Journal of Shatt Al Arab University College for Administration and Legal Sciences

مجلة كلية شط العرب الجامعة للعلوم الادارية والقانونية

VoL(4). No. (1) 2026 المجلد. (4) العدد. (1)

الفراغ القانوني في تنظيم مسؤولية الفاعلين السياديين والخاصين في الهجمات السيبرانية العابرة للحدود: دراسة في القانون الدولي العام

"The Legal Gap in Regulating the Responsibility of State and Private Actors in Cross-Border Cyberattacks: A Study under Public International Law."

الباحث الاول المدرس المساعد السيد محمد ستار جبر
وزارة التعليم العالي والبحث العلمي ، دائرة التعليم الجامعي الاهلي
(mohammedsattar@mohesr.edu.iq)

الباحث الثاني المدرس المساعد السيد اسيل عبدالوهاب خليل
وزارة التعليم العالي والبحث العلمي ، الدائرة الإدارية والمالية
(aseel.a.khalil@moheser.edu.iq)

المستخلص

يتناول هذا البحث إشكالية الفراغ القانوني في تنظيم مسؤولية الفاعلين السياديين والخاصين عن الهجمات السيبرانية العابرة للحدود في إطار القانون الدولي العام. فمع التحولات العميقة التي شهدتها طبيعة النزاعات الدولية، برز الفضاء السيبراني كساحة جديدة للصراع، تُمارَس فيها أنماط مستحدثة من الهجمات التي تستهدف البنى التحتية الحيوية للدول، بما يشكل تهديداً مباشراً للأمن والسلم الدوليين. وتزداد تعقيدات هذه الظاهرة مع تنامي دور الشركات الخاصة بوصفها فاعلين مؤثرين في البيئة الرقمية، سواء من خلال امتلاكها أدوات تكنولوجية متقدمة أو بسبب تقصيرها في حماية البيانات أو تورطها غير المباشر في بعض الهجمات. ويهدف البحث إلى تحليل قصور القواعد القانونية الدولية القائمة في تحديد المسؤولية القانونية عن هذه الهجمات، والكشف عن أبعاد الفراغ التشريعي الذي يحد من فعالية المساءلة الدولية. ويعتمد البحث المنهج التحليلي القانوني لتقييم النصوص الدولية ذات الصلة، وصولاً إلى تقديم رؤية قانونية قد تسهم في بلورة إطار دولي ملزم ينظم مسؤولية الدول والجهات الخاصة في الفضاء السيبراني.

الكلمات المفتاحية: الفضاء السيبراني ، الهجمات السيبرانية العابرة للحدود ، مسؤولية الدولة ، الفاعلون من غير الدول ، الشركات الخاصة ، القانون الدولي العام ، الفراغ القانوني ، الأمن السيبراني الدولي.

Abstract

This study examines the legal vacuum surrounding the regulation of responsibility for transboundary cyberattacks under public international law, with a particular focus on both state and private actors. In light of the profound transformations in the nature of international conflicts, cyberspace has emerged as a new arena of confrontation, where sophisticated attacks increasingly target critical infrastructure, posing serious threats to international peace and security. The complexity of this issue is further amplified by the growing role of private companies as influential actors in the digital domain, whether through their technological capabilities, failures in data protection, or indirect involvement in cyber operations. The research aims to analyze the shortcomings of existing international legal rules in addressing responsibility for cyberattacks and to identify the dimensions of the prevailing legal gap that undermines effective international accountability. Adopting an analytical legal approach, the study evaluates relevant international legal texts and proposes a balanced legal vision that may contribute to the development of a binding international framework governing responsibility in cyberspace.

Keywords : Cyberspace ، Transboundary Cyberattacks ، State Responsibility ، Non-State Actors ، Private Companies ، Public International Law ، Legal Vacuum ، International Cybersecurity

المقدمة الموسعة

شـــهد العالم خلال العقدين الأخيرين تحولات جوهرية في طبيعة النزاعات الدولية، حيث لم تعد مقتصـرة على الهجمات المسـلحة التقليدية أو الخروقات الحدودية، بل اتسـعت لتشـمل سـاحات رقمية جديدة، أبرزها الفضـاء السـيبراني. فقد باتت الهجمات الإلكترونية تشكل تهديداً جدياً على البنى التحتية الحيوية، كشبكات الطاقة، والمؤسسـات الأمنية، وأنظمة الاتصـالات، ما يجعل من الفضاء الرقمي ساحة نزاع غير معلنة لكنها حقيقية وذات أثر بالغ.

وتتفاقم هذه الإشـــكالية مع بروز جهات فاعلة جديدة في هذه البيئة، منها الدول ذات القدرات السيبرانية المتقدمة، ومنها أيضـاً شركات خاصـة أصـبحت تمثل أطرافاً مباشرة أو غير مباشرة في هذه الهجمات، ســـواء عبر أدواتها التكنولوجية، أو من خلال إهمالها في حماية بيانات المســـتخدمين أو حتى بتواطئها أحياناً. هذا الوضـــع يطرح تســـاؤلات ملحّة حول موقع القانون الدولي العام من هذه التحديات، ومدى قدرته على احتواء الظاهرة ضـمن إطاره التقليدي الذي لم يتطور بالسرعة ذاتها التي تطورت بها أدوات الحرب والهجوم.

تكمن خطورة المسـألة في أن القانون الدولي ما زال يفتقر إلى اتفاقية دولية شـاملة وملزمة تنظم الفضـاء السـيبراني وتحدد بدقة مسؤوليات الفاعلين، سواء أكانوا دولاً أم شركات خاصـة. ومن هنا تبرز الحاجة إلى البحث في أوجه القصور، أو ما يمكن تسميته بـــ"الفراغ القانوني"، الذي يترك المجال واسعاً للعبث والخرق دون محاسبة قانونية دولية رادعة.

إن هذا البحث يســـعى إلى تســـليط الضـــوء على هذا الفراغ من خلال دراســـة تحليلية قانونية لمسـؤولية الدول والشـركات الخاصـة في الهجمات السـيبرانية العابرة للحدود، والوقوف على

مكامن القصور في النصوص القانونية الدولية الحالية، وصولاً إلى تقديم تصور قانوني متوازن قد يُسهم في بلورة معاهدة دولية ملزمة تنظم هذا النوع المستحدث من النزاعات.

مشكلة البحث

يواجه المجتمع الدولي تحديًا قانونيًا غير مسبوق يتمثل في الفراغ التشريعي المتعلق بتنظيم الفضاء السيبراني، لا سيما فيما يتعلق بمسؤولية الدول والشركات الخاصة عن الهجمات السيبرانية العابرة للحدود. فعلى الرغم من اتساع رقعة هذه الهجمات وخطورتها على الأمن والسلم الدوليين، إلا أن القانون الدولي العام ما زال عاجزًا عن تقديم إطار قانوني ملزم ومحدد لتلك المسؤوليات. وعليه، تتمثل مشكلة البحث في:

ما مدى قدرة القانون الدولي العام على تنظيم مسؤولية الدول والشركات الخاصة في الهجمات السيبرانية العابرة للحدود في ظل غياب إطار قانوني دولي ملزم؟

أهداف البحث

1. تحليل الإطار القانوني الدولي الحالي المتعلق بالهجمات السيبرانية.
2. دراسة مسؤولية الدول والشركات الخاصة وفق القانون الدولي العام.
3. تقييم النماذج الدولية الحالية والمبادرات غير الملزمة.
4. اقتراح رؤية قانونية شاملة لسد الفراغ التشريعي في هذا المجال.

