بناء أمن سيبراني قوي للاتحاد الأوروبي"، بهدف رفع جاهزية التكتل الأوروبي وتحسين قدرته المجمعة على الوقاية والكشف والرد على التهديدات السيبرانية المتصاعدة. الرابط: https://www.consilium.europa.eu/en/press/press-releases/2017/11/20/eu-to-beef-up-cybersecurity/

[5] اعتمد مجلس السلم والأمن التابع للاتحاد الإفريقي في 29 يناير 2024 وثيقة "الموقف الإفريقي المشترك." بشأن تطبيق القانون الدولي على استخدام تكنولوجيا المعلومات والاتصالات في الفضاء السيبراني"، تؤكد الوثيقة انطباق قواعد القانون الدولي وميثاق الأمم المتحدة على الفضاء السيبراني، وتشدد على التزام الدول بسلوك مسؤول، وحظر استخدام القوة، وتسوية النزاعات بالطرق السلمية. بشأن تطبيق القانون الدولي على استخدام تكنولوجيا المعلومات والاتصالات في الفضاء السيبراني". https://cyberlaw.ccdcoe.org/wiki/Common_position_of_the_African_Union_(2024)

6 منظمة حلف شمال الأطلسي (الناتو)، إعلان قمة ويلز، 5 سبتمبر 2014، الفقرة 72؛ (وليس 2015). وتتناول **الفقرة 72** من هذا الإعلان سياسة الدفاع السيبراني للحلف، حيث نصّت على إقرار "سياسة دفاع سيبراني معززة" لمواجهة التهديدات المتزايدة والمتطورة، مع التأكيد على أن الدفاع السيبراني يعد جزءاً أساسياً من مهام الدفاع الجماعي للحلف . https://assets.publishing.service.gov.uk/media/5a7ece9740f0b6230268baa1/Wales_Summit_Declaration.pdf

7 اعتمد المجلس الدائم لـ منظمة الأمن والتعاون في أوروبا القرار رقم 1202 في 10 مارس 2016، مضيفاً خمسة تدابير جديدة لبناء الثقة للحد من مخاطر النزاعات الناتجة عن استخدام تكنولوجيا المعلومات والاتصالات، استكمالاً للقرار السابق لعام 2013 عبر حماية البنى التحتية الحرجة وتعزيز الشراكات. https://ccdcoe.org/incyder-articles/osce-expands-its-list-of-confidence-building-measures-for-cyberspace-common-ground-on-critical-infrastructure-protection/

8 أكدت أستراليا في الجلسة الرابعة للفريق العامل المفتوح العضوية (مارس 2023) على انطباق القانون الدولي بالكامل في الفضاء السيبراني لتعزيز الاستقرار، ودعت إلى تعزيز المشاورات مع الخبراء الأكاديميين والممارسين. كما دعمت أستراليا

تنطبق على تصرفات الدول في الأنشطة المرتبطة بتقنيات المعلومات والاتصالات، وعلى اختصاصها بالبنية التحتية لتقنيات المعلومات والاتصالات

داخل أراضيها"[9]، وهو ما يؤكد أن هذا المبدأ يُعدُ قاعدة دولية أساسية[10] تنظم الفضاء السيبراني؛ والدلالة على ذلك، يمكن لنا ملاحظة أن ماورد في معظم أوراق المواقف الوطنية للدول [11] ما هو إلا اتجاهاً عاماً نحو إعادة تأكيد مبدأ السيادة بوصفه قاعدة دولية مُلزمة.

غير أنه في المقابل، يبرز موقف خاص في الورقة البريطانية[12]،الذي ترفض فيه المملكة المتحدة صراحةً فكرة وجود "سيادة مستقلة في الفضاء السيبراني"كقاعدة منفصلة في القانون الدولي العرفي، مؤكدةً أن السيادة مبدأ عام وليست قاعدة يمكن انتهاكها بشكل مستقل من خلال العمليات السيبرانية. وحجتها في ذلك أن (المفهوم العام للسيادة بحد ذاته لا يوفر أساساً كافياً أو واضحاً لاستخلاص قاعدة قانونية محددة للسيادة أو حظر إضافي للسلوك السيبراني يتجاوز قاعدة عدم التدخل)Jiarong Fu (2023) . ويقتصر هذا الرأي بشأن السيادة على كونها مبدأ سياسي؛ ولهذا مبدأ السيادة هو مبدأ قانوني مستقل بذاته ينطبق على الفضاء السيبراني ويُنتج آثاراً قانونية.,Tsagourias, N (2021)

إضافة إلى ذلك، قررت محكمة العدل الدولية أن القواعد العرفية يمكن استخلاصها[13] من المبادئ الأساسية

المقترحات الرامية إلى تعميق الفهم الموضوعي لتطبيق أطر القانون الدولي من خلال مشاركة الخبراء ، ص 1–2. https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/OEWG4_-_Australia_intervention_-_law

[9] تنص الفقرة 27 من تقرير فريق الخبراء الحكوميين لعام 2015) وثيقة الأمم المتحدة (A/70/174 المعني بالتطورات في مجال تكنولوجيا المعلومات والاتصالات في سياق الأمن الدولي، على أن سيادة الدول والأعراف والمبادئ الدولية المستمدة من السيادة تنطبق على أنشطة الدول المتعلقة بتكنولوجيا المعلومات والاتصالات وعلى ولايتها القضائية على البنية التحتية لتكنولوجيا المعلومات والاتصالات داخل أراضيها. https://digitallibrary.un.org/record/799853/files/A_70_174-EN.pdf

10 انظر: دليل تالين 2.0 هو مرجع أكاديمي غير ملزم صدر عام 2017 بإشراف مركز التميز التعاوني للدفاع السيبراني التابع لحلف الناتو(NATO CCDCOE) ، يحدد كيفية تطبيق القانون الدولي على العمليات السيبرانية في السلم وفي النزاعات المسلحة عبر 154 قاعدة. أوراق المواقف الوطنية لهذه الدول تتطابق أو تختلف معه بشأن السيادة وعدم التدخل. https://modeldiplomat.com/learn/glossary/tallinn-manual-2-0

11 دليل تالين 2.0، المرجع السابق ذكره.

[12] ترفض المملكة المتحدة صراحةً فكرة وجود "سيادة مستقلة في الفضاء السيبراني" كقاعدة منفصلة في القانون الدولي العرفي، مؤكدةً أن السيادة مبدأ عام وليست قاعدة يمكن انتهاكها بشكل مستقل من خلال العمليات السيبرانية.

13 قضية تعيين الحدود البحرية في خليج مين، توضح الفقرة 111 من حكم محكمة العدل الدولية لعام 1984 في قضية خليج مين أن القانون الدولي العرفي يتكون من معايير أساسية للتعايش وقواعد مستمدة من ممارسات الدول وقناعتها القانونية .وتؤكد الفقرة أن هذا القانون يمثل مبادئ توجيهية للتعاون الدولي وليس مجرد قواعد تفصيلية دقيقة لكل حالة. اقرأ نص الحكم الكامل على الرابط : https://www.icj-cij.org/node/103109

للنظام القانوني الدولي[14]، وباتباع المنهج الذي اعتمدته المحكمة في قضية نيكاراغوا15، يتضح أن مبدأ عدم التدخل ومبدأ السيادة لا يمكن فصلهما بشكل مستقر.

من جهة أخرى، و"بالنظر إلى أن من السيادة تنبثق مجموعة الحقوق التي تتمتع بها الدولة بصفتها دولة في مواجهة الدول الأخرى R (2021), Tsagourias,N & Buchan,؛ وأن "الواجب الأساسي المتمثل في عدم التدخل" يفترض منطقيًا ضرورةً وجود السيادة,(2015)MAFTE,J16والاستقلال Wheatley ، باعتبارهما مجموعتين متكاملتين من الحقوق والواجبات، رغم كونهما مستقلتين ذاتيًا في بنيتهما. وبناءً عليه، فإن موقف المملكة المتحدة، بصيغته المعروضة17، لا يمكن أن ينكر وجود السيادة في الفضاء السيبراني (2022)Visger, M، بل إنه اختيار سياسي يرفض تطبيقها في هذا الاتجاه Abaigeal Lorge(2025),

كما أيّد كورن وتايلور الرأي القائل بـ –السيادة كمبدأ–، حيث يريان أن "القانون الدولي، عبر كلاً من العرف والمعاهدات، يضع حظرًا واضحًا على الاستخدامات غير المشروعة للقوة، كما يحظر بعض أشكال التدخل بين الدول. وبينما تبقى أسئلة قائمة بشأن النطاق والحجم الدقيقين للآثار السيبرانية التي من شأنها أن تُخالف هذه القواعد الملزمة، يجب الاعتراف بأن هذه القواعد توفر إطارًا واضحًا إلى حد معقول لتقييم مشروعية أنشطة الدول في الفضاء السيبراني فوق هذه الاعتبارات، بما في ذلك خيارات الرد المتاحة للدول؛ أما دون هذه الاعتبارات، فلا يوجد دليل كافٍ سواء بشأن ممارسة الدول أو حتى لدعم القول بأن مبدأ السيادة يعمل كقاعدة مستقلة من قواعد القانون الدولي العرفي كتلك التي تنظم تصرفات الدول في الفضاء السيبراني".(2018)Gary Corn

وبدلاً من ذلك، يرى هذا الاتجاه أن "السيادة هي مبدأ أساسي في النظام الدولي الويستفالي؛ وهو يُشكّل الأساس للقواعد الملزمة ERIC. T. J(2018), لكنه لا يُنتج بذاته نتائج قانونية مُلزمة مباشرة في القانون الدولي،)(2018)p.208,Gary Corn

14 قاعدة حصانة الدولة تنبع من مبدأ المساواة السيادية بين الدول." محكمة العدل الدولية، قضية حصانات الدولة، ألمانيا ضد إيطاليا، 2012، الفقرة 57.

INTERNATIONAL COURT OF JUSTICE, Jurisdictional Immunities of the State (Germany v. Italy: Greece intervening)
https://www.icj-cij.org/case/143

15 قضية الأنشطة العسكرية وشبه العسكرية في نيكاراغوا وضدها، حكم محكمة العدل الدولية، 1986، حيث أكدت المحكمة أن مبدأ عدم التدخل جزء من القانون الدولي العرفي وأن احترام السيادة الإقليمية أساس العلاقات الدولية.

INTERNATIONAL COURT OF JUSTICE, Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America) https://www.icj-cij.org/case/70

16، السيادة والاستقلال «مترابطان جوهريًا مع الدولة ولا ينفصلان عنها

17 تؤطر المملكة المتحدة موقفها رسميًا على أنه تفسير قانوني دقيق. فمن خلال التأكيد على أن العملية السيبرانية لا تُعدّ انتهاكًا للقانون الدولي إلا إذا انتهكت قاعدة محددة – كحظر التدخل في الشؤون الداخلية للدول الأخرى – بدلًا من مفهوم غامض للسيادة السيبرانية الإقليمية، تسعى المملكة المتحدة إلى إنشاء إطار عمل أكثر قابلية للتنبؤ ومحدد قانونيًا لسلوك الدول في الفضاء الرقمي.

وبأن "الاختلاف في كيفية تجسّيد السيادة في القانون الدولي في مجالات الفضاء الجوي والفضاء .بل يوجّه تفاعلات الدول الخارجي والبحار يدعم أيضًا الرأي القائل بأن السيادة مبدأ مرن يخضع للتكييف حسب المجال والاعتبارات العملية للدول، وليس .كما أن "تعدد الأنظمة القانونية المنظمة للفضاء الجوي والفضاء الخارجي والمجال (2018) Gary Cornقاعدة جامدة ثابتة البحري يبرز خطأ افتراض وجود قاعدة عامة موحدة للسيادة قابلة للتطبيق المباشر على الفضاء السيبراني. فعلى سبيل المثال، في الفضاء الخارجي، تكون الأجسام المدارية خارج نطاق السيادة الإقليمية لأي دولة، ويكون الفضاء الخارجي متاحًا للاستخدام من جميع الدول. أما في المجال الجوي، فإن النظام القانوني شديد التقييد، بحيث يُعد أي دخول غير مصرح به إلى المجال الجوي لدولة أخرى انتهاكًا خطيرًا للقانون الدولي، مع استثناءات محدودة مثل الدفاع الشرعي أو تفويض مجلس الأمن أو القوة القاهرة. أما في المجال البحري، فإن العديد من أشكال المرور والدخول مسموح بها دون إذن الدولة الساحلية، ولكن مع وجود حالات يُعد فيها ذلك انتهاكًا للقانون الدولي، ويتوقف الأمر على الوقائع والظروف المحددة" Gary Corn((2018),

ويؤكد هذا الاتجاه أيضًا على أن "هذه هي النقطة التي ينهار عندها هذا الطرح، لأنه يفشل في إدراك أن كل النظم القانونية المشار إليها — الجوية والفضائية والبحرية، وكذلك النظام المنظم للتجسس — تقوم على مبدأ السلامة الإقليمية وعدم جواز انتهاك سيادة الإقليم"18 Schmitt & Vihul (2017

وبالتالي، وحتى يتم تطوير قواعد خاصة عرفية أو اتفاقية تنظم الفضاء السيبراني، فإن العمليات السيبرانية التي تنتهك سيادة الدولة الإقليمية تبقى محظورة بموجب القانون الدولي.