أهمية البحث

تبرز أهمية هذا البحث من خلال النقاط الآتية:

- معالجة إشكالية قانونية حديثة ومؤثرة تتعلق بأمن الدول وسيادتها الرقمية.

http://joshuc.edu.iq ISSN: 2079 -7486

- تسليط الضوء على الثغرات القانونية في تعامل القانون الدولي العام مع الهجمات السيبرانية.
- تقديم تحليل قانوني لمسؤولية الشركات الخاصة، وهو جانب غالبًا ما يُهمل في الدراسات التقليدية.
- اقتراح حلول قانونية قد تُسهم في بلورة معاهدة دولية تنظم الأمن السيبراني.

فرضيات البحث

1. يفتقر القانون الدولي الحالي إلى أدوات فعالة لإلزام الدول بوقف أو منع الهجمات السيبرانية.
2. تلعب الشركات الخاصة دورًا متزايدًا في تنفيذ أو تسهيل الهجمات السيبرانية دون مساءلة قانونية كافية.
3. غياب اتفاقية دولية ملزمة يُبقي الأمن السيبراني في منطقة رمادية قانونياً، ما يعقد مسألة المسؤولية الدولية.
4. يمكن تطوير إطار قانوني دولي متوازن عبر دمج القواعد العرفية والممارسات الجيدة المعترف بها دوليًا.

منهجية البحث

يعتمد هذا البحث على المنهج التحليلي والمقارن، من خلال:

- تحليل النصوص القانونية الدولية ذات العلاقة.
- دراسة الاتفاقيات والمعاهدات الدولية (مثل ميثاق الأمم المتحدة، اتفاقيات بودابست، وغيرها).
- استعراض السوابق القضائية، والممارسات الدولية للدول والمنظمات.
- المقارنة بين التشريعات الوطنية والدولية لتقييم أوجه القصور.

- استخدام منهج الاستقراء لتقديم مقترحات قانونية.

خطة البحث

تم تقسيم البحث إلى خمسة أبواب رئيسية كما في الفهرست، يتناول كل منها أحد أركان المشكلة بشكل متكامل، من المفاهيم الأساسية إلى التوصيات القانونية.

الباب الأول: الإطار المفاهيمي والقانوني للهجمات السيبرانية

المبحث الأول: تعريف الهجمات السيبرانية وتصنيفها

أولاً: مفهوم الهجمات السيبرانية

أ- تُعد الهجمات السيبرانية (Cyber Attacks) من أخطر الظواهر المعاصرة المرتبطة بالتقدم التكنولوجي الهائل في مجال الاتصالات وتكنولوجيا المعلومات. ورغم تعدد التعريفات، إلا أنه لا يوجد تعريف دولي موحّد للهجوم السيبراني، ما يعكس حجم التعقيد في ضبط هذه الظاهرة قانونيًا.

ب- من الناحية الاصطلاحية: يُعد مصطلح **"الهجمات السيبرانية "** تركيباً اصطلاحياً يجمع بين لفظة *"سيبراني "* المشتقة من مفهوم الفضاء الإلكتروني والحوسبة والبيئات الرقمية، ولفظة *"هجمات "* التي تحيل في أصلها اللغوي إلى أفعال عدائية أو أعمال إكراه ترمي إلى الإضرار بالطرف المستهدف أو تعطيله. وقد شهد هذا المصطلح تطوراً دلالياً مهماً، إذ انتقل من نطاقه المجازي المستوحى من سياقات الصراع العسكري التقليدي إلى دلالة تقنية متخصصة تُستخدم للإشارة إلى كل فعل

http://joshuc.edu.iq ISSN: 2079 -7486

عدائي يُنفَّذ عبر الوسائط الرقمية أو الأنظمة الحاسوبية بهدف اختراق أو تعطيل أو التلاعب بالمعلومات أو بالبنى التحتية المعلوماتية.

ويمتاز هذا التركيب الاصطلاحي بكونه يُجسد تحوّلاً لغوياً واضحاً، حيث توسّعت الدلالة التقليدية لكلمة *"هجمات "*من معناها الفيزيائي المباشر إلى معنى غير مادي يتعلق باعتداءات تُمارَس في فضاء افتراضي لا يخضع لحدود جغرافية. كما اكتسب المصطلح مع مرور الوقت طابعاً مؤسساتياً داخل الخطاب القانوني والتقني، ليصبح مفهوماً محدداً يميّز الهجمات السيبرانية عن غيرها من الظواهر المشابهة مثل *الحوادث السيبرانية* أو *الاختراقات الرقمية* أو *التدخلات الشبكية* .وبذلك، يعكس المصطلح في تطوره الاصطلاحي تفاعلاً بين اللغة والواقع التقني، مظهراً قدرة اللغة على استيعاب المفاهيم المستحدثة وصياغتها بدقة تتوافق مع الاستخدامات العلمية والعملية المعاصرة.

ويُعرف الهجوم السيبراني بأنه:

"أي فعل متعمد يتم باستخدام الوسائل التقنية الرقمية يستهدف نظم المعلومات أو الشبكات أو البيانات بهدف إلحاق الضرر أو التدمير أو التعطيل أو التلاعب، سواء لأغراض سياسية أو اقتصادية أو عسكرية."

وفي السياق الدولي، تكتسب هذه الهجمات أهمية مضاعفة إذا كانت عابرة للحدود، أو صادرة عن جهات سيادية أو خاصة تتقاطع مصالحها مع الأمن القومي لدولة ما.

ثانيًا: أنواع الهجمات السيبرانية

يمكن تصنيف الهجمات السيبرانية من حيث طبيعتها والغرض منها إلى ما يلي:

1. هجمات تعطيلية (Disruptive Attacks):

تهدف إلى تعطيل الأنظمة عن العمل، كالهجمات على الشـــبكات الكهربائية أو المصـــارف أو خدمات الإنترنت.

2. هجمات تدميرية (Destructive Attacks):

تُســـتخدم فيها برمجيات خبيثة لتدمير البنية التحتية للمعلومات مثل الفيروســـات والبرمجيات المدمرة (Malware).

3. هجمات التجسس الإلكتروني (Cyber Espionage):

تهدف إلى سرقة المعلومات والبيانات الحساسة، سواء من جهات حكومية أو شركات.

4. هجمات التأثير (Influence Operations):

تستخدم لأغراض التضليل والتلاعب بالمعلومات أو التلاعب بالرأي العام، كما حصل في بعض الانتخابات العالمية.

5. الهجمات ذات الطابع الحربي (Cyber Warfare):

وهي الهجمات التي تُنفذ خلال نزاع مسلح، وتُستخدم فيها أدوات سيبرانية لأغراض عسكرية صرفة، وغالبًا ما تنفذها أجهزة استخبارات أو جهات رسمية.

ثالثاً: الفاعلون الرئيسيون في الهجمات السيبرانية

1.الدول:(States)

تمتلك بنى تحتية رقمية وقدرات متقدمة، وتســـتخدم الهجمات الســـيبرانية كأداة لتحقيق أهداف سياسية أو عسكرية.

2. الجهات غير الحكومية (Non-State Actors):

تشـمل الجماعات الإرهابية أو القراصـنة السـيبرانيين الذين يسـعون لتحقيق مكاسـب مالية أو إيديولوجية.

3. الشركات الخاصة (Private Corporations):

http://joshuc.edu.iq ISSN: 2079 -7486

قد تكون فاعلة بشكل مباشر أو غير مباشر سواء بالتورط، أو بعدم اتخاذ تدابير وقائية كافية ضد الهجمات.

4. التحالفات السيبرانية:

وهي مجموعات تضـــم دولًا أو شـــركات تتعاون في تنفيذ أو مواجهة الهجمات، وغالبًا ما تكون غير رسمية.

المبحث الثاني: الطبيعة القانونية للهجمات السيبرانية في القانون الدولي العام

أولاً: موقع الهجمات السيبرانية في القانون الدولي التقليدي

ينقسم القانون الدولي العام في تنظيمه للنزاعات إلى:

- قانون السلمPeace Law
- قانون الحرب (القانون الدولي الإنساني)

ولا يوجد نص صريح في المواثيق الدولية يعالج الهجمات السيبرانية، لكن بعض المبادئ العامة تنطبق عليها، كعدم التدخل في الشؤون الداخلية للدول، وحظر استخدام القوة.

ثانيًا: مبدأ حظر استخدام القوة

وفقًا للمادة (4/2) من ميثاق الأمم المتحدة، يُحظر على الدول اســـتخدام القوة ضـــد ســـلامة الأراضـي أو الاستقلال السياسـي لأي دولة. والسؤال المطروح هو: هل الهجوم السـيبراني يُعد "استخدامًا للقوة"؟

ترى لجنة "تالين" التابعة لحلف الناتو أن بعض الهجمات الســيبرانية يمكن أن تُعتبر اســتخدامًا للقوة إذا نتج عنها آثار مادية تماثل الهجوم العســـكري التقليدي، مثل تعطل منشـــآت الطاقة أو وسائل النقل.

http://joshuc.edu.iq ISSN: 2079 -7486

ثالثًا: مبدأ عدم التدخل

يحظر القانون الدولي تدخل دولة في الشؤون الداخلية لدولة أخرى، سواء بشكل مباشر أو غير مباشر. ويشمل ذلك التدخل عبر الفضاء السيبراني، كالتأثير على الانتخابات، أو دعم جماعات داخلية معارضة.

رابعًا: قاعدة السيادة الرقمية

تُعد السيادة أحد المبادئ الأساسية في القانون الدولي، وتنصرف في العصر الرقمي إلى ما يُعرف بـ"السيادة السيبرانية"، أي حق الدولة في السيطرة على بنيتها التحتية الرقمية ومصادر معلوماتها. إلا أن هذه القاعدة ما زالت في طور التكوين القانوني ولم تحظَ باعتراف عالمي موحد.

خامسًا: غياب الإلزام القانوني الدولي

حتى اللحظة، لا توجد اتفاقية دولية شاملة وملزمة تُنظّم الفضاء السيبراني على غرار اتفاقيات جنيف أو قانون البحار. وهذا ما يخلق تحديًا كبيرًا في تحديد المسؤوليات الدولية.

الباب الثاني: مسؤولية الدول عن الهجمات السيبرانية

المطلب الأول: مسؤولية الدول وفقًا لاتفاقيات القانون الدولي

أولاً: الإطار العام لمسؤولية الدول

تنص مسودة مواد مسؤولية الدول عن الأفعال غير المشروعة دولياً، التي أعدتها لجنة القانون الدولي عام 2001، على أن الدولة تتحمل المسؤولية القانونية عن أي فعل يُنسب إليها ويخالف

http://joshuc.edu.iq ISSN: 2079 -7486

التزاماتها الدولية، سواء ارتكبته مؤسساتها الرسمية أو فاعلون من غير الموظفين الرسميين بتوجيه منها أو برعايتها أو بقبولها الضمني.

وبالتالي، فإن الهجمات السيبرانية التي تنفذها دولة أو تُمكِّن تنفيذها تصبح محل مساءلة وفق القانون الدولي، إذا توفرت الشروط الآتية:

1. نسبة الفعل إلى الدولة: ويكون ذلك إذا نفذه موظفون حكوميون، أو جهات خاصة تعمل بتوجيه أو موافقة الدولة.
2. وجود خرق لالتزام دولي: مثل مبدأ عدم استخدام القوة، أو مبدأ عدم التدخل، أو انتهاك السيادة الرقمية لدولة أخرى.
3. غياب المبرر القانوني للفعل: كالدفاع الشرعي أو موافقة الدولة المتضررة.

ثانيًا: تحديات إثبات النسبة والمسؤولية

تعد مسألة "إثبات المسؤولية" في الهجمات السيبرانية من أكثر الإشكاليات تعقيدًا، وذلك بسبب:

- الطبيعة الخفية للهجمات الإلكترونية.
- إمكانية استخدام جهات ثالثة أو شبكات "زومبي" (Botnets) لتنفيذ الهجوم.
- صعوبة تتبع مصدر الهجوم بدقة فنية وقانونية.
- استخدام أدوات تقنية تمويهية مثل (VPN, IP Spoofing).

ولذا فإن أغلب الدول تمتنع عن إعلان المسؤولية أو اللجوء إلى المحاكم الدولية لعدم كفاية الأدلة القاطعة.

ثالثًا: موقف ميثاق الأمم المتحدة

رغم أن ميثاق الأمم المتحدة لم يذكر الفضاء السيبراني، فإن مبادئه قابلة للانطباق، ومن بينها:

http://joshuc.edu.iq ISSN: 2079 -7486

- المادة (4/2): حظر استخدام القوة.
- المادة (7/2): عدم التدخل في الشؤون الداخلية.
- المادة (51): الحق في الدفاع الشرعي.

وتجدر الإشارة إلى أن بعض الفقهاء يرون أن هجومًا سيبرانيًا يفضي إلى شلل اقتصادي أو أمني بالغ يمكن أن يُعد "هجومًا مسلحًا"، ما يبرر رد فعل مسلح بموجب المادة (51).

المطلب الثاني: تحليل نماذج عملية للهجمات السيبرانية بين الدول

الهجمات السيبرانية العابرة للحدود: النشأة والنماذج

تُعد الهجمات السيبرانية العابرة للحدود إحدى أبرز المظاهر المعاصرة لتحوّل النزاعات من ساحاتها التقليدية إلى فضاءات رقمية لا تعترف بالحدود السياسية أو الجغرافية. وقد نشأ هذا النمط من الهجمات مع التطور المتسارع لتقنيات الاتصال والحوسبة في أواخر القرن العشرين، لاسيما مع الانتشار الواسع للإنترنت وتحول البنى التحتية الحيوية—من الطاقة والمياه إلى الأنظمة المصرفية والدفاعية—إلى فضاءات تعتمد اعتماداً كاملاً على الشبكات الرقمية. ومع هذا التحول، برز مستوى جديد من التهديدات يمكن أن يُنفَّذ من أي مكان في العالم ليطال دولاً ومؤسسات تبعد آلاف الكيلومترات عن مصدر الهجوم، دون أن يمرّ عبر أي معبر حدودي تقليدي.