وكما أشار شميت وفيوهل، فإن "الأدلة على وجود القاعدة القانونية بهذا الشكل عديدة إلى درجة تجعل من ينكر عدم انطباقها على العمليات السيبرانية التي تظهر آثارها في إقليم دولة أخرى مُلزَمًا قانونًا بإثبات سبب عدم انطباقها، وهو ما لم يستطيع كلا منهم وفشل في القيام به، إذ يُستبدل ذلك بحجج سياسية وتحليلات عامة لمحاولة نقض مفهوم قانوني راسخ" Schmitt &Vihul ,,(2017)19 ؛ ويضيفان أن "تغيير القواعد يتطلب دعم الفاعلين الرئيسيين القادرين على تغيير النظام، وهو ما لن يحدث إلا إذا كانت البدائل المقترحة تقدم نتائج أفضل ,Stephen D. Krasner (2010)p98"

وبالنظر إلى قابلية تطبيق مبدأ السيادة في الفضاء السيبراني؛ باعتباره يفرض التزامات قانونية قائمة بذاتها Buchan& Navarrete (2021) P. 243,، يبقى السؤال المطروح بشأن بيان الحدود التي يُعتبر عندها هذا المبدأ منتهكًا.

---

18), Respect for Sovereignty in Cyberspace,,

دراسة تناقش جميع الأطر القانونية في المجالات الجوية والفضائية والبحرية وكذلك قانون التجسس تستند إلى مبدأ حرمة الإقليم وعدم قابليته للانتهاك.

https://centaur.reading.ac.uk/89703/8/Sovereignty%20Texas%20LR_removed.pdf

19 يؤكدان أن إنكار تطبيق مبدأ السيادة في الفضاء السيبراني غير مدعوم قانونيًا وأن عبء الإثبات يقع على من يدعي ذلك.

https://books.google.com.ly/books/about/Sovereignty.html?id=tHJ5m56sBX4C&redir_esc=y

وللإجابة عن هذا التساؤل تعددت الآراء المختلفة متضمنة تفسيرات متعددة، إلا أن معظمها20 تبنّى ما يُعرف بـ "معيار الحد الأدنى ,Buchan& Navarrete (2021) والذي يؤيد القاعدة رقم 4 في دليل تالين 2.0 بشأن تحديد حدود السيادة في الفضاء السيبراني21

وبحسب هولندا، ووفقًا لهذه القاعدة، يُعد انتهاك السيادة قائمًا إذا تحقق شرطان: الأول منهما؛ المساس بالسلامة الإقليمية للدولة المستهدفة. والشرط الثاني: التدخل في الوظائف الحكومية الأصيلة أو اغتصابها. غير أن التفسير الدقيق لهذه العوامل لا يزال محل جدل22

ومن جهة أخرى يتفق الموقف الالماني إلى حد كبير مع ما ورد في دليل تالين 2.0، من أن العمليات السيبرانية المنسوبة إلى دولة ما والتي تؤدي إلى آثار مادية وأضرار داخل إقليم دولة أخرى تُعد انتهاكًا لسيادة تلك الدولة الإقليمية23

ويقر الموقف الألماني أيضًا بأن "الآثار المادية البسيطة أو الإعاقات الوظيفية التي تقل عن حدود تأثير معينة لا يمكن، بمفردها، اعتبارها انتهاكًا للسيادة الإقليمية"24؛ كما أوضحت أن مجرد كون البنية التحتية متأثرة—خصوصًا إذا كانت بنية تحتية حرجة أو ذات أهمية عامة خاصة—قد يشير إلى احتمال وقوع انتهاك للسيادة[25]

كما أنه في الوقت ذاته لا يمكن أن يُعد ذلك انتهاكًا بحد ذاته، نظرًا لعدم وجود تعريفات دولية موحدة لهذه المفاهيم26

---

20 من بين دول أخرى: كندا، جمهورية التشيك، هولندا، المانيا، السويد، سويسرا.

21 القاعدة 4 - السيادة والحرمة وعدم القابلية للانتهاك: أي تدخل من دولة في البنية التحتية السيبرانية على متن منصة، أينما كانت، تتمتع بالحصانة السيادية، يشكل انتهاكًا للسيادة.

22 مملكة هولندا، ملحق: القانون الدولي في الفضاء السيبراني، ص 3: يوضح معايير انتهاك السيادة في العمليات السيبرانية
https://ceipfiles.s3.amazonaws.com/pdf/CyberNorms/LawStatements/Appendix_+International+Law+in+Cyberspace+(Statement+by+the+Nethe

23 الحكومة الاتحادية الألمانية، ورقة موقف بشأن تطبيق القانون الدولي في الفضاء السيبراني، مارس 2021، ص 4: تؤكد أن العمليات السيبرانية ذات الأثر المادي داخل إقليم دولة أخرى تُعد انتهاكًا للسيادة.
https://database.cyberpolicyportal.org/entity/pio8ogf79r?file=1659689750058j3zijc9a99.pdf&page=1

24 يؤكد أن الأضرار البسيطة أو غير الجوهرية لا تشكل انتهاكًا للسيادة (المرجع السابق ذكره)

25 يشير إلى أن استهداف البنية التحتية الحيوية قد يدل على احتمال وجود انتهاك لسيادة الدولة. (المرجع السابق ذكره)

26 الإقرار بعدم وجود تعريفات دولية موحدة للمفاهيم ذات الصلة. (المرجع السابق ذكره)

وفي هذا الاتجاه، تكمن الإشكالية الأولى في – معيار الحد الأدنى– من حيث أنه: بما أن أي اختراق غير سيبراني لا يتطلب فيه لإثبات انتهاك السيادة الإقليمية أن يُحدث آثارًا ضارة؛ وهو ما تؤكده ممارسات الدول على نطاق واسع27؛ فإنه لا يتضح لماذا ينبغي اعتبار العمليات السيبرانية، إذا كانت تتم عبر الوسائل الرقمية، متوافقة مع القانون الدولي، الأمر الذي يؤدي إلى منح البنية التحتية السيبرانية حماية أقل من الإقليم المادي للدولة Buchan& Navarrete (2021), p.248

فالسيادة تحمي جميع أوجه وجود الدولة، وبذلك "الضرر هنا هو ضرر معياري؛ أي ضرر يمس مبدأ السيادة والحقوق التي يحميها "Tsagourias, N (2021) ,

وقد أكدت محكمة التحكيم الدائمة في قضية لوتس أن "أول وأهم قيد يفرضه القانون الدولي على الدولة هو أنه — في غياب قاعدة تجيز خلاف ذلك — لا يجوز لها ممارسة سلطتها بأي شكل داخل إقليم دولة أخرى – دون أساس قانوني–" https://lawsforum.com/public-international-law/lotus-case-france-v-turkey-pcij-1927

ثانيًا، لا ينبغي اعتبار السيادة والحقوق السيادية مقتصرة على الوظائف الحكومية أو تعطيلها فقط، إذ أن أي عملية غير مصرح بها أو غير مبررة قانونيًا تتدخل في الحقوق السيادية للدولة قد تشكل انتهاكًا لمبدأ السيادة؛ بغضّ النظر عن درجة التدخل أو الضرر، وبغضّ النظر عما إذا كان ينتج آثارًا مادية أو غير مادية، أو ما إذا كانت العملية تستهدف الخدمات الحكومية والبنية التحتية أو لا

ثالثًا، وبصرف النظر عن غياب التوافق حول تعريف العديد من المصطلحات الأساسية للفضاء السيبراني بما فيها البنية التحتية الحرجة، وحتى مع افتراض وجود هذه التعريفات، فإن مفاهيم مثل البنية التحتية الحرجة، والخدمات الحكومية، والوظائف الحكومية بطبيعتها، أو مستوى الحماية لا يمكن أن تكون معيارًا أساسيًا لتوصيف انتهاك السيادة؛ لأنه في هذه الحالة سيتم إنشاء نطاقات وأشكال مختلفة من السيادة بناءً على اختلافات الدول في تنظيمها الداخلي، مما يؤدي إلى إضفاء الطابع الذاتي على السيادة في الفضاء السيبراني بدلًا من وضع معيار قانوني دولي موحّد.

وقد قدّمت أقلية من الدول (مثل فرنسا والاتحاد الأفريقي28 تصورًا أوسع لمبدأ السيادة – ما يُعرف بنهج الإضرار بالشخصية القانونية– حيث اعتُبر أن أي هجوم سيبراني ضد الأنظمة الرقمية الفرنسية أو أي آثار تُحدث داخل الأراضي الفرنسية بوسائل رقمية

---

27 من بينها: قضية سافاكار (1910–1911)، حادثة طائرة2–U(1960)، حادثة بويبل(1968) ، حادثة راينبو (1985)، وقمر كوزموس 954 (1978)

28 يؤكد الاتحاد الأفريقي أن أي وصول غير مصرح به من قبل دولة إلى البنية التحتية لتكنولوجيا المعلومات والاتصالات الموجودة على أراضي دولة أجنبية يعد غير قانوني. كما يؤكد أن الالتزام باحترام السيادة الإقليمية للدول في الفضاء السيبراني لا يتضمن حدود من الآثار الضارة أدنى منها لا يُعد الدخول غير المصرح به غير قانوني." الاتحاد الأفريقي، الموقف الأفريقي المشترك بشأن العديد تطبيق القانون الدولي على استخدام تكنولوجيا المعلومات والاتصالات في الفضاء السيبراني، 2024، الفقرة 16. https://cyberlaw.ccdcoe.org/wiki/Common_position_of_the_African_Union202)_(4

من قبل دولة أو من قبل أشخاص يعملون بتوجيه أو تحت سيطرة دولة، يشكّل انتهاكًا للسيادة وأن "خطورة انتهاك السيادة تُقيَّم على أساس كل حالة على حدة مع حماية الولاية السيبرانية للدولة ليس فقط عند وجود آثار، بل أيضًا عند وجود تدخل في أنظمة المعلومات الخاصة بها" https://dig.watch/updates/france-publishes-white-paper-application-international-law-cyberspace

من جهة أخرى قد يرى البعض أن غياب معيار الحد الأدنى قد يزيد من احتمالية النزاعات؛ إلا أن هذا الأمر محل جدل إذ يمكن القول أن قبول أي عملية سيبرانية عدائية تقع تحت حدود الضرر المادي أو لا تستهدف الخدمات الحكومية (البنية التحتية) لا تُعد فعلًا غير مشروع دوليًا، يعني عمليًا ترك مثل هذه العمليات دون تنظيم وتجريد الدولة المستهدفة من فرصة مهمة للمطالبة بحقوقه Tsaugourias, N (2015)p.23 ا، هو ما يزيد فعليًا من خطر النزاعات. وباستخدام كلمات محكمة العدل الدولية الدائمة، فإن سيادة الدولة تُنتهك كلما تمت ممارسة دولة أخرى سلطتها بأي شكل في إقليمها (دون موافقة صحيحة من تلك الدولة أو دون وجود قاعدة تجيز ذلك في القانون الدولي Roscini M(2024)p.393

المبحث الثاني

تأثير الهجمات السيبرانية على سيادة الدولة بموجب ميثاق الأمم المتحدة

من أهم المسائل القانونية ذات الصلة بالعمليات السيبرانية والأكثر حساسية ليس من الناحية السياسية فقط إنما من الناحية القانونية أيضًا؛ فيما يتعلق بالبيئة السيبرانية، تتمثل في تحديد معايير تتقرر من خلالها متى تنتهك العمليات ً السيبرانية سيادة دولة ما.

التعليق المفسر للقاعدة الرابعة من دليل تالين جاء فيه عن انتهاك سيادة الدولة بأنها مسألة «لا يجوز لأي دولة القيام بعمليات إلكترونية تنتهك سيادة دولة أخرى؛ وبالنظر إلى هذه القاعدة في سياق القانون الدولي الأوسع الذي ينظم أنشطة الدول الإلكترونية، فإنها تمثل الخط الفاصل الأهم بين السلوك المحظور والسلوك غير المحظور على المستوى الدولي؛ وتعود هذه الأهمية البالغة إلى أن القواعد الرئيسية الأخرى المعنية بسيادة الدولة من بينها قاعدة حظر التدخل –أنها تخضع أيَضا لأحكام لقانون دولي

بناءً على هذا الاستدلال؛ سنناقش التدخل السيبراني المحظور كمطلب أول؛ ومن ثم سنعرض نماذج للتدخلات السيبرانية التي أدت إلى تعطيل الوظائف وفقدانها للدولة المستهدفة (المطلب الثاني) ؛ وكليهما على التفصيل التالي:

المطلب الأول

التدخل السيبراني المحظور

https://cyberlaw.ccdcoe.org/wiki/Common_position_of_the_African_Union (2024)_

لم تستخدم مواد ميثاق الأمم المتحدة صراحةً مصطلح التدخل في أي موضع منه، باستثناء المادة الثانية الفقرة (7)29 ؛ وهذا النص الفقرة (7) من المادة الثانية المشار إليه ينطبق حصريًا على العلاقات بين أجهزة الأمم المتحدة والدول الأعضاء؛ ولا يمكن تفسيره بأنه تقنينًا للمبدأ العرفي (عدم التدخل) الذي يسري على العلاقات بين الدول Roscini, M,(2024),p100 ؛ غير أن نص المادة 78 من ميثاق الأمم المتحدة المشار إليه؛ في أحكامه ما يؤكد الاعتراف الضمني من الأمم المتحدة بمبدأ عدم التدخل الذي يتطلب أن تكون العلاقات قائمة على احترام مبدأ المساواة في السيادة" 30.