وتعود الجذور الأولى للهجمات السيبرانية العابرة للحدود إلى التسعينيات، حين بدأت مجموعات قرصنة منظمة باستخدام الفضاء الإلكتروني لاستهداف شبكات عسكرية وتجارية في دول مختلفة. إلا أن الظاهرة اكتسبت طابعها الاستراتيجي بعد عام 2000، مع دخول الدول نفسها في سباق القدرات السيبرانية، واستخدام الهجمات الرقمية كأداة إسقاطية تستهدف التأثير في خصومها دون الدخول في حرب مباشرة.

وقد شهد العالم نماذج بارزة تعكس خطورة هذه الهجمات، من بينها:

http://joshuc.edu.iq ISSN: 2079 -7486

أولاً: هجوم" ستكسنت2010 – (Stuxnet) "

يُعد من أشـهر الهجمات السـيبرانية العابرة للحدود، حيث اسـتُخدم فيروس متطور لتعطيل أنظمة تخصـيب اليورانيوم في منشـآت نووية إيرانية. أظهر هذا الهجوم قدرة الفضـاء السـيبراني على إحداث أضرار مادية حقيقية في البنى التحتية الصناعية.

- الجهة المتهمة: الولايات المتحدة وإسرائيل.
- الهدف: تدمير أجهزة الطرد المركزي في المنشآت النووية الإيرانية.
- النتيجة: أول استخدام معروف لسلاح إلكتروني فعّال تسبب بأضرار مادية ملموسة.
- الموقف القانوني: رغم أن الهجوم لم يسفر عن ضحايا بشرية، إلا أنه أثار نقاشًا كبيرًا حول ما إذا كان يشكل "استخدامًا للقوة" يخضع لأحكام ميثاق الأمم المتحدة.

ثانيًا: هجوم2017 – "NotPetya"

- الجهة المتهمة: روسيا (حسب ادعاء عدة دول غربية).
- الهدف: تعطيل شبكات ومؤسسات في أوكرانيا، وتسبب بأضرار لشركات دولية.
- النتيجة: خسائر مالية بمليارات الدولارات، وتوقف أنظمة خدمات عامة.
- الموقف القانوني: أدى الهجوم إلى دعوات لوضـــع اتفاقية دولية تحظر اســـتخدام البرمجيات الخبيثة، وتحدد مسؤولية الدول عنها.

ثالثًا: التدخل السيبراني في الانتخابات الأمريكية – 2016

- الجهة المتهمة: روسيا.
- الهدف: التأثير على نتائج الانتخابات الرئاسـية من خلال اختراق البريد الإلكتروني وتسـريب المعلومات والتضليل عبر وسائل التواصل.

• النتيجة: أزمة دبلوماسية بين واشنطن وموسكو، وفرض عقوبات أمريكية.

• الموقف القانوني: اعتُبر التدخل السيبراني خرقًا لمبدأ عدم التدخل في الشؤون الداخلية، رغم عدم وجود قاعدة دولية واضحة بشأن التلاعب بالمعلومات الرقمية.

رابعاً: **الهجمات الروسية على إستونيا عام 2007**

تعرضت إستونيا لسلسلة هجمات سيبرانية واسعة عطّلت مؤسسات حكومية ومصارف ووسائل إعلام. وقد مثّلت هذه الواقعة أول مثال لنزاع رقمي واسع يستهدف دولة بأكملها عبر الحدود.

خامساً: **هجوم "WannaCry" عام 2017**

وهو هجوم فدية عالمي استهدف أكثر من 150 دولة، وأصاب أنظمة طبية ونقل واتصالات. وقد أبرز هذا الهجوم طبيعة الترابط الشبكي العالمي، إذ يمكن لرمز خبيث واحد الانتشار دولياً خلال ساعات قليلة.

سادساً: هجمات "SolarWinds" عام 2020

استهدفت الهجمة سلاسل التوريد الرقمية عبر اختراق تحديثات برامج موثوقة، مما أدى إلى الوصول غير المشروع إلى شبكات حكومية في الولايات المتحدة ودول أخرى، في سابقة كشفت هشاشة البنية السيبرانية العالمية المشتركة.

وتشير هذه النماذج إلى أن الهجمات السيبرانية العابرة للحدود لم تعد مجرد أفعال فردية أو حوادث تقنية معزولة، بل أصبحت جزءاً من بنية النزاعات السياسية والعسكرية والاقتصادية الحديثة. كما تؤكد على الحاجة الملحة إلى تطوير أطر قانونية دولية قادرة على استيعاب خصوصية هذه الهجمات التي تتجاوز الحدود وتطال سيادة الدول في الفضاء الرقمي.

الباب الثالث: مسؤولية الشركات الخاصة في الهجمات السيبرانية

المبحث الأول: التكييف القانوني لدور الشركات الخاصة في الفضاء السيبراني

أولًا: صعود دور الشركات في بيئة الأمن السيبراني

في العقدين الأخيرين، تحولت الشركات الخاصة، لا سيما تلك العاملة في قطاع التكنولوجيا، إلى فاعلين مؤثرين في الفضاء السيبراني العالمي، سواء كمطورين للأدوات الرقمية أو كمشغلين للبنى التحتية أو كمزودين لخدمات الأمن السيبراني. وهذا الدور المتنامي يجعلها إما أدوات مباشرة للهجمات أو حاضنات غير مباشرة لها، عن قصد أو غير قصد.

بعض هذه الشركات تقوم بتطوير أدوات هجومية تُباع لحكومات أو جهات مشبوهة، مثل:

- شركات أمن سيبراني تنتج برمجيات تجسسية (مثل "NSO Group" وبرنامج "Pegasus")
- شركات تقدم خدمات Cloud وتستضيف مواقع تنفذ منها هجمات سيبرانية
- شركات تتقاعس في تفعيل أنظمة حماية كافية تُمكّن المهاجمين من استغلالها

ثانيًا: التكييف القانوني لمسؤولية الشركات

في ضوء القانون الدولي العام، لا تُعد الشركات الخاصة فاعلًا أصليًا في قواعد المسؤولية الدولية، التي صُممت في الأساس لتنظيم علاقات الدول. إلا أن التطورات الحديثة تفرض تحديًا لهذا النموذج، مما أدى إلى:

1. بروز مبدأ "المسؤولية غير المباشرة"

إذ قد تتحمل الدولة المسؤولية إذا تبيّن أن شركة تعمل تحت إشرافها أو برعايتها ارتكبت أفعالًا إلكترونية ضارة.

2. إدراج بعض الشركات ضمن مفهوم "الفاعل غير الحكومي"

خاصة إذا كانت تعمل في مناطق نزاع أو مع أطراف ذات أهداف سياسية أو عسكرية.