ومع ذلك، فإن إعلان الجمعية العامة لعام 1965 بشأن عدم جواز التدخل، وإعلان 1970 بشأن مبادئ القانون الدولي المتعلقة بالعلاقات الودية والتعاون بين الدول وفقًا لميثاق الأمم المتحدة (والذي يُعد تفسيرًا للميثاق من الجمعية العامة)، يقرران أن أي شكل من أشكال التدخل ... يُعد انتهاكًا لروح الميثاق ونصه Roscini, M,(2024.p121) .

وأكدت محكمة العدل الدولية في كل الأحوال أنه؛ لم يكن المقصود أبدًا أن يتضمن الميثاق تأكيدًا مكتوبًا لكل مبدأ أساسي من مبادئ القانون الدولي النافذ. إن وجود هذه المبادئ في القانون الدولي العرفي تأييدًا على وجودٍ راسخٍ وواسع النطاق في ممارسات الدول يؤكد مبدأ عدم التدخل CASE CONCERNING MILITARY AND PARAMILITARY ACTIVITIES IN AND AGAINST NICARAGUA(1986

وبهذا؛ بالنظر للطبيعة العرفية لمبدأ عدم التدخل، فإن معظم الفقهاء يشيرون إليه تقليديًا بوصفه كمبدأً وليس كقاعدة قانونية، مما أبقى مسألة تحديد ماهية التدخل المحظور بدقة؛ وكيف يختلف عن التدخل غير المحظور مسائل غير محسومة والدلالة على ذلك ما أشار إليه في أحكام محكمة العدل الدولية AFFAIRE DU DETROIT DE CORFOU (1949) بأنه عندما لا تتفق الدول بسبب تباين مواقفها حول مسائل جوهرية تتطلب في جميع الأحوال نوعًا من الإرشاد، فإن النتيجة غالبًا تكون صياغة مبادئ عامة.

وبناءً على ذلك، ونظرًا للغموض الذي يُلازم هذا المبدأ، لا شيء يمنعه من أن يُفسَّر وفق ثنائية الحق والواجب: أي أنه يتضمن حق كل دولة في إدارة شؤونها الداخلية دون تدخل خارجي، ويقابله واجب الدول الأخرى بالامتناع عن مثل هذا التدخل؛ بمعنى: يشمل الحق (السلبي) لكل دولة في إدارة شؤونها الداخلية دون تدخل خارجي، وما يقابله من واجب (إيجابي) على الدول الأخرى

---

29 وتنص هذه المادة على أنه " ليس في هذا الميثاق ما يسوغ "للأمم المتحدة" أن تتدخل في الشؤون التي تكون من صميم السلطان الداخلي لدولة ما، وليس فيه ما يقتضي الأعضاء أن يعرضوا مثل هذه المسائل لأن تحل بحكم هذا الميثاق، على أن هذا المبدأ لا يخلّ بتطبيق تدابير القمع الواردة في الفصل السابع.

30 "لا يطبق نظام الوصاية على الأقاليم التي أصبحت أعضاء في هيئة "الأمم المتحدة" إذ العلاقات بين أعضاء هذه الهيئة يجب أن تقوم على احترام مبدأ المساواة في السيادة".https://www.un.org/ar/about-us/un-charter/chapter-12

بالامتناع عن مثل هذا التدخل القسري Roscini, M,(2024.p121), وفقًا لما تم بيانه، فإن ما يميز مجرد التدخل غير المحظور عن التدخل المحظور هو، من جهة، انصراف الفعل إلى مسائل تكون الدول، وفقاً للقانون الدولي، حرة في اتخاذ القرار بشأنها Roscini, M,(2024.p162), ومن جهة أخرى، عنصر الإكراه. هو الإكراه (الدكتاتوري والقسري) ومحاولة تحديده وتوصيفه علمياً، إلى جانب إشكاليات الإكراه الاقتصادي والدبلوماسي هو ما يُقصد به التدخل السيبراني المحظور.

وبالتالي ينطبق عدم التدخل ويكتسب معناه عند وجود عبور فعلي للحدود أو تدخل في الجوانب الداخلية للسيادة ، وبهذا المعنى تبين الحدود ما يقع ضمن سيادة الدولة وما يقع خارجها؛ وهو أمر بالغ الأهمية أيضًا في تحديد ما هو محظور وغير محظور من التدخل ؛ لعل الإجابة عن ذلك – التدخل السيبراني في سيادة الدولة- تظهر في نص المادة 51 من دليل تالين بأن يحدث انتهاك السيادة كلما عبرت دولة ما فعليًا إلى أراضي دولة أخرى أو مجالها الجوي الوطني دون موافقتها أو أي مبرر أخر في القانون الدولي.

وبذلك حظر التدخل السيبراني تأتي أحكامه في ذات الاتجاه من حيث أنه تدخل استبدادي أو قسري المعروف ب (الإكراه)؛ غير أنه يتم بواسطة وسائل سيبرانية في مسائل تكون الدولة حرة في تقريرها بموجب القانون الدولي – فقد جرى تنظيمه استناداً إلى موضوع التدخل وغايته أكثر من اعتماده على الوسيلة المستخدمة أو الهدف المستهدف أو حجم الدمار الناتج عنه

بمعنى؛ كيفية تطبيق مبدأ عدم التدخل المستقر في القانون الدولي التقليدي على الأنشطة السيبرانية التي ترعاها الدول في وقت السلم تأتي في إطار الأحكام الآتية؛ الإكراه، وانتهاك المجال المحفوظ للدولة، والعمليات السيبرانية منخفضة الكثافة Gill,T(2013 .

أما الإكراه :يُقصد منه لكي تشكل العملية السيبرانية خرقاً لمبدأ عدم التدخل، يجب أن تتضمن عنصر إكراه الدولة الضحية على إتيان أو الامتناع عن فعل؛ بمعنى أن يكون الهدف من العملية السيبرانية فرض إرادة دولة ما على خيارات دولة أخرى.

في حين المجال المحفوظ؛ يُفسر على أنه يجب أن يستهدف التدخل السيبراني الخيارات السيادية البحتة للدولة الضحية؛ كما في حالة التدخل في نظامها السياسي أو الاقتصادي أو حتى الثقافي أو تنظيم انتخاباتها . أما العمليات السيبرانية منخفضة الكثافة؛ هي تلك العمليات التي من أمثلتها التجسس السيبراني وقت السلم أو العمليات التخريبية البسيطة؛ والتي قد لا تصل دائماً إلى حدود الإكراه؛ الذي يُفسر بأنه تدخل محظور" قانوناً بموجب المفهوم الضيق لعدم التدخل، ما لم تتدخل تلك العمليات مباشرة في قدرة الدولة على ممارسة وظائفها السيادية الأساسية أو تُعطل بنيتها التحتية الحيوية بشكل قسري.

نستنتج مما تقدم ؛ أن تطور التقنيات الرقمية المتقدمة منح الدول فرصاً أكبر لممارسة النفوذ خارج حدودها والتدخل في شؤون دول أخرى (حكومة مملكة هولندا، ملحق: القانون الدولي في الفضاء السيبراني، ص3)، كما أن "حظر التدخل يُعد ذا أهمية خاصة في سياق الفضاء السيبراني"(مجلس السلم والأمن التابع للاتحاد الإفريقي)، بالنظر إلى أن "الدول لا تحتاج إلى أدوات قسرية للتأثير بشكل غير مشروع وجوهري على مجال الاختصاص المحجوز لدولة أخرى" **Kilovaty.I) (2021)** .

من جهة أخرى؛ يمكن تتبع اتجاه واسع في الفقه الدولي مفاده؛ أن قاعدة القانون الدولي العرفي التي تحظر التدخل تنطبق كذلك حتى على الأنشطة السيبرانية(justsecurity) ؛ وإن كانت الحدود الدقيقة وتطبيق هذا الحظر Schmitt, M.(2017.p12) لم تتبلور بالكامل بعد(**National position of Slovenia (2026)**)

ومن منظور النصوص القانونية؛ فإن صياغة مبدأ عدم التدخل الواردة في ميثاق منظمة الدول الأمريكية؛ المادة 19 منه لا تحظر فقط استخدام القوة المسلحة، بل أيضاً أي شكل آخر من أشكال التدخل أو التهديد ضد شخصية الدولة أو ضد عناصرها السياسية والاقتصادية والثقافية CHARTER OF THE ORGANIZATION OF AMERICAN STATES- 19

وقراري الجمعية العامة United Nations General Assembly 2131 [31]وأيضًا 2625[32]، ووثيقة هلسنكي الختامية[33]، تتسم بالاتساع بما يكفي للسماح بتطبيقه في الفضاء السيبراني من خلال التفسير التطوري للمبدأ Roscini, M,(2024)

وبهذا؛ في المجال السيبراني أيضاً، العاملين اللذين يميزان بين التدخل المسموح به والتدخل غير المسموح به هما: (1) عنصر الإكراه، و(2) (الحصانة السيادية)؛ وكليهما يتقرر في المسائل التي تكون الدولة حرة في اختيارها وفقاً للقانون الدولي. وفيما يتعلق بالعامل الأول وهو الإكراه، فإن ما تم بيانه بشأن الإكراه القسري والدكتاتوري ينطبق على المجال السيبراني.

أما مفهوم المسائل التي تكون الدولة، وفقاً للقانون الدولي، حرة في اختيارها؛ فهي مرادفة لاختصاصها الداخلي CASE CONCERNING MILITARY AND PARAMILITARY ACTIVITIES IN AND AGAINST NICARAGUA(1986.paragraph205، أي المسائل التي لا يقيّدها لا القانون العرفي الدولي، ولا تلك المسائل التي لم تقم الدولة بتقييدها ذاتياً بموجب معاهدات دولية,(Roscini, M,(2024.p381 .

نستنتج من ذلك أن انتهاك مبدأ عدم التدخل قد لا يقع حتى في حال ممارسة الإكراه بشأن وظيفة حكومية بطبيعتها للدولة المستهدفة، إذا كانت تلك الوظيفة لم تعد داخلة ضمن اختصاصها الداخلي. وكذلك العمليات التي تُحدث فقداناً للوظائف أو تعطلاً؛ أو تلك العمليات المصممة لإحداث أضرار مادية و/أو إصابة أو وفاة أشخاص فهي تعرف أيضًا تُعرف بالتدخل غير المسموح به أو المحظور كقاعدة عامة.

بناءً عليه؛ التدخل المحظور المنفذ بوسائل سيبرانية أيضًا يتمثل في العمليات المصممة لإحداث أضرار مادية وإصابة أو وفاة أشخاص؛ حتى في حالة القوة المسلحة لكونها ليست سوى شكل متطرف من أشكال التدخل، ولذلك فإن هذه العمليات لا تنتهك

[31] قرار الجمعية العامة للأمم المتحدة رقم 2131 (د20) المؤرخ في 21 ديسمبر 1965 بشأن إعلان عدم جواز التدخل في الشؤون الداخلية للدول وحماية استقلالها وسيادتها. https://legal.un.org/avl/pdf/ha/ga_2131-xx/ga_2131-xx_a.pdf

[32] قرار الجمعية العامة للأمم المتحدة رقم 2625 (د-25)، الصادر في 24 أكتوبر 1970 بشأن اعلان مبادئ القانون الدولي المتعلقة بالعلاقات الودية والتعاون بين الدول وفقا لميثاق الامم المتعدة. https://docs.un.org/ar/a/res/2625(xxv)

[33] **وثيقة هلسنكي الختامية** هي اتفاقية سياسية وُقِّعت في مدينة هلسنكي بفنلندا يوم 1 أغسطس 1975 في ختام مؤتمر الأمن والتعاون في أوروبا؛ أول محاور هذه الوثيقة لتنظيم العلاقات الدولية يتقرر في مبادئ السيادة، واحترام الحدود القائمة، وعدم استخدام القوة أو التهديد بها. https://en.wikipedia.org/wiki/Helsinki_Accords

فقط حظر استخدام القوة المنصوص عليه في المادة 2(4) من ميثاق الأمم المتحدة، بل تشكل أيضاً انتهاكاً للمبدأ العام لعدم التدخل(Roscini, M,(2024.p386).