3. إمكانية مساءلة الشركات بموجب القانون الدولي لحقوق الإنسان

إذا أسهمت أعمالها في انتهاكات واسعة، كالتجسس، قمع الصحفيين، أو تعطيل شبكات الصحة أو التعليم.

المبحث الثاني: مدى مسؤولية الشركات المدنية والجنائية في القانون الداخلي والدولي

أولًا: المسؤولية المدنية

تُعد المسـؤولية المدنية من أبرز أشـكال المحاسـبة المطبقة على الشـركات في حالة تورطها في أفعال إلكترونية ضارة. تشمل هذه المسؤولية:

- التعويض عن الأضرار الناتجة عن الإهمال الأمني
- إعادة بناء النظم المتضررة أو البنية التحتية الرقمية
- الالتزام بالإصلاح المؤسسي لمنع تكرار الخرق

ومع ذلك، تختلف تطبيقات هذه المسؤولية من دولة إلى أخرى، بحسب:

- التشريعات الوطنية للأمن السيبراني
- قدرة الدول على فرض اختصاصها القضائي العابر للحدود
- الاتفاقيات الثنائية حول تبادل البيانات والتعاون القانوني

ثانيًا: المسؤولية الجنائية

بعض الدول بدأت تقنين مسؤولية الشركات عن الجرائم السيبرانية، خصوصًا في الحالات التي تتورط فيها إدارات الشركة بشكل مباشر، ومنها:

- تسهيل الهجوم، من خلال بيع أدوات اختراق.
- التقاعس عن تبليغ الجهات المعنية بعد حدوث اختراق.
- انتهاك قوانين حماية البيانات الشخصية (GDPR، CCPA، وغيرها).

ورغم أن القانون الدولي لا يُلزم الشـــركات بنفس القواعد المطبقة على الدول، فإن التوجه نحو تطوير اتفاقية دولية يُلزم حتى الفاعلين من القطاع الخاص صار أمرًا مطروحًا وبقوة.

ثالثًا: ممارسات دولية بارزة

• الاتحاد الأوروبي من خلال اللائحة العامة لحماية البيانات (GDPR) فرض عقوبات بمليارات اليوروهات على شركات تورطت في خروقات أمنية.
• الولايات المتحدة لديها قوانين فدرالية تلزم الشركات بالإبلاغ عن الهجمات.
• الأمم المتحدة لا تزال تناقش مسؤولية القطاع الخاص من خلال "اللجنة الحكومية لبحث الأمن السيبراني" دون أن تُقر معايير ملزمة حتى اليوم.

الباب الرابع: التحديات القانونية الناشئة عن الفراغ التشريعي الدولي في الأمن السيبراني

المبحث الأول: غياب اتفاقية دولية شاملة لتنظيم الفضاء السيبراني

أولاً: غياب إطار قانوني موحد

رغم تزايد التهديدات السيبرانية على السلم والأمن الدوليين، لم يتم التوصل حتى اليوم إلى اتفاقية دولية شاملة تحكم سلوك الدول والجهات الخاصة في الفضاء السيبراني. ويرجع ذلك إلى:
1. الخلافات السياسية بين الدول الكبرى حول التعاريف والمفاهيم (هل الهجوم السيبراني استخدام للقوة أم لا؟).
2. صعوبة تتبع مصدر الهجمات بدقة قانونية قابلة للإثبات.
3. تعارض المصالح السيادية والتجارية بين الدول (خصوصًا بين الولايات المتحدة، روسيا، الصين، والاتحاد الأوروبي).
4. تعدد الجهات الفاعلة: من دول، جماعات مسلحة، شركات خاصة، وحتى أفراد.

ثانيًا: غلبة المبادرات غير الملزمة (Soft Law)
يوجد عدد من المبادرات القانونية غير الملزمة، منها:
• دليل تالين (Tallinn Manual):

وثيقة فقهية أعدتها مجموعة خبراء حول كيفية تطبيق قواعد القانون الدولي على الهجمات السيبرانية، لكنها غير ملزمة قانونًا.

• توصيات الجمعية العامة للأمم المتحدة (مجموعة الخبراء الحكوميين – GGE):

تقدم مبادئ توجيهية عامة، لكن دون طابع إلزامي، منها مبدأ احترام سيادة الدول، وعدم استخدام الفضاء السيبراني لزعزعة استقرار الدول.

• قواعد باريس 2018 وقواعد لاهاي 2019:

تحث الشركات الكبرى على الالتزام بالمعايير الأخلاقية في الأمن السيبراني، لكنها أيضًا ليست ملزمة.

المبحث الثاني: التحديات القانونية والسياسية أمام تنظيم الهجمات السيبرانية

أولاً: إشكالية السيادة السيبرانية

ما زال الجدل قائمًا حول مدى حق الدول في فرض سيطرتها على الفضاء الرقمي الذي يقع داخل حدودها، مع صراع واضح بين:

• الدول التي تدعم الانفتاح (كالولايات المتحدة والاتحاد الأوروبي)

• والدول التي تدعو إلى الرقابة والسيادة الرقمية الصارمة (كالصين وروسيا)

هذا الخلاف يُعطل التوصل إلى اتفاق دولي موحد.

ثانيًا: صعوبة إثبات النسبة والمسؤولية القانونية

كما أشرنا سابقًا، فإثبات أن دولة ما أو شركة تقف خلف هجوم سيبراني مسألة شديدة التعقيد تقنيًا وقانونيًا، إذ:

• تُستخدم تقنيات التمويه وتزييف العناوين (IP Spoofing).

• قد يتم تنفيذ الهجوم من أراضٍ تابعة لدول أخرى دون علمها.

• تنشط "مجموعات وسيطة" يصعب الربط بينها وبين جهات رسمية بشكل مباشر.

ثالثًا: ضعف آليات الردع والعقوبة

لا توجد حتى اليوم:

• محكمة دولية مختصة بالفضاء السيبراني
• آليات جزائية دولية لردع الدول والشركات
• إلزام قانوني بنظام التعويض عن الأضرار الناتجة عن الهجمات

وهذا يُسهم في إفلات العديد من الجهات من العقاب.

رابعًا: تعارض التشريعات الوطنية

في ظل غياب التشريع الدولي الموحد، ظهرت تشريعات وطنية متباينة قد تتصادم:

• بعض الدول تعتبر الرقابة الإلكترونية "وسيلة دفاع مشروعة".
• أخرى تصنفها "اعتداءً على الخصوصية".
• قوانين حماية البيانات تختلف جذريًا من مكان لآخر.

المبحث الثالث: الحاجة إلى تطوير إطار قانوني دولي شامل

أولاً: عناصر الاتفاقية المقترحة

أي اتفاقية دولية مستقبلية لتنظيم الأمن السيبراني يجب أن تتضمن:

1. تعريف موحد للهجوم السيبراني
2. تصنيف واضح للأعمال المحظورة رقمياً
3. تحديد مسؤولية الدولة والشركات
4. آليات لحل النزاعات السيبرانية دوليًا

http://joshuc.edu.iq ISSN: 2079 -7486

5. نظام للإبلاغ والإنذار المبكر
6. تعويض الدول المتضررة

ثانيًا: دور المنظمات الدولية

- الأمم المتحدة عبر مجلس الأمن والجمعية العامة يمكنها الدفع نحو صياغة اتفاق ملزم.
- الاتحاد الأوروبي يمكن أن يكون نموذجًا إقليميًا متقدمًا لتنظيم الأمن السيبراني.
- المنظمة الدولية للاتصالات (ITU) يمكنها التنسيق الفني والإشراف على البنية التحتية العالمية للإنترنت.

الباب الخامس: العراق أنموذجًا – التحديات والتشريعات الوطنية في مواجهة الهجمات السيبرانية

المبحث الأول: واقع الأمن السيبراني في العراق

أولًا: التحديات السيبرانية في العراق

يعاني العراق من عدد من التحديات البنيوية في قطاع الأمن السيبراني، أبرزها:

1. البنية التحتية الرقمية الضعيفة:

معظم الشبكات في المؤسسات الحكومية غير محمية بأنظمة أمنية متطورة، ما يجعلها عرضة للاختراق.

2. غياب استراتيجية وطنية موحدة للأمن السيبراني:

بالرغم من محاولات صياغة "الاستراتيجية الوطنية للأمن السيبراني" بالتعاون مع جهات دولية، إلا أن التنفيذ ما زال بطيئًا ومجزأً.

3. التعدد المؤسساتي وتداخل الاختصاصات:

http://joshuc.edu.iq ISSN: 2079 -7486

تتداخل مسؤوليات وزارات الاتصالات، والداخلية، وجهاز الأمن الوطني، وهيئة الإعلام والاتصالات، دون تنسيق مركزي فعال.

4. التهديدات المستمرة من جهات داخلية وخارجية:

تشمل هجمات على مواقع حكومية، محاولات تجسس، نشر المعلومات المضللة، والتلاعب بالبيانات البنكية والطبية.

المبحث الثاني: الإطار القانوني للأمن السيبراني في العراق

أولًا: غياب قانون خاص للأمن السيبراني

حتى لحظة إعداد هذا البحث، لا يمتلك العراق قانونًا شاملًا لتنظيم الأمن السيبراني، رغم تعدد المحاولات التشريعية التي بقيت في أروقة البرلمان، ومن أبرزها:

- مشروع قانون الجرائم المعلوماتية (2011، 2019، و2023):

واجهت هذه المسودات انتقادات حادة من المجتمع المدني بسبب بعض المواد التي اعتُبرت مهددة لحرية التعبير، ولم يتم إقرار أي منها بشكل رسمي حتى الآن.

ثانيًا: التشريعات المساندة ذات الصلة

1. قانون العقوبات العراقي رقم 111 لسنة 1969 (المعدل):

لا يشمل صراحة الجرائم الإلكترونية، لكنه يحتوي على مواد يمكن أن تطبق تأويليًا في بعض الحالات.

2. قانون الاتصالات والمعلوماتية (مسودة):

يعالج بعض القضايا التقنية، لكن لم يُقر نهائيًا.

3. قانون الهيئة الوطنية للأمن السيبراني (مقترح):

طُرح في مجلس النواب لتأسيس هيئة متخصصة، لكنه لم يُفعّل رسميًا.

4. قانون حماية الخصوصية والبيانات الشخصية (مقترح):

لا يزال في مراحل النقاش الفني ولم يُشَرَّع حتى الآن.

المبحث الثالث: مسؤولية الدولة العراقية والشركات الخاصة عن الهجمات السيبرانية

أولًا: مسؤولية الدولة العراقية

الدولة تتحمل مسؤولية مزدوجة:

1. حماية مواطنيها ومؤسساتها من الهجمات الرقمية، وفق مبدأ "واجب الحماية" الذي يستند إلى القانون الدولي العام.
2. تنظيم الفضاء السيبراني الوطني، وتوفير إطار قانوني للمساءلة والرقابة ومنع استخدام الأراضي العراقية في شن هجمات على دول أخرى.

لكن واقع الحال يُظهر أن العراق:

- لا يمتلك جهات تحقيق رقمية متخصصة بقدرات تقنية متقدمة.
- لا يشارك بفعالية في المبادرات الدولية لمكافحة الجريمة الإلكترونية.
- يعتمد على التعاون التقني المحدود مع بعض الدول والمنظمات.

ثانيًا: مسؤولية الشركات العراقية

مع توسع القطاع الخاص الرقمي، خاصة في مجالات الاتصالات والخدمات المصرفية، أصبحت الشركات مطالَبة بـ:

- اعتماد أنظمة حماية معلومات متقدمة
- الإبلاغ عن الاختراقات فورًا
- حماية بيانات العملاء بموجب معايير دولية (ISO 27001، PCI DSS)

لكن في الواقع:

http://joshuc.edu.iq ISSN: 2079 -7486

- لا توجد جهة رقابية متخصصة تفرض هذه المعايير.
- معظم الشركات الصغيرة والمتوسطة تفتقر للوعي السيبراني الكافي.
- لا توجد عقوبات واضحة تُطبق في حال تقصير الشركات في الحماية.

الباب الســـادس: مقترحات إصـــلاحية لتطوير النظام القانوني الدولي والوطني في مجال الأمن السيبراني

المبحث الأول: مقترحات لتطوير الإطار القانوني الدولي للأمن السيبراني

أولاً: ضرورة وضع اتفاقية دولية شاملة وملزمة

ينبغي أن تبادر الأمم المتحدة أو عبر مجلس الأمن أو الجمعية العامة، إلى صـــياغة اتفاقية دولية للأمن السيبراني، تأخذ في الاعتبار النقاط التالية:

1. وضع تعريف موحد للهجمات السيبرانية وتحديد نطاق استخدام القوة الرقمية.
2. تحديد المسؤولية القانونية للدول عن الأفعال السيبرانية التي تقع من داخل أراضيها.
3. إدراج مسؤولية الفواعل غير الدولاتية، مثل الشركات الخاصة، والمنظمات غير الحكومية.
4. إنشاء آلية دولية لحل النزاعات السيبرانية ومحاسبة الجناة.
5. وضع نظام دولي لتعويض الدول المتضررة.

ثانيًا: تعزيز مبادئ الشفافية والتعاون الدولي

- إلزام الدول بالإبلاغ عن الهجمات التي تستهدف بنيتها التحتية الرقمية.
- توسيع نطاق اتفاقيات التعاون القضائي الدولي لتشمل الجرائم السيبرانية.
- دعم جهود "التحقيق الرقمي المشترك" بين الدول.

ثالثًا: إنشاء هيئة دولية مختصة بالفضاء السيبراني

- تكون على غرار "الوكالة الدولية للطاقة الذرية"، وتتمتع بصلاحيات رقابية واستشارية.
- تُشرف على المعايير التقنية والأمنية الدولية.
- تُصدر تقارير دورية عن التهديدات السيبرانية العابرة للحدود.