بناءً عليه؛ التدخل المحظور المنفذ بوسائل سيبرانية أيضًا يتمثل في العمليات المصممة لإحداث أضرار مادية وإصابة أو وفاة أشخاص؛ حتى في حالة القوة المسلحة لكونها ليست سوى شكل متطرف من أشكال التدخل، ولذلك فإن هذه العمليات لا تنتهك فقط حظر استخدام القوة المنصوص عليه في المادة 2(4) من ميثاق الأمم المتحدة، بل تشكل أيضاً انتهاكاً للمبدأ العام لعدم التدخل.

على سبيل المثال، فيروس ستكسنت(Stuxnet) ، بغض النظر عن تكييفه القانوني كاستخدام محظور فإن كان الهدف منه إبطاء البرنامج النووي الإيراني تدريجياً وبشكل متواصل؛ وأيضًا كان القصُد منه إلحاق الضرر بأجهزة الطرد المركزي34 ؛ لاشك أن هذا الاستنتاج يجعل هذه العملية وفق معايير القانون الدولي تستوفي كلّاً من عنصر الاختصاص الداخلي المحفوظ وعنصر الإكراه القسري.

نستنتج من ذلك: أن المُلاحظ على العمليات السيبرانية التي تُحدث أو يُقصد بها إحداث أضرار مادية في أشياء مادية يمكن أن تُشكّل أيضاً تدخلاً دكتاتورياً عندما يُستخدم تهديد إحداث الضرر أو استمراره كوسيلة ضغط للحصول على تنازلات من الدولة المستهدفة,(2015)Alvarez,J . .

والجدير بالذكر في هذا الشأن؛ إن مبدأ عدم التدخل لا يحظر إلا الإكراه، أي التصرفات والسلوكيات غير الرضائية

Roscini, M,(2024.p171).

في حين المادة 2(4) من ميثاق الأمم المتحدة تحظر أيضاً استخدام القوة المسلحة حتى في الحالات التي يكون فيها الاستخدام برضا الدولة إذا كان غير متوافق مع أغراض ميثاق الأمم المتحدة(2024)Butchard,P .

لذا؛ القاعدة القانونية في هذا الشأن تتحدد في حالة ما كان الهجوم السيبراني لا يصل إلى حدود استخدام القوة المحظور، فإن رضا الدولة المستهدفة يجعل السلوك مشروعاً وفق أحكام القانون الدولي.

من جهة أخرى؛ التدخل السيبراني كما أشرنا يتمثل في العمليات الموجهة ضد الاختصاص المحفوظ للدولة والتي تؤدي إلى فقدان وظائف البنى التحتية ITALIAN POSITION PAPER ON 'INTERNATIONAL LAW AND CYBERSPACE'، مثل الهجمات السيبرانية التي تؤدي إلى تعطّل أنظمة الحاسوب في المستشفيات؛ تعطيل سلاسل الإمداد الخاصة بالقطاع الصحي؛ الأدوية الأساسية واللقاحات؛ التعليم ... الخ؛ بقصد التسبب في توقف سلسلة إمداد

[34] أصدر معهد العلوم والأمن الدولي (ISIS)في 22 ديسمبر 2010 تقريراً بارزاً حول فيروس "ستوكسنت(Stuxnet) "، خلص فيه إلى أن الهجوم السيبراني ربما أدى إلى تدمير نحو 1000 جهاز طرد مركزي في محطة ناتنز الإيرانية لتخصيب اليورانيوم بين أواخر 2009 وأوائل 2010. https://isis-online.org/isis-reports/stuxnet-malware-and-natanz-update-of-isis-december-22-2010-reportsupa-href1

الطاقة عن العمل (Chatham House, 19 May 2022) ؛ إضافة إلى التأثير على عمل البرلمان United Nations document A/76/136, issued on 13 July 2021؛ أو التسبب في فقدان وتعطيل وظائف البنك الوطني أو الاحتياطي الفيدرالي ,Moynihan. H(2019.P39) ؛ أو منع تقديم الإقرارات الضريبية عبر الإنترنت United The Republic of Poland's position on the application of international law in cyberspace؛ أو شلّ عمل شركة ذات أهمية نظامية Nations document A/76/136, issued on 13 July 2021,P88 أو السيطرة على نظام النقل في دولة أخرى أو إيقافه. وبالنظر إلى أن عنصر الإكراه في الحالات المعروضة يبدو بديهياً بذاته، فإن الأمثلة المقترحة تهدف أساساً إلى اغتصاب الاستقلال السياسي للدولة المستهدفة (Blay S. 2010)، بما يجسد جوهر القرارات 2131 و2625 المشار إليهما أعلاه.

المطلب الثاني

نماذج للتدخلات السيبرانية المحظورة في سيادة الدولة

التدخل عبر الفضاء السيبراني في إقليم الدولة المستهدفة تفسيراته القانونية تتحدد في إطار وجوب أن تُنتهك (على الأقل) السيادة الإقليمية لتلك الدولة، ويتوقف ذلك على أن تتسبب هذه العملية في آثار تتجاوز الحد الأدنى للتدخل القسري في شؤون دولة أخرى؛ وعادةً ما يشمل ذلك العمليات السيبرانية التي تتضمن إدخال البيانات أو تعديلها أو حذفها في الأنظمة السيبرانية للدولة المستهدفة؛ لذا من الأهمية بمكان أن نعرض بعض النماذج للتدخلات السيبرانية المحظورة لدولة ما في مصالح دولة أخرى؛ نذكر منها:

أولًا: التدخلات السيبرانية التي تهدف إلى التلاعب بالتصويت

تُعدّ مسألة شائعة (مواقف الدول) ولكنها تتطلب حذراً خاصاً تلك المتعلقة بالتدخلات السيبرانية التي تهدف إلى التلاعب بسلوك التصويت (وزارة الخارجية الإيطالية، الورقة الوطنية الإيطالية)

ويمكن تبني نهج مفيد عبر التمييز بين نوعين رئيسيين من العمليات:

عمليات التأثير السيبراني(Cyber influence operations ، أي عمليات تهدف إلى دفع الناخبين أو تثبيطهم عن التصويت؛

الهجمات السيبرانية على البنية الانتخابية(Cyberattacks against electoral infrastructure) ، أي عمليات تستهدف التلاعب بآلية الانتخابات أو تغيير نتائج الفرز .

وبالبدء بالنوع الثاني، فإن جوهر هذه الهجمات يتمثل في تقويض قدرة الدولة على إجراء انتخابات حرة ونزيهة، وبالتالي المساس باستقلالها(2023) International Law Commission ؛ ومن الأمثلة الواضحة على ذلك استخدام الوسائل السيبرانية لتلاعب في نتائج فرز الأصوات.

وبذلك؛ تعطيل آليات الانتخابات أو التسبب في تعطلها، أو حجب التصويت الإلكتروني، أو جعل من المستحيل على الناخبين في دائرة معينة الإدلاء بأصوات Schmitt, M (2020), ؛ أو تغيير وضع الناخبين في سجل الناخبين بحيث يُسجَّل صوتهم كصوت مؤقت فقط؛ أو حذف أسماء الناخبين من السجل الانتخابي؛ وما شابه ذلك.Schmidt, M (2018)

وقد اقترحت اللجنة العالمية لاستقرار الفضاء السيبراني (GCSC) اعتماد قاعدة خاصة لحماية البنى التحتية الانتخابية (الضرورية للانتخابات أو الاستفتاءات أو الاستطلاعات الشعبية) Moynihan, H(2019؛

من جهة أخرى وبشكل عام، يمكن ملاحظة وجود اتجاه واسع Global Commission on the Stability of Cyberspace (GCSC), بين فقهاء القانون الدولي مفاده؛ أن أي عملية سيبرانية تقوم بها دولة وتتدخل في قدرة دولة أخرى على إجراء انتخابات أو تتلاعب بنتائج الانتخابات تُعد انتهاكاً واضحاً لقاعدة عدم التدخل المعروفة في أحكام القانون الدولي JENSEN ,ERIC(2018)؛ باعتبار أن العنصر الأول المكوّن للتدخل في هذه الحالة هو انتهاك (المجال المحفوظ او المحمي او المحجوز للدولة) ؛ إذ يتحقق ذلك بوضوح في المجال الانتخابي لكونه من المسائل التي يتركها القانون الدولي للاختصاص الداخلي للدول؛ كما أيضًا يتحقق حتى في عنصر الإكراه (القسري) باعتبار أن هذه الأنشطة السيبرانية (التلاعب بالأصوات الانتخابية) تجعل من المستحيل –وفقًا للجانب الموضوعي– على الدولة ممارسة سياسة أو نشاط معين تُحقق بها سلامة العملية الانتخابية أو على أقل تقدير تجعل هذا الأمر أكثر صعوبة بشكل جوهري,(2020) Schmitt, M .

من جانب أخر من الأهمية بمكان في هذا الصدد التفطن إلى قاعدة غاية في الأهمية؛ بأنه ما من قيود ملزمة أو وجوب تحقق شروط تنص على أن يكون فعل الإكراه قد نجح فعلاً في إجبار الدولة المستهدفة على تغيير سلوكها، بمعنى: حتى محاولة التدخل الفاشلة في المجال المحفوظ أو المحجوز للدولة تُعد غير مشروعة في القانون الدولي COMMON AFRICAN

بناءً عليه؛ وإضافة إلى ما تقدم: يجب التنبه إلى أن وسائل وآليات عمليات التأثير السيبراني عديدة تلك التي يُقصد منها تدخل دولة ما في العملية الانتخابية هي تحت ولاية دولة أخرى، يمكن أن تشمل من بين هذه الوسائل والآليات – من بين أمور أخرى – حملات مدعومة من دول تستخدم روبوتات سياسية للتأثير على الرأي العام عشية الانتخابات الرئاسية Research Handbook on International Law and Cyberspace ؛ أو نشر رسائل مسربة وبريد إلكتروني (وبشكل عام بيانات) تخص أحد المرشحين بهدف تقويضه.

بل أن البعض يرى من بين وسائل عمليات التأثير السيبراني على الانتخابات توصف حتى في حالة الأنشطة والعمليات التي تحرم الناخبين، أو عدداً كبيراً من الأفراد، من المعلومات ذات الصلة بالانتخابات.(2020)Schmidt M

وتُصنَّف هذه العمليات أو الأنشطة؛ باعتبارها تهدف إلى التأثير في العملية الانتخابية خارج البنية التحتية للدولة المستهدفة نفسها، إلى عمليات كشف البيانات ؛ كما في حالة اختراق ونشر معلومات غير متاحة للعامة، وكذلك تصنف أيضًا إلى عمليات القصد منها تضليل المعلومات وتنقسَّم بدورها إلى عمليات التضليل المعلوماتي الجزئي؛ وتتحقق في حالة نشر معلومات سرية صحيحة دون إذن؛ – وعمليات أخرى تُعرف بالتضليل المعلوماتي الكامل؛ ومن أمثلتها نشر أخبار كاذبة أو غير دقيقة؛ بالنسبة للاتحاد الأوروبي، التضليل المعلوماتي هو تصنيع أو تشويه متعمد للمحتوى الإعلامي بهدف الخداع (European Commission, p2018, p. 10).

ولمناقشة مسألة عمليات الكشف عن البيانات وحملات التضليل في العملية الانتخابية نشير إلى الحالات الآتية:

تدخل في الانتخابات الأمريكية لعام 2016 :

وتتلخص هذه العملية أنه في أعقاب الانتخابات الرئاسية لعام 2016، اتهم مسؤولون في الإدارة المنتهية ولايتها، بمن فيهم الرئيس باراك أوباما وكبار قادة الاستخبارات الأمريكية، الحكومة الروسية بالتدخل في الانتخابات الأمريكية(2018) Schmidt, M .

ووفقاً لملخص تقرير سري حول الحملة أعدته وكالة الاستخبارات المركزية (CIA) ومكتب التحقيقات الفيدرالي (FBI) ووكالة الأمن القومي (NSA) تحت إشراف مدير الاستخبارات الوطنية(ODNI) ، الرئيس الروسي فلاديمير بوتين أمر بحملة تأثير في عام 2016 استهدفت الانتخابات الرئاسية الأمريكية؛ وقد هدفت روسيا من ذلك تقويض ثقة الجمهور في العملية الديمقراطية الأمريكية، وتشويه صورة وزيرة الخارجية كلينتون، والإضرار بفرصها الانتخابية ورئاستها المحتملة للولايات المتحدة الأمريكية إشارة واضحة لتفضيل للرئيس المنتخب Office of the Director of National Intelligence Background Report.

أيضاً بوتين والحكومة الروسية سعيا إلى دعم فرص الرئيس المنتخب ترامب في الفوز عندما أمكن ذلك، من خلال تشويه سمعة وزيرة الخارجية كلينتون ومقارنتها بشكل سلبي علني مع ترامب Office of the Director of National Intelligence Background Report.

ووفقاً للتقرير، فإن حملة التأثير السيبراني الروسية، التي تمت الموافقة عليها من أعلى مستويات الحكومة الروسية، كانت متعددة الأوجه. ومن حيث المسؤولية القانونية الروسية، فإن العنصر الأكثر أهمية يتعلق بالفعل.