المبحث الثاني: مقترحات لتطوير التشريعات الوطنية في العراق

أولًا: إقرار قانون شامل للأمن السيبراني

يجب أن يُصاغ ويُقر قانون وطني جديد يعالج:

1. تعريف الهجمات السيبرانية وتوصيفها الجنائي.
2. تحديد مسؤوليات الجهات الحكومية والخاصة.
3. إنشاء هيئة وطنية مستقلة للأمن السيبراني ترتبط بمجلس الأمن الوطني، وتملك صلاحيات رقابية وتنفيذية.

ثانيًا: بناء القدرات الرقمية في المؤسسات الحكومية

- تدريب كوادر متخصصة في التحقيق السيبراني والتحليل الجنائي الرقمي.
- اعتماد بروتوكولات استجابة وطنية موحدة للهجمات السيبرانية.
- الربط الشبكي الآمن بين الوزارات والمؤسسات الحيوية.

ثالثًا: تنظيم قطاع الشركات الخاصة والتزاماتها الرقمية

- إلزام الشركات الكبرى في قطاعات الاتصالات، المصارف، والخدمات الإلكترونية بـ:
- اعتماد أنظمة أمن معلومات متقدمة (مثل ISO 27001).
- الإبلاغ الفوري عن الاختراقات.

- تدريب موظفيها على الأمن السيبراني.
- إنشاء هيئة رقابية متخصصة تتابع التزام القطاع الخاص بالمعايير.

رابعًا: التعاون الإقليمي والدولي

- الانضمام الفاعل للاتفاقيات الدولية الخاصة بالأمن السيبراني (مثل اتفاقية بودابست).
- إنشاء مراكز استجابة وطنية (CERTs) للتواصل مع نظيراتها في المنطقة والعالم.
- المشاركة في التمارين السيبرانية الدولية.

المبحث الثالث: دور المجتمع الأكاديمي والمجتمع المدني في تعزيز الأمن السيبراني

أولًا: المجتمع الأكاديمي

- دعم البحث العلمي في مجالات الأمن السيبراني من الناحية القانونية والتقنية.
- إنشاء برامج دراسات عليا متخصصة في القانون السيبراني.
- إعداد كوادر متخصصة للعمل في المؤسسات السيادية والرقابية.

ثانيًا: المجتمع المدني

- نشر الوعي الرقمي بين المواطنين حول حماية البيانات الشخصية والخصوصية.
- مراقبة تنفيذ التشريعات وضمان عدم تحولها إلى أدوات رقابة سياسية.
- الدفع نحو شفافية القرارات المتعلقة بتنظيم الفضاء الرقمي.

الخاتمة

في ظل التطور الهائل للتكنولوجيا الرقمية وانتشار الهجمات السيبرانية، أصبح الأمن السيبراني قضـية أسـاسـية تؤثر على السـيادة الوطنية والأمن الدولي. أظهر هذا البحث أن القانون الدولي العام يواجه تحديات كبيرة في تنظيم سـلوك الدول والشـركات الخاصـة في الفضـاء السـيبراني بسـبب غياب اتفاقية دولية ملزمة، وتعقيدات إثبات المسـؤولية القانونية، بالإضـافة إلى تعدد الفاعلين وتضـارب المصـالح. كما بيّن البحث أن العراق، كحالة دراسية، يعاني من ضـعف البنية التحتية التشريعية والمؤسساتية لمواجهة هذه التهديدات، حيث لا يمتلك قانوناً شاملاً ينظم الأمن السيبراني ويعاقب على الهجمات الإلكترونية.

إن تحقيق الأمن السـيبراني يتطلب تعاوناً دولياً وإقليمياً قوياً، بالإضـافة إلى تطوير تشـريعات وطنية متطورة تلبي التحديات التقنية والقانونية. لذا، من الضـروري إقرار إطار قانوني متكامل يجمع بين الضـبط القانوني الفعال والمسؤولية الواضـحة للدول والشـركات الخاصـة، مع تعزيز القدرات التقنية والمؤسسية.

http://joshuc.edu.iq ISSN: 2079 -7486

النتائج

1. غياب إطار قانوني دولي ملزم للأمن السـيبراني يخلق فراغاً قانونياً يجعل من الصـعب محاسبة الفاعلين الدوليين وغير الدوليين.

2. عدم وضـوح مسـؤولية الدول والشـركات الخاصـة يؤدي إلى اسـتغلال الثغرات القانونية في شن الهجمات السيبرانية دون رادع حقيقي.

3. التحديات التقنية والقانونية في إثبات النسـبة تعوق الإجراءات القضـائية وتزيد من إفلات المجرمين من العقاب.

4. العراق يعاني من ضعف البنية التشريعية والتنظيمية في مجال الأمن السيبراني، ويحتاج إلى تطوير قوانين وإجراءات متكاملة.

5. التنسيق بين الجهات الوطنية مختلف وغير كافٍ، مما يضعف الاستجابة للهجمات السيبرانية واحتواء آثارها.

6. نقص الوعي والتدريب في القطاع الخاص يساهم في تفاقم الثغرات الأمنية.

http://joshuc.edu.iq ISSN: 2079 -7486

التوصيات

1. إقرار قانون وطني شـامل للأمن السـيبراني في العراق يحدد التعاريف، العقوبات، والجهات المسؤولة، مع ضمان حماية الحقوق الأساسية وحريات التعبير.

2. إنشـاء هيئة وطنية مسـتقلة ومتخصـصـة في الأمن السـيبراني تعمل على الرقابة، التحقيق، والتنسيق بين الجهات الحكومية والخاصة.

3. تبني استراتيجية وطنية شاملة للأمن السيبراني تشمل بناء القدرات التقنية، التدريب، تطوير البنية التحتية، وتوعية المجتمع المدني.

4. الانضـمام الفاعل للاتفاقيات الدولية المتعلقة بالأمن السـيبراني، والعمل على التنسـيق مع المنظمات الدولية مثل الاتحاد الدولي للاتصالات ومنظمة الأمم المتحدة.

5. فرض معايير أمنية صـارمة على الشـركات الخاصـة، خاصـة في قطاعات الاتصـالات والمصارف، وإلزامها بالإبلاغ عن الهجمات فور وقوعها.

6. تطوير آليات قانونية دولية ملزمة لتنظيم الفضـاء السـيبراني، تتضـمن آليات حل نزاعات فعالة، نظام تعويض عادل، وتحديد مسؤولية الفواعل غير الدوليين.

7. تشجيع البحث العلمي والدراسات الأكاديمية في القانون السيبراني لتعزيز المعرفة والابتكار في هذا المجال.

8. تعزيز دور المجتمع المدني في الرقابة والمناصـرة لضـمان تطبيق القوانين وحماية الحقوق الرقمية.

Summary

Title: International Public Law, State and Private Companies' Responsibility, and Cybersecurity Challenges
Introduction:
The rapid advancement of digital technology and the increasing reliance on cyberspace have made cybersecurity a critical issue for national sovereignty and international security. Cyberattacks can destabilize governments, disrupt critical infrastructure, and violate individual rights, creating complex challenges for international public law. This research explores the legal frameworks governing state and private actors' responsibilities regarding cybersecurity threats, focusing on international law principles and the specific challenges faced by Iraq.

Main Body:
1. International Legal Framework:
Currently, there is no binding international treaty that comprehensively regulates state responsibility in cyberspace. Although principles of sovereignty, non-intervention, and the prohibition of the use of force apply, their application to cyber operations remains ambiguous. States struggle to attribute cyberattacks definitively to other states or non-state actors, complicating accountability. The research highlights the urgent

need for an international treaty that clearly defines cyberattacks, sets rules for state responsibility, and includes mechanisms for dispute resolution and sanctions.

2. Private Sector Responsibilities:

With private companies increasingly operating critical infrastructure and digital platforms, their role in cybersecurity governance has grown. However, international law lacks clear regulations imposing obligations or liabilities on private entities in cyberspace. This gap creates vulnerabilities exploited by malicious actors. The research emphasizes the necessity of legal frameworks that bind private companies to cybersecurity standards, incident reporting, and cooperation with state authorities.

3. Case Study: Iraq's Cybersecurity Landscape:

Iraq faces multiple cybersecurity challenges, including weak digital infrastructure, fragmented institutional roles, and the absence of comprehensive cybersecurity legislation. Current laws are outdated or non-existent, and there is no dedicated cybersecurity authority. These gaps expose Iraq to persistent cyber threats, undermining national security and economic stability. The research underscores the need for Iraq to enact a robust cybersecurity law, establish an independent cybersecurity agency, and foster regional and international cooperation.

Conclusions:

Cybersecurity threats transcend national borders, demanding a coordinated legal response that integrates international and domestic law. The research concludes that:

• International law must evolve to provide clear, binding rules on state and private actor responsibilities in cyberspace.

• Iraq must urgently reform its cybersecurity legal and institutional frameworks to address emerging threats effectively.

• Multilateral cooperation and capacity building are essential for sustainable cybersecurity governance.

Recommendations:

• Adoption of an international cybersecurity treaty that defines cyber

operations, clarifies state responsibility, and establishes enforcement mechanisms.
• Development and enforcement of national cybersecurity legislation in Iraq, including clear roles for government agencies and private companies.
• Creation of an independent national cybersecurity authority with investigative and regulatory powers.
• Mandatory cybersecurity standards and incident reporting obligations for private sector entities.
• Strengthening regional and international cooperation through information sharing and joint cyber defense exercises.
• Investment in cybersecurity education, research, and public awareness programs.

قائمة المصادر والمراجع

كتب ومراجع أساسية:

أولاً: المراجع العربية

1. شميت، مايكل ن. (محرر). (2017). *دليل تالين 2.0 بشأن القانون الدولي المنطبق على العمليات السيبرانية*. مطبعة جامعة كامبريدج.
—مرجع أساسي في فهم سريان القانون الدولي على الفضاء السيبراني.
2. مولر، ميلتون. (2010) *الشبكات والدول: السياسة العالمية لحوكمة الإنترنت*. معهد ماساتشوستس للتكنولوجيا.
—تحليل معمّق لحوكمة الإنترنت وعلاقة الدول بها.
3. كافلتي، ميريام دنمار. (2014) *الأمن السيبراني وسياسات التهديد: الجهود الأمريكية لتأمين عصر المعلومات*. روتليدج.
—دراسة شاملة للاستراتيجيات والسياسات السيبرانية الأمريكية.
4. ليندسي، جون ر. (2013). "هجوم ستاكسنت وحدود الحرب السيبرانية". *مجلة الدراسات الأمنية*، 22(3)، 365-404.
- بحث متخصص حول هجوم ستاكسنت وتأثيره على مفاهيم الحرب الإلكترونية.

5. شميت، مايكل ن. (2013). "العمليات السيبرانية ومبدأ اللجوء إلى القوة من جديد ." *دراسات القانون الدولي*، 89، 1-39 .
- تحليل قانوني لاستخدام القوة في الفضاء السيبراني.
6. هاثاوي، أورلي، وآخرون. (2012). "قانون الهجمات السيبرانية ."*مجلة كاليفورنيا للقانون*، 100(4)، 817-885.
- دراسة شاملة للقواعد القانونية المنظمة للهجمات السيبرانية.
7. تيك، إيلين؛ كاسكا، كريستيان؛ فيهول، لي. (2010) *الحوادث السيبرانية الدولية: اعتبارات قانونية* .منشورات مركز الدفاع السيبراني التعاوني (الناتو).
- دراسة متخصصة في الاعتبارات القانونية للحوادث السيبرانية.
8. مجموعة الخبراء الحكوميين للأمم المتحدة .(2015). (UNGGE) *تقرير مجموعة الخبراء الحكوميين بشأن التطورات في مجال المعلومات والاتصالات في سياق الأمن الدولي* .الأمم المتحدة.
- تقرير دولي حول قواعد السلوك والمسؤوليات في الفضاء السيبراني.
9. الاتحاد الدولي للاتصالات. (2020) *مؤشر الأمن السيبراني العالمي* .منشورات الاتحاد الدولي للاتصالات.
- تقييم دولي لقدرات الدول في الأمن السيبراني.
10. مجلس أوروبا. (2001) *اتفاقية بودابست بشأن الجرائم السيبرانية* .
- أول اتفاقية دولية متخصصة في مكافحة الجرائم الإلكترونية.
11. **قانون العقوبات العراقي رقم 111 لسنة (1969)** المعدل
- التشريعات الجزائية العراقية المتصلة بالجرائم الإلكترونية.
12. **مشروع قانون الجرائم المعلوماتية في العراق** سنوات متعددة.
- المسودات التشريعية المنظمة للفضاء السيبراني في العراق.

ثانياً: المراجع الأجنبية (English Sources)

1. Schmitt, M. N. (Ed.). (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge University Press.
— A foundational resource on the application of international law to cyber operations.
2. Mueller, M. (2010). *Networks and States: The Global Politics of Internet Governance*. MIT Press.
— A comprehensive analysis of Internet governance and its geopolitical implications.

3. Cavelty, M. D. (2014). *Cybersecurity and Threat Politics: US Efforts to Secure the Information Age*. Routledge.
— A detailed study of U.S. cybersecurity strategy from legal and political perspectives.
4. Lindsay, J. R. (2013). Stuxnet and the limits of cyber warfare. *Security Studies*, 22(3), 365–404. https://doi.org/10.1080/09636412.2013.816122
— A critical examination of the Stuxnet incident and its strategic implications.
5. Schmitt, M. N. (2013). Cyber operations and the *jus ad bellum* revisited. *International Law Studies*, 89, 1–39.
— A legal reassessment of the use of force in cyberspace.
6. Hathaway, O. A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., & Spiegel, J. (2012). The law of cyber-attack. *California Law Review*, 100(4), 817–885. https://doi.org/10.15779/Z38G44M
— An extensive legal analysis of international law governing cyberattacks.
7. Tikk, E., Kaska, K., & Vihul, L. (2010). *International Cyber Incidents: Legal Considerations*. NATO CCD COE Publications.
— A critical study of legal frameworks applicable to international cyber incidents.
8. United Nations Group of Governmental Experts (UNGGE). (2015). *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. United Nations.
— A UN