وقد نفذت هذه العمليات من قبل الاستخبارات العسكرية الروسية التابعة لهيئة الأركان العامة. حيث قامت باختراق حسابات البريد الإلكتروني الخاصة بمسؤولي الحزب الديمقراطي وشخصيات سياسية أخرى، واستخرجت كمية كبيرة من البيانات من اللجنة الوطنية الديمقراطية في مارس 2016. وتم استخدام موقع DCLeaks.com ومنصة WikiLeaks لنشر هذه المواد، بما في ذلك عبر تسريبات حصرية لوسائل الإعلام.

وخلال هذه الفترة، كانت هناك أيضاً حملة دعائية روسية نشطة شملت العديد من وسائل الإعلام إلا أن الأكثر أهمية من الناحية القانونية؛ من هذا الشكل التقليدي من الدعاية السياسية؛ كانت أنشطة وسائل التواصل الاجتماعي التي نفذها ما يشبه الذباب الإلكتروني الحكومي، والتي عملت على تضخيم أخبار الفضائح المتعلقة بالمرشحة هيلاري كلينتون ودور ويكيليكس في الحملة الانتخابية. كما أن مزرعة المتصيدين التي ضمت أكثر من تسعين متصيداً قامت بشراء إعلانات مضادة لكلينتون ومؤيدة لترامب على منصات التواصل الاجتماعي مثل تويتر وفيسبوك وإنستغرام. ومن خلال أكثر من 120 مجموعة وحساباً، لم يكن الهدف فقط التأثير على اختيار الناخبين، بل أيضاً تثبيط بعضهم عن الذهاب إلى صناديق الاقتراع(2018) Schmidt, M .

نستنتج من العرض السابق من خلال تفسير الأحداث المشار إليها؛ أن التصرفات الروسية في هذه العملية استوفت الشرط الأول للتدخل غير المشروع من خلال استهداف عملية الانتخابات نفسها,(2019).Tsagourias, N ؛ أما فيما يتعلق بشرط الإكراه، فقد قدم الفقهاء آراء مختلفة، لكنها تتفق جميعاً على أن التأثير في القدرة على اتخاذ القرار الحر يعني إخضاع الإرادة السيادية وتقليص السلامة السياسية للدولة المستهدفة.

ويتفق بعض الفقه على هذا الاستدلال بأن "العمل القسري في جوهره يهدف إلى إجبار الدولة على اتخاذ قرار لم تكن لتتخذه في الظروف العادية، أو منعها من القيام بعمل كانت ستقوم به؛ ويمكن القول أن الطبيعة السرية لعمليات المتصيدين الإلكترونيين حرمت الناخب الأمريكي من حرية الاختيار من خلال خلق وضع لم يتمكن فيه هذا الناخب من تقييم المعلومات المقدمة له بشكل عادل؛ وبما أن الناخبين لم يكونوا على علم بأنهم يتعرضون للتلاعب من قبل قوة أجنبية، فإن عملية اتخاذ القرار لديهم، وبالتالي قدرتهم على التحكم في نظام الحكم، قد ضعفت وتشوهت.

وبذلك الطبيعة الخادعة لهذه العمليات هي ما يميزها عن مجرد عمليات التأثير؛ إذ أن اختراق البيانات وتسريبها تشوّه العملية الانتخابية من خلال إدخال معلومات تم الحصول عليها بطرق محظورة صراحةً في القانون الداخلي الأمريكي وهي قواعد موثقة في معظم قوانين دول أخرى، وبالتالي يمكن القول أنه اختراق غير مشروع للبيانات الخاصة؛ الأمر الذي نتج عنه تقويض حرية الاختيار لدى الناخبين؛ بمعنى: في حالة الانتخابات، هذا النوع من الاختراقات قد يؤدي إلى انتخاب مرشح لم يكن ليفوز لولا ذلك الاختراق غير المشروع للبيانات Schmidt, M (2018)

نضيف إلى ما تقدم ما جاء عن الفقيه شميت في تفسير هكذا حالات بأنه: "قد يكون من الممكن الاتفاق على بعض العوامل غير الحصرية التي تؤثر في تصنيف العملية المعلوماتية الأجنبية خلال الانتخابات على أنها قسرية أو لا. ويبدو أن نطاق العملية وتأثيراتها من العوامل المهمة للغاية. حيث يشمل ذلك مدى انتشار التدخل في الانتخابات، ومدى خطورته، وربما طبيعة وأهمية الانتخابات نفسها فيما كانت محلية أم وطنية على مستوى الدولة كالانتخابات الرئاسية؛ ومن العوامل الأخرى التي قد تؤثر في التقييم هي مدى صدق المعلومات محل النزاع؛ وبالتالي يبدو أنه من الأسهل اعتبار حملات التضليل ذات طابع قسري" Schmitt, M (2020),

بناءً عليه؛ يترتب على الرأي السابق أن كل دولة تتمتع بالحق في الاستقلال، وبالتالي ممارسة اختيارها

بحرية ودون أي إملاءات من أي دولة أخرى(2023) International Law Commission لكونه يقع في نطاق المجال المحجوز للدولة ضمن سلامة إرادتها السياسية المبنية على حرية التصرف؛ وهو ما يُقصد بمبدأ عدم التدخل في شأن حماية اختيارات الدولة التي تقع ضمن نطاق اختصاصها الداخلي؛ إذ أن الفهم التقليدي لدى الدول لمفهوم مبدأ التدخل يركز على المظهر الداخلي وحتى الخارجي لممارسة الدولة لسلطاتها التي تمثلها الحكومة، دون أن يأخذ بعين الاعتبار كيفية تكوّن هذه السلطة والإرادة، أو كيف يمكن للتدخل أن يؤثر في عملية تكوينهما(2020).Tsagourias, N

استدلالاً على صحة هذا الرأي؛ أولًا: قد يتمثل التدخل القسري المحظور في عملية تجعل مواقع الإنترنت والحسابات على شبكات التواصل الاجتماعي الخاصة بمرشح سياسي وحزبه غير قابلة للوصول طوال السنة السابقة للانتخابات، أو التي تعمد إلى تعطيل بث خطاباته ومقابلاته بشكل منهجي عبر التلفاز؛ ففي هكذا حالة لا يقوم الحظر على مجرد تقييد الوصول إلى المعلومات الموثوقة حول المرشحين أو القضايا، وهو أمر يبدو أساسياً لضمان أن تكون الانتخابات ذات معنى، بل إن هذا السلوك يُعد تدخلاً محظوراً لأنه يقوّض بالقوة حق الدولة في إجراء انتخابات حرة ,Schmitt, M (2020).

ثانياً: حتى مع قبول هذا التوسع في نطاق الحماية التي يقرها مبدأ عدم التدخل، فإن التدخلات الروسية المفترضة التي أشرنا إليها يمكننا القول أنها تفتقر إلى عنصر الإكراه، لأنها لا تتجاوز كونها عمليات تأثير وإقناع (Tallinn Experts Group, p318) ؛ فالإكراه يعني الإلزام القسري أو الاستحواذ القهري على القرار؛ أما مجرد القول بأن إرادة الناخبين تم إضعافها وتشويهها ,Tsagourias, N.(2019)؛ فهو لا يرقى إلى مستوى من الضغط أو الشدة أو الحجم الكافي الذي يُمكن اعتباره إكراهاً بالمعنى القانوني.

بناءً عليه؛ يُقر البعض بوجود بعض الإشكاليات فيما يتعلق بشرط الإكراه ,Tsagourias, N.(2019) ؛ لذا يستلزم في هذا الشأن ضرورة إعادة النظر في ظاهرة التدخل بهدف وضعها في سياقها وإعادة صياغة مفهوم مبدأ عدم التدخل كما يجب أن يُطبق في الفضاء السيبراني؛ إذ أن معنى التدخل في القرن التاسع عشر لم يعُد بذات التوصيف، كما في التدخل العسكري أو الدبلوماسي أو السياسي أو القانوني ؛ إذ كلًا منهما قد تغيرت؛ لذا من غير المقبول إنكار القول بأن مبدأ عدم التدخل بمفهومه التقليدي يكتسب معناه ضمن بنية العلاقات السيادية من خلال حماية و سلامة واستقلال سلطة الدولة وإرادتها ضد أي تدخل خارجي؛ وبالتالي مبدأ عدم التدخل يركز على المظهر الداخلي و/أو الخارجي للسلطة والإرادة التي تمارسها الدولة ممثلةً في الحكومة. وبعبارة أخرى، فإنها تُسند جميع مظاهر السيادة والسلطة والإرادة إلى الحكومة، التي تُحمى بعد ذلك من التدخل، غير أنه لا يؤخذ في الاعتبار كيفية تشكّل هذه السلطة والإرادة، وكيف يمكن للتدخل أن يؤثر في عملية تكوينها. باعتبار أن سلطة الحكومة وإرادتها لا تبقى حرة إلا إذا كانت مصادر تكوينها هي أيضاً حرة.

من جهة أخرى معيار القانون الدولي الخاص بشأن مبدأ عدم التدخل ينطبق فقط على الأفعال ذات الطبيعة القسرية، مما يترك الأنشطة والعمليات المُعطِّلة لوظائف الدولة خارج نطاق التدخل المحظور. باعتبار عنصر الإكراه كشرط لوجود مبدأ عدم التدخل يبدو غير متوفرًا في حالة عمليات المعلومات؛ لذا أصبح لزامًا على القانون الدولي أن يتكيف مع العصر الرقمي حيث تُستخدم

المعلومات كسلاح باعتبارها انتهاكات لقاعدة أو مبدأ عدم التدخل ,Kilovaty,I(2018.p.147) ؛ من خلال إعادة تقييم تطبيق مبدأ عدم التدخل على الهجمات السيبرانية غير القسرية من الناحية التقنية ولكن عالية التأثير والتعطيل؛ إذ أن تحديد توافر عنصر الإكراه في الشأن مبني على معيار الأثار الناتجة عن الفعل ؛ وهو معيار يأخذ في الاعتبار ثلاثة عوامل: أهمية وعدد القيم المتأثرة، ومدى تأثر تلك القيم، وعدد المشاركين الذين تتأثر قيمهم. وبناءً عليه، في سياق الهجمات السيبرانية، يُفترض أن قاعدة عدم التدخل تُنتهك عندما يُحدث الهجوم تعطيلاً بدلاً من المفهوم التقليدي المتقادم ل الإكراه ,Kilovaty,I(2018.p.169) ؛ ويجد هذا الرأي مبرراته في بعض الأمثلة منها:

الفارق بين حجز شخص داخل غرفة تفسيره (تدخل قسري)، يتساوى هذا الاستنتاج مع تهديد هذا الشخص بالعنف إذا خرج (تدخل ديكتاتوري)، أو الادعاء زوراً بوجود إرهابي خارج الغرفة يرتدي حزاماً ناسفاً (تلاعب قسري بالمعلومات)، وبهذا في كل هذه الحالات الفرق ليس إلا فرقاً كمياً وليس نوعياً؛ بمعنى: في جميع الحالات سيبقى الشخص داخل الغرفة دون قدرة على اتخاذ قرار حر وواعٍ.

كما أن من هذا المنظور، يمكن اعتبار الكذب بشأن الوقائع بهدف دفع شخص ما إلى القيام بفعل أو الامتناع عنه بمثابة المكافئ الوظيفي لعنصر الإكراه؛ عندما يؤدي ذلك إلى ممارسة سيطرة على سلوك الضحية,(Roscini, M(2024. P.398.

والجدير بالذكر في هذا الصدد أن كل هذه الاستنتاجات مدعومة بمواقف بعض الدول؛ على سبيل المثال: موقف كوستاريكا التي قررت أن الإكراه يمكن أن يحدث إذا حرمت دولةٌ ما دولةً أخرى من القدرة على اتخاذ قرارات حرة ومبنية على معلومات صحيحة فيما يتعلق بشؤونها الداخلية أو الخارجية بما في ذلك من خلال نشر الأخبار الكاذبة35.

وكذلك الحال بالموقف الألماني الذي أشار إلى أنه؛ في سياق التدخل غير المشروع، يمكن—على سبيل المثال—تصور أن تقوم دولة، عبر نشر معلومات مضللة من خلال الإنترنت، بتحريض متعمد على اضطرابات سياسية عنيفة أو أعمال شغب ونزاعات

---

35 تطرح كوستاريكا من خلال هذا الموقف رؤية قانونية متقدمة لتفسير عنصر "**الإكراه (Coercion)** "في العصر الرقمي وفقاً للآتي:
إعادة تعريف الإكراه في البيئة الرقمية: في القانون الدولي التقليدي جاء عن (محكمة العدل الدولية في حكمها الشهير بشأن قضية *نيكاراغوا ضد* بأنه: يُشترط لتحقق التدخل غير المشروع أن ينطوي على عنصر إكراه، وعادة ما كان يُربط ذلك بالضغط العسكري 1986*الولايات المتحدة* عام أو الاقتصادي المباشر. لكن كوستاريكا جادلت بأن **الإكراه يمكن أن يتخذ أشكالاً حديثة** تشمل:

- حرمان الدولة المستهدفة من القدرة على اتخاذ قرارات حرة ومبنية على معلومات صحيحة.
- تلاعب دولة أخرى بالإرادة السياسية أو السيادية للدولة عبر وسائل سيبرانية أو إعلامية موجهة.

الموقف الوطني الرسمي لكوستاريكا الصادر عام 2023 بشأن تطبيق القانون الدولي في الفضاء السيبراني، وتحديداً القواعد المتعلقة بـ "**مبدأ عدم التدخل في الشؤون الداخلية للدول**" National position of Costa Rica (2023) (2023)_https://cyberlaw.ccdcoe.org/wiki/National_position_of_Costa_Rica

داخلية في دولة أجنبية، مما يعيق بشكل كبير إجراء الانتخابات بشكل منظم والإدلاء بالأصوات. وقد تكون هذه الأنشطة قابلة للمقارنة من حيث الحجم والأثر بدعم التمردات، وبالتالي قد تكون مماثلة للإكراه بالمعنى المذكور أعلاه36.

كما أكدت وجهة نظر فنلندا في هذا الشأن هذا الرأي؛ فقد جاء فيها بأن؛ التدخل العدائي بالوسائل السيبرانية يشكل أيضاً انتهاكاً للحظر العرفي لمبدأ عدم التدخل في الشؤون الداخلية لدولة أخرى، بشرط أن يتم بهدف إجبار أو إكراه تلك الدولة فيما يتعلق بشؤون تقع ضمن مجال اختصاصها الداخلي.

إن شرط الإكراه يستبعد الأشكال الأقل من التأثير والإقناع التي تعد شائعة في العلاقات الدولية. كما لا يوجد التزام مقابل مشتق من السيادة يفرض على الدول الأخرى الامتناع عن نشر المعلومات لتلك الدول، أو السماح لمواطنيها بذلك؛ ولكي ترقى العملية السيبرانية إلى تدخل محظور، يجب توافر العنصرين المعنية بتحقيق التدخل؛ وتظل معظم الإشكاليات المفتوحة مرتبطة بعنصر الإكراه وكيفية تجسده في العمليات السيبرانية. فعلى سبيل المثال، بينما يُعد إجراء الانتخابات من الشؤون الداخلية لكل دولة بلا جدال، فإن جميع أساليب التدخل الانتخابي لا تتضمن بالضرورة عنصر الإكراه؛ إلا أن اختراق قواعد بيانات الناخبين أو التلاعب في نتائج التصويت بهدف تغيير نتائج الانتخابات قد تم الاعتراف به كحالة واضحة نسبياً International law and cyberspace: Finland's national positions.

وعلى سبيل الاستطراد في هذا الصدد يجدر بنا الإشارة إلى أن هذا التردد مفهوم إذا ما أُخذ في الاعتبار أن مفهوم الإكراه عبر التلاعب قد يُستخدم من قبل الدول السلطوية لتقييد الحريات الفردية: ففي مارس 2022، على سبيل المثال، قامت روسيا بحظر خدمة Google News على مستخدمي الإنترنت بدعوى نشر معلومات غير موثوقة بشأن سير العمليات العسكرية في أوكرانيا37.

ثانيًا: اختراق البرلمان الألماني (البوندستاغ)

هجوم سيبراني واسع النطاق استهدف شبكة البيانات الداخلية للبرلمان الألماني (البوندستاغ) في شهر مايو 2015؛ ويُصنف هذا

---

[36] (Non-Intervention Principle). "عدم التدخل في الشؤون الداخلية" **الرؤية القانونية لألمانيا** بشأن كيفية تطبيق القانون الدولي في الفضاء السيبراني، وتحديداً مبدأ **الإكراه؛ لذا** تجادل ألمانيا "؛ الذي يتقرر وفقاً للقانون الدولي التقليدي، يشترط في التدخل غير المشروع وجود عنصر هنا بأن الهجمات السيبرانية وحملات التضليل الرقمي الممنهجة يمكن أن ترقى إلى مستوى الإكراه إذا حققت ذات "الحجم والأثر" الذي تحققه الوسائل العسكرية أو المادية التقليدية. On the Application of International Law in Cyberspace Position Paper – March 2021 https://www.auswaertiges-amt.de/resource/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspac

1. Google announced action against users who 'exploit, dismiss or condone' Putin's war . https://www.theguardian.com/world/2022/mar/24/russia-blocks-google-news-after-it-bans-ads-on-proukraine-invasion-content

الهجوم كواحد من أخطر الاختراقات السيبرانية التي تعرضت لها المؤسسات الحكومية الألمانية **he Cyber Law Toolkit** ، وهذه الشبكة مستخدمة من قبل جميع أعضاء البرلمان وكذلك المستشارة الألمانية إنذاك. وقد تمكنت الجهة المنفذة للعملية38 من الحفاظ على وصول غير مصرح به لمدة أشهر إلى بيانات الاتصالات الداخلية السرية (مثل رسائل البريد الإلكتروني السرية لأعضاء البرلمان)، وجداول أعمالهم، وتفاصيل الاجتماعات، وبيانات حساسة أخرى، مع اختراق أكثر من 20,000 حساب

Efrony, D& Shany,Y(2018),، بل وتمكنت حتى من الوصول إلى جهاز حاسوب في مكتب المستشارة داخل البرلمان. وأسفرت العملية عن سرقة أكثر من 16 غيغابايت من البيانات39.

وبناءً على كل هذه المعطيات، يمكن القول إنه سواء نُسبت العملية التي اخترقت البنية التحتية السيبرانية الألمانية بشكل غير توافقي إلى فاعلٍ تابعٍ لدولة أم لا—وبغض النظر عن توصيفها كعملية تجسس—فإنها كانت ستشكل انتهاكاً للسيادة الألمانية.

والسؤال؛ عما إذا كانت العملية، بالنظر إلى أن السلطات الألمانية قامت عقبها بإيقاف نظام الحاسوب في البوندستاغ لعدة أيام بهدف تعزيز أمن الشبكة، فهل يمكن أن تُصنّف كعمل من أعمال التدخل المحظور.

بافتراض أن العملية تدخلت فعلاً في المجال الداخلي لألمانيا، وهو ما يحقق العنصر الأول من عناصر التدخل غير المشروع، فإن هذا السلوك يفتقر في جميع الأحوال إلى عنصر الإكراه. إذ إن قرار السلطات الألمانية بإيقاف تشغيل الشبكات وتحسين آليات الحماية كان قراراً سيادياً ألمانيّاً,Efrony, D& Shany,Y(2018)؛ وحتى لو كان هذا القرار قد تأثر بمدة وشدة الحادثة، فإنه يظل مختلفاً عن حالة الإكراه القسري أو الإلزامي الذي يجبر الدولة على تبني سلوك معين أو تغيير إرادتها.

نستنتج مما سبق؛ القاعدة: أن سيادة الدولة تُعد منتهكة عندما تُمارس سلطتها بأي شكل في إقليم دولة أخرى دون موافقة صحيحة من تلك الدولة أو دون وجود قاعدة قانونية دولية تجيز التصرف؛ باعتبار أي تدخل غير توافقي أو غير مبرر قانونياً داخل المجال السيادي القانوني لدولة ما يشكل انتهاكاً لسيادتها.

---

[38] المرتبطة بجهاز الاستخبارات (Fancy Bear/Sofacy المعروفة باسم) APT28 تشير التحقيقات الألمانية إلى أن مجموعة القرصنة الروسية كانت مسؤولة عن العملية. وبعد اكتشاف الهجوم، تم إيقاف نظام حاسوب البوندستاغ لمدة أربعة أيام لإجراء أعمال الصيانة، GRU العسكرية الروسي كما تم تركيب آليات أمنية إضافية.

Merkel blames Russia for 'outrageous' cyberattack on German parliament,
https://www.politico.eu/article/merkel-blames-russia-for-outrageous-cyber-attack-on-german-parliament/

39 German parliament foiled cyber attack by hackers via Israeli website,
https://www.reuters.com/article/world/german-parliament-foiled-cyber-attack-by-hackers-via-israeli-website-idUSKBN1701VV/

وبذلك؛ أي عملية سيبرانية غير مصرح بها أو غير مبررة قانونياً تستهدف البنية التحتية السيبرانية لدولة أخرى، والتي لا تصل إلى مستوى العنف المطلوب وفق قاعدة استخدام القوة، قد تُشكل انتهاكاً لسيادتها,(Tsagourias, N(2021

ثالثًا: عملية تسريب (Doxing) وزارة الدفاع المكسيكية

يُعرف أكبر تسريب للبيانات والمعلومات الحساسة في تاريخ وزارة الدفاع المكسيكية (SEDENA) باسم "تسريبات غواكامايا " (Guacamaya Leaks)، والذي وقع في سبتمبر 2022 (مركز الدراسات الاستراتيجية والدولية CSIS) ، وقد استهدف الهاكرز وزارة الدفاع المكسيكية وتمكنوا من الوصول إلى ستة تيرابايت من البيانات، وقاموا بتسريب معلومات تشمل اتصالات داخلية، وبيانات جنائية، ومعلومات عن عمليات إنفاذ القانون، وأوضاعاً صحية للرئيس المكسيكي، بالإضافة إلى بيانات تكشف مراقبة المكسيك للسفير الأمريكي كين سالازار(مركز الدراسات الاستراتيجية والدولية CSIS) .

بناءً عليه؛ بافتراض إمكانية نسبة العملية إلى دولة ما، فيما يتعلق بالاختراق غير التوافقي وسرقة البيانات، من خلال استحضار التحليلات المقدمة في اختراق البرلمان الألماني، يتبين لنا أن هذا السلوك الأول انتهاكاً لسيادة الدولة المكسيكية.

أما فيما يتعلق بتسريب البيانات السرية، يمكن القول بوجه عام إن نشر معلومات تتعلق من بين أمور أخرى بالصحة الشخصية لرئيس الدولة، وعمليات الاستخبارات، وعمليات إنفاذ القانون الجنائي؛ قد يصل إلى درجة من الجسامة تجعلها قادرة على انتزاع الاستقلال السياسي للدولة بشكل قسري في المسائل التي تُعد وفقاً للقانون الدولي من صميم الاختصاص الداخلي.

نستنتج في هذا الصدد أمرين:

القانون الدولي محايد تقنياً (Technology Neutrality) وهو مبدأ قانوني أساسي وراسخ؛ وتعني هذه العبارة (القانون الدولي محايد تقنياً) أن القواعد القانونية الدولية تطبق على السلوك البشري بغض النظر عن الوسيلة أو التكنولوجيا المستخدمة في تنفيذ هذا السلوك؛ الدلالة على ذلك في قواعد القانون الدولي الإنساني كمثال :أكدت محكمة العدل الدولية في آرائها الاستشاريةhttps://www.icj-cij.org/case/93أن هذه القواعد تطبق على "جميع أشكال الحروب والأسلحة"، بما في ذلك الأسلحة التي لم تكن موجودة وقت صياغة المعاهدات (مثل الأسلحة النووية سابقاً، والأمن السيبراني حالياً).

وبذلك عندما تنخرط الدولة المُكرِهة مباشرة في سلوك غير مصرح به داخل إقليم دولة أجنبية، يُفترض وجود نية الإكراه ولا يلزم إثباتها لإثبات الفعل غير المشروع.

تفسيراً للعملية السيبرانية التي تعرضت لها دولة المكسيك، من الواضح أن عملية تسريب البيانات قد تكون ذات دقة كافية؛ مما يجعلها قادرة على التأثير في إرادة الدولة المستهدفة أو إضعاف قدرتها على ممارسة سلطتها ,Roscini, M(2024)؛ الأمر الذي قد يُفضي إلى إلزام الحكومة بالدخول في سلوك داخل نطاق اختصاصها الداخلي كانت لن تقوم به لولا ذلك التدخل؛ بدلالة

أنه قد كان من أهم نتائجها أن الرئيس أوبرا دور أضطر إلى الاعتراف بوقوع هجوم سيبراني40 والكشف عن مشكلات صحية تتعلق به41.

رابعًا: الهجوم السيبراني على شبكة الكهرباء الأوكرانية

تتلخص الوقائع بأن شركات الطاقة الأوكرانية تعرضت في 23 ديسمبر 2015، لهجوم سيبراني غير مسبوق تسبب في انقطاع الكهرباء. وقد نُفذت هذه الهجمات من قبل مهاجمين سيبرانيين عن بُعد، استخدموا بيانات اعتماد شرعية تم الحصول عليها بطرق غير معروفة، وتمكنوا من تشغيل القواطع الكهربائية عن بعد لفصل التيار42. مما تسبب في انقطاع الكهرباء لعدة ساعات عن ما يقارب 225,000 مستهلك في غرب أوكرانيا ,Power grid cyberattack in Ukraine (2015)؛ واختراق ثلاث مؤسسات أخرى، بعضها تابع لقطاعات بنية تحتية حيوية أخرى، لكنها لم تتعرض لآثار تشغيلية مباشرة (التقرير الأمني، **المركز الوطني لتكامل الأمن السيبراني والاتصالات**، وزارة الأمن الداخلي الأمريكية). وأفادت جميع الشركات المتضررة أن الجهات المهاجمة قامت أيضاً بمسح بعض الأنظمة باستخدام برمجية KillDisk في نهاية العملية؛ "وبرمجية KillDisk الخبيثة تقوم بمسح الملفات المختارة على الأنظمة المستهدفة وإتلاف سجل الإقلاع الرئيسي(Master Boot Record) ، مما يؤدي إلى جعل الأنظمة غير قابلة للتشغيل.

ولم تكن لدى الشركات الأوكرانية خطة استعادة مُعدة مسبقاً، إلا أن خبرتها في التشغيل اليدوي لأنظمة التوزيع سمحت لها بالتعافي بسرعة خلال بضع ساعات. وقد استغرق الأمر عدة أشهر لإعادة مراكز التحكم إلى التشغيل الكامل. وقد خلص المحققون الأوكرانيون، بالتعاون مع نظرائهم من مكتب التحقيقات الفيدرالي (FBI) ووزارة الأمن الداخلي الأمريكية(DHS) ، إلى أن عملية BlackEnergy 1 نشأت من دولة أو من مجموعة مدعومة من دولة، وكانت تهدف أساساً إلى توجيه تحذير وليس إحداث تدمير واسع النطاق"(Efrony, D& Shany,Y(2018),

[40] **Mexican government suffers major data hack, president's health issues revealed, https://www.reuters.com/world/americas/mexican-president-confirms-hack-government-files-2022-09-30/**

41 وصرّح بأنه "كان هناك خطر حدوث نوبة قلبية وتم نقلي إلى المستشفى، وأوصوا بإجراء قسطرة قلبية ؛و أنا مريض ولدي عدة أمراض أتناول مزيجاً من الأدوية ليلاً لعدة حالات، بما في ذلك ارتفاع ضغط الدم ومشاكل الغدة الدرقية، لكنني بخير جداً، وأخضع للفحص كل ثلاثة أو أربعة أشهر.

[42] التقرير الأمني الصادر عن **المركز الوطني لتكامل الأمن السيبراني والاتصالات (NCCIC)** التابع لوزارة الأمن الداخلي الأمريكية (DHS) بتاريخ **7مارس 2016**، والذي يحمل الرقم المرجعي **IR-ALERT-H-16-043-01AP**وتحت عنوان *"الهجوم السيبراني ضد البنية التحتية الحرجة في أوكرانيا* (Cyber-Attack Against Ukrainian Critical https://nsarchive.gwu.edu/media/15896/oc_

ولذلك بناءً على اختراق البنية التحتية السيبرانية الواقعة داخل الأراضي الأوكرانية لا شك أنه يُشكّل عملًا في حد ذاته انتهاكاً لسيادة أوكرانيا؛ والسؤال عما إذا كان هذا الهجوم يمكن أن يرقى إلى مستوى التدخل المحظور؛ من خلال نتائج هذا الهجوم؛ فالإجابة نعم.

يفسر الباحثين هذا الهجوم كخرق محتمل لمبدأ عدم التدخل43، حيث يُمثل تدخلاً قسرياً في الشؤون الداخلية للدولة عبر شلّ قطاع الطاقة الحيوي، وهو خيار سيادي يقع ضمن الاختصاص الحصري للدولة المتضررة.

نستنتج من ذلك؛ أن التدخل في شبكة الطاقة الكهربائية لدولة ما يدخل بوضوح ضمن نطاق اختصاصها الداخلي، وهو أمر لا شك فيه أنه يحقق العنصر الأول من عناصر التدخل؛ كما أن التسبب في انقطاعات الكهرباء يمثل مثالاً واضحاً على الإكراه القسري، إذ يحل محل إرادة الدولة المستهدفة في ممارسة اختصاصاتها الداخلية.

وبهذا؛ من الواضح أن الشبكة الوطنية لأي دولة تُعد قطاع حيوي في تفسيرات الأمن القومي للدولة، بما في ذلك الأمن الفردي والمجتمعي والحكومي ROSCINI, M (2014) وعندما تُعطّل عملية ما وظائف هذه الشبكة فقد يكون لذلك القدرة على الارتقاء إلى مستوى انتهاك للمادة 2(4) من ميثاق الأمم المتحدة (Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue & Julia Spiegel(2011) ؛ الأمر الذي يجعلنا نتأكد من قاعدة مستقرة تظهر في مفهوم مفاده: "أن حظر التدخل ليس معياراً قائماً على النتائج وحده Roscini, M(2024. P.154)، لذا؛ ليس من الضروري أن يحقق الفعل غير المشروع هدفه لكي يُعد انتهاكاً لمبدأ عدم التدخل؛ إذ يكفي وجود إكراه غير مشروع، سواء استسلمت الدولة الضحية أو قاومت الضرر.

الخاتمة

السيادة مجال معقد ومتغير في القانون الدولي، ويوصف تطبيق أحكامها على الفضاء الإلكتروني بالغموض؛ الأمر الذي جعل البعض يُقر بأن السيادة كيان مستقل عن القانون الدولي، ويمثل ضمانة مطلقة لحرمة الأراضي، مع مراعاة الاستثناءات أو الموافقة؛ وبالتالي القاعدة التي يُبنى عليها مبدأ سيادة الدولة في علاقاتها مع غيرها من الدول هي الرضا؛ فالرضا أو قبول الدولة بتصرف أو سلوك ما صادر عن دولة أخرى هو فعل سيادي ينبثق من الرضا طواعية حتى في الفضاء السيبراني، وبالتالي سيادة الدولة في الفضاء السيبراني مستوفية الأركان وتحقق أحكامها بوضوح رغم غموض القيود التي تطرأ بشأنها مهما تطورت.

بناءً عليه؛ توصلت الدراسة إلى عدة نتائج مرفقة ببعض التوصيات؛ وذلك على النحو التالي:

النتائج:

[43] يُدرج دليل القانون السيبراني (**Cyber Law Toolkit**) الهجوم الإلكتروني على شبكة الكهرباء في أوكرانيا عام 2015 كحالة دراسية تطبيقية رئيسية في **السيناريو 03(Scenario 03: Cyber operation against the power grid)** ، وذلك لتحليل كيفية تطبيق القانون الدولي العام والقانون الدولي الإنساني على العمليات السيبرانية التي تستهدف البنية التحتية الحيوية.

- تظل سيادة الدولة مبدأً أساسيًا من مبادئ القانون الدولي، وهو متحقق بالكامل في أحكام الفضاء السيبراني.
- لا يقصد من السيادة في الفضاء السيبراني أنها مطلقة ولا مرادفة للتحرر من القيود القانونية.
- غياب الحدود المادية لا يُقيد أحكام المسؤولية الدولية للدول عن الأنشطة السيبرانية التي تنتهك سلامة دول أخرى أو ولايتهم القضائية.
- تبدو الحاجة ملحة لتطوير مستمر لمعايير متعددة الأطراف لتوضيح حدود سلوك الدول في المجال السيبراني
- التعاون الدولي والمسؤولية المشتركة مطلبًا أساسيًا لتحقيق التوازن بين السيادة والحرية والأمن في الفضاء السيبراني.

التوصيات:

- زيادة المبادرات الحكومية والإقليمية التي تهدف إل لتعزيز الدفاعات وزيادة التعاون في الفضاء الإلكتروني، من أجل هدف وضع حد للهجمات الإلكترونية
- لتحديد مسؤولية الدولة في الفضاء السيبراني ينبغي أن تستند إلى شرط بذل العناية الواجبة بدلًا من الالتزام بتقديم رابط رسمي بين سلطة الدولة وأفعال مرتكبي الهجمات السيبرانية
- آن الآوان أن تتفق الدول على قواعد قانونية ملزمة تنص على سيادة سيبرانية مشتركة ؛ على أن تحتفظ الدول بسلطتها واستقلالها من خلال اتفاقات ومعاهدات متعددة الأطراف تحدد آليات حوكمة رقمية بما يضمن الأمن والشفافية وحماية حقوق الإنسان

المراجع:

بلغة الإنجليزية:

- Abaigeal Lorge (2025), The UK's New Take on Cyber, https://www.irregularwarfare.org/uk-cyber-power-strategy-cybersecurity-sovereignty-influence/
- Buchan, R. & Navarrete, I. (2021), Cyber espionage and international law, in Research Handbook on International Law and Cyberspace, https://www.elgaronline.com/edcollchap/edcoll/9781789904246/9781789904246.00021.xml

- Buchan, R. (2019), Cyber Espionage and International Law, Hart Publishing / Bloomsbury.
- Ducheine, B. et al. (2021), The Concept of Cyber Operations, in Research Handbook on International Law and Cyberspace, p. 272, https://www.e-elgar.com/shop/gbp/research-handbook-on-international-law-and-cyberspace-9781789904246.html
- Efrony, D. & Shany, Y. (2018), A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyber Operations and Subsequent State Practice, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3172743
- Jensen, Eric Talbot (2018), THE TALLINN MANUAL 2.0: HIGHLIGHTS AND INSIGHTS, https://www.law.georgetown.edu/international-law-journal/wp-content/uploads/sites/21/2018/05/48-3-The-Tallinn-Manual-2.0.pdf
- Ferrándiz, Emilia (2023), A Sea of Law: The Romans and Their Maritime World, https://anetoday.org/ferrandiz-roman-maritime-law/
- Corn, Gary (2018), Sovereignty in the Age of Cyber, https://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?article=3172&context=facsch_lawrev
- Gill, T. (2013), Non-intervention in the cyber context, https://dare.uva.nl/id/51a91270-2486-49c2-bf49-52b29479cace
- Global Commission on the Stability of Cyberspace (GCSC) (2019), Initiative Overview / Final Report, https://hcss.nl/global-commission-on-the-stability-of-cyberspace-final-report/
- Goldsmith, J. (1998), Against Cyberanarchy, 65 U. Chi. L. Rev., https://hls.harvard.edu/bibliography/against-cyberanarchy/
- Kułaga, Łukasz (2024), MAPPING THE POSITION OF STATES ON THE APPLICATION OF SOVEREIGNTY IN CYBERSPACE, POLISH REVIEW OF INTERNATIONAL AND EUROPEAN LAW, Vol. 13, Issue 1, https://czasopisma.uksw.edu.pl/priel/article/view/14264/12758
- Hardin, G. (1968), The Tragedy of the Commons, Science, Vol. 162, Issue 3859,

https://www.garretthardinsociety.org/articles_pdf/tragedy_of_the_commons.pdf

- Crawford, James (2019), Brownlie's Principles of Public International Law, Oxford University Press, https://www.researchgate.net/publication/335370498_Brownlie's_Principles_of_Public_International_Law
- Jensen, Eric Talbot (2018), THE TALLINN MANUAL 2.0: HIGHLIGHTS AND INSIGHTS, https://www.law.georgetown.edu/international-law-journal/wp-content/uploads/sites/21/2018/05/48-3-The-Tallinn-Manual-2.0.pdf
- Fu, Jiarong (2023), Comments on Speech by the Attorney General of UK on International Law in Cyberspace, Studies in Law and Justice, https://www.pioneerpublisher.com/slj
- Johnson, D. & Post, D. (1996), Law and Borders: The Rise of Law in Cyberspace, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=535
- Alvarez, Joshua (2015), Stuxnet: The world's first cyber weapon, https://cisac.fsi.stanford.edu/news/stuxnet
- Kilovaty, Ido (2021), Chapter 5: The international law of cyber intervention, in Research Handbook on International Law and Cyberspace, https://www.elgaronline.com/edcollchap/edcoll/9781789904246/9781789904246.00014.xml
- Lasky, Jack (2022), Cyberspace, Salem Press Encyclopedia / EBSCO, https://www.ebsco.com/research-starters/science/cyberspace
- Maftei, Jana (2015), Sovereignty in International Law, https://www.researchgate.net/publication/311581450_Sovereignty_in_International_Law
- Mhajne, Anwar (2024), A feminist cybersecurity: addressing the crisis of cyber(in)security, https://www.ebsco.com/articles/computer-science/98e15e9d-8516-5f61-85d8-0166a7396cd9/a-feminist-cybersecurity-addressing-the-crisis-of-cyber-in-sec
- Delerue, François (2020), Cyber Operations and International Law, Cambridge University Press,

https://www.academia.edu/42085508/Cyber_Operations_and_International_Law

- Moynihan, Harriet (2019), The Application of International Law to State Cyberattacks: Sovereignty and Non-Intervention, Chatham House Research Paper, https://www.chathamhouse.org/sites/default/files/publications/research/2019-11-29-Intl-Law-Cyberattacks.pdf
- Moynihan, Harriet (2019), The Application of International Law to State Cyberattacks: Sovereignty and Non-intervention, International Law Programme, https://www.astrid-online.it/static/upload/chat/chatham-house_2019-11-29-intl-law-cyberattacks.pdf
- Butchard, Patrick (2024), Territorial Integrity, Political Independence, and Consent: The Limitations of Military Assistance on Request under the Prohibition of the Use of Force, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4759531
- Pierucci, F. (2025), Sovereignty in the Digital Era: Rethinking Territoriality and Governance in Cyberspace, https://doi.org/10.1007/s44206-025-00189-4
- Bokil, Rohit (2023), Cyber Warfare: Taking War to Cyberspace and its Implications for International Humanitarian Law, International Journal For Multidisciplinary Research (IJFMR), https://www.ijfmr.com/papers/2023/1/1494.pdf
- Roscini, Marco (2024), International Law and the Principle of Non-Intervention: History, Theory, and Interactions with Other Principles, Oxford University Press, https://global.oup.com/academic/product/international-law-and-the-principle-of-non-intervention-9780198786894
- Schmitt, Michael N. (2018), Virtual Electoral Exclusion: Cyber-Manipulation of Elections in the Grey Zones of International Law, Chicago Journal of International Law, https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=1736&context=cjil

- Schmitt, Michael N. & Vihul, Liis (2017), Respect for Sovereignty in Cyberspace, Texas Law Review, Vol. 95, pp. 1639–1670, https://centaur.reading.ac.uk/89703/8/Sovereignty%20Texas%20LR_removed.pdf
- Schmitt, Michael N. (2020), Foreign Cyber Interference in Elections: An International Law Primer, Part I, EJIL:Talk!, https://www.ejiltalk.org/foreign-cyber-interference-in-elections-an-international-law-primer-part-i/
- Schrijver, Nico (2000), THE CHANGING NATURE OF STATE SOVEREIGNTY, British Yearbook of International Law, https://doi.org/10.1093/bybil/70.1.65
- Shokri, Ashkan (2025), Sovereignty in Cyberspace from the Viewpoint of International Law, Asian Journal of International Law, https://www.cambridge.org/core/journals/asian-journal-of-international-law/article/abs/sovereignty-in-cyberspace-from-the-viewpoint-of-international-law/2193733BFBAA268E7E211FA
- Krasner, Stephen D. (1999/2010), Sovereignty: Organized Hypocrisy, Princeton University Press, https://books.google.com/books/about/Sovereignty.html?id=tHJ5m56sBX4C
- Tsagourias, Nicholas (2021), The legal status of cyberspace: sovereignty redux?, in Research Handbook on International Law and Cyberspace, https://www.elgaronline.com/edcollchap/edcoll/9781789904246/9781789904246.00010.xml
- Tsagourias, Nicholas (2021), The legal status of cyberspace, https://ideas.repec.org/h/elg/eechap/15436_1.html
- Tsagourias, Nicholas & Buchan, Russell (Eds.) (2021), Research Handbook on International Law and Cyberspace (2nd ed.), Edward Elgar Publishing, https://www.e-elgar.com/shop/gbp/research-handbook-on-international-law-and-cyberspace-9781789904246.html
- Tsagourias, Nicholas (2020), Malicious Cyber Operations against Health Infrastructure during the COVID-19 Pandemic and the Renvoi to

Sovereignty in Cyberspace, ESIL Reflections, Vol. 9, No. 4, https://esil-sedi.eu/esil-reflection-international-law-in-an-age-of-post/

- Tsagourias, Nicholas (2015), The legal status of cyberspace, in Research Handbook on International Law and Cyberspace (1st ed.), p. 13, https://www.elgaronline.com/edcollchap/edcoll/9781782547389/9781782547389.00010.xml
- Vattel, Emer de (1777), Le Droit Des Gens, Ou Principes De La Loi Naturelle: Appliqués à la conduite & aux affaires des Nations & des Souverains, Volume 1, https://books.google.com/books?id=D5hCAAAAcAAJ
- Visger, M. (2022), The International Law Sovereignty Debate and Development of International Norms on Peacetime Cyber Operations, Lawfare, https://www.lawfaremedia.org/article/international-law-sovereignty-debate-and-development-international-norms-peacetime-cyber-operations
- Wheatley, Steven (2023), Election hacking, the rule of sovereignty, and deductive reasoning in customary international law, Leiden Journal of International Law, Volume 36, Issue 3, https://doi.org/10.1017/S0922156523000092

اللغة العربية:

- أسامة فرج ضو عبدالجليل (2026)، الطبيعة القانونية للمنطقة البحرية الدولية، https://cjhes.com.ly/index.php/cjhes/ar/article/view/189/209
- أسماء قطاف .عبد الرؤوف دبابش (2017) ، الدور الإقليمي في السياسة الخارجية : دراسة مفاهيمية نظرية ، https://asjp.cerist.dz/en/article/135172
- **حمد قدوره (2020)**، أزمة السيادة الإقليمية في القرن الواحد والعشرين، المركز الديمقراطي العربي، **https://democraticac.de/?p=70563**
- **الغزير، نعيمة (2025)، الأثار القانونية للتكنولوجيا على سيادة الدولة في المجال الجوي والفضاء الخارجي؛ بحث مقدم للمؤتمر الدولي بعنوان السيادة الجوية الواقع والتحديات) (وزارة الدفاع الليبية؛ 24 إلى 28 فبراير 2025**
- **كامش طيب (2025) . القانون الدولي ومعايير الفضاء السيبراني، بين الفراغ القانوني والاستغلال الجيوسياسي، الرابط:** https://asjp.cerist.dz/en/article/282348

- **محناوي، محمد (2026)، إشكالية السيادة الوطنية في الفضاء السيبراني: بين مبدأ عدم التدخل ومسؤولية الدول،** https://bcchj.uobabylon.edu.iq/index.php/bcchj/ar/article/view/2848/2861
- **محمود، (2026)، الفضاء السيبراني** https://arabica.dohainstitute.org/pages/cyberspace.aspx

التقارير والمنشورات:

- **وزارة الدفاع الأمريكية، استراتيجية الدفاع عن الوطن والدعم المدني (2005)، ص 12.** https://policy.defense.gov/portals/11/Documents/hdasa/ASDHD_Statement%20_HASCTUTC_%2015%20Mar%2005.pdf
- **مجلس الاتحاد الأوروبي:** https://www.consilium.europa.eu/en/press/press-releases/2017/11/20/eu-to-beef-up-cybersecurity/
- **مجلس السلم والأمن التابع للاتحاد الإفريقي**
- https://cyberlaw.ccdcoe.org/wiki/Common_position_of_the_African_Union_(2024)_n
- منظمة حلف شمال الأطلسي (الناتو)، . https://assets.publishing.service.gov.uk/media/5a7ece9740f0b6230268baa1/Wales_Summit_Declaration.pdf
- المجلس الدائم لـ منظمة الأمن والتعاون في أوروبا https://ccdcoe.org/incyder-articles/osce-expands-its-list-of-confidence-building-measures-for-cyberspace-/common-ground-on-critical-infrastructure-protection
- أستراليا في الجلسة الرابعة للفريق العامل المفتوح العضوية (مارس 2023) . https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technol-_ogies_-_(2021)/OEWG4_-_Australia_intervention_-_law
- من تقرير فريق الخبراء الحكوميين لعام 2015) وثيقة الأمم المتحدة (A/70/174 https://digitallibrary.un.org/record/799853/files/A_70_174-EN.pdf
- دليل تالين 2.0 هو مرجع أكاديمي غير ملزم صدر عام 2017 بإشراف مركز التميز التعاوني للدفاع السيبراني التابع لحلف الناتو(NATO CCDCOE) . https://modeldiplomat.com/learn/glossary/tallinn-manual-2-0
- الحكومة الاتحادية الألمانية، ورقة موقف بشأن تطبيق القانون الدولي في الفضاء السيبراني، مارس 2021.
- https://database.cyberpolicyportal.org/entity/pio8ogf79r?file=165968975005_8j3zijc9a99.df&page=1

- حكومة مملكة هولندا، ملحق: القانون الدولي في الفضاء السيبراني
https://ceipfiles.s3.amazonaws.com/pdf/CyberNorms/LawStatements/Appendix_+International+Law+in+Cyberspace+(Statement+by+the+Netherlands).pdf
- الموقف النمساوي بشأن الأنشطة السيبرانية والقانون الدولي، أبريل 2024،
- https://www.justsecurity.org/96993/austrias-stance-cyber-operations-international-la
- وزارة الخارجية الإيطالية، الورقة الوطنية الإيطالية بشأن "القانون الدولي والفضاء السيبراني
https://www.esteri.it/mae/resource/doc/2021/11/italian_position_paper_on_international_law_and_cyberspace.pdf
- خطاب المستشار العام للمملكة المتحدة، برافرمان ، الأكاديمية القانونية الدولية ,Chatham House ، 19 مايو 2022.
- https://www.chathamhouse.org/events/all/members-event/international-law-future-frontiers

الوثيقة الرسمية الصادرة عن وزارة الخارجية الفنلندية تحت عنوان "القانون الدولي والفضاء السيبراني": المواقف الوطنية لفنلندا International law and cyberspace: Finland's national positions.
https://um.fi/documents/35732/0/KyberkannatPDF_EN.pdf/12bbbbde-623b-9f86-b254-07d5af3c6d85?t=1603097522727

- مركز الدراسات الاستراتيجية والدولية(CSIS) ، https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents
- التقرير الأمني الصادر عن **المركز الوطني لتكامل الأمن السيبراني والاتصالات (NCCIC)** التابع لوزارة الأمن الداخلي الأمريكية (DHS) بتاريخ **7مارس 2016**، والذي يحمل الرقم المرجعي IR-ALERT-H-16-043-01AP وتحت عنوان *"الهجوم السيبراني ضد البنية التحتية الحرجة في أوكرانيا* (Cyber-Attack Against Ukrainian Critical
https://nsarchive.gwu.edu/media/15896/oc

- Russia blocks Google News after ad ban on content condoning Ukraine invasion,
Google announced action against users who 'exploit, dismiss or condone' Putin's war. https://www.theguardian.com/world/2022/mar/24/russia-blocks-google-news-after-it-bans-ads-on-proukraine-invasion-content



Issue - 28 - Part 2- September - 2026 - Year 6 Refereed Quarterly Scientific Journal

American International Journal of Humanities and Social Sciences

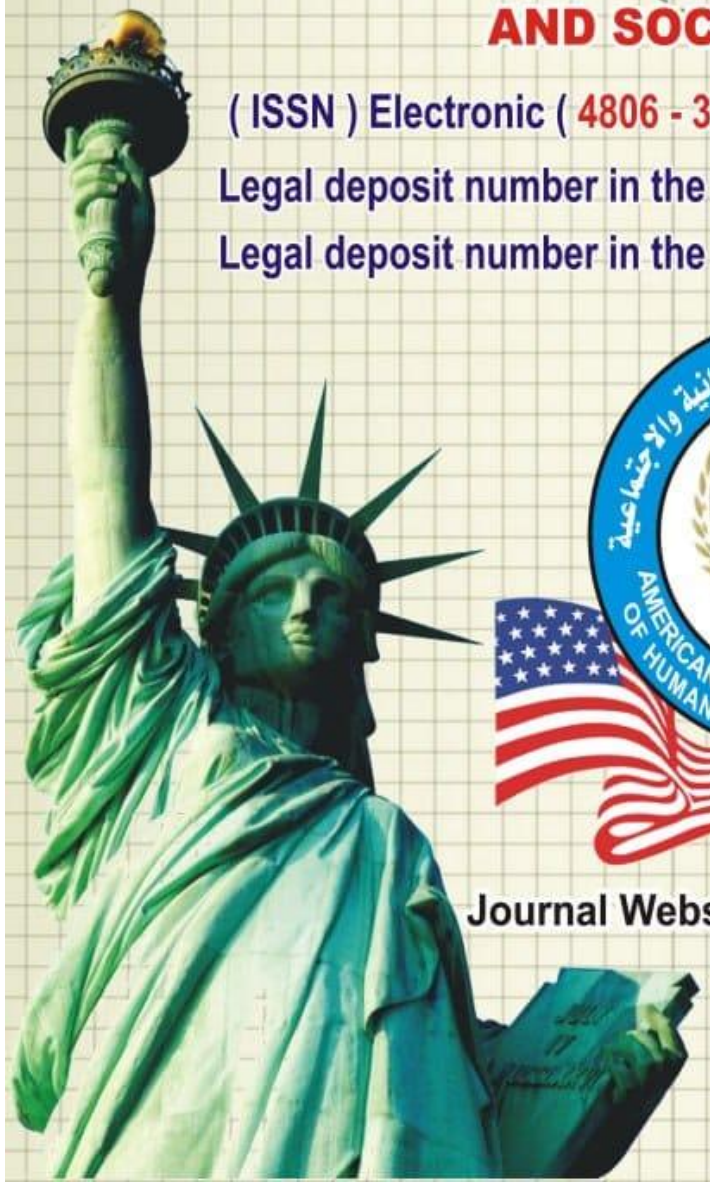
ISSUED BY AMERICAN INTERNATIONAL ACADEMY FOR HIGHER EDUCATION AND TRAINING

QUARTERLY JOURNAL ON HUMANITARIAN AND SOCIAL AFFAIRS

(ISSN) Electronic (4806 - 3085) / (ISSN) Paper (4830 - 3085)

Legal deposit number in the Moroccan National Library (2025PE00006)

Legal deposit number in the Iraq National Library and Archives (2735)



Journal Website : https://iajphss.us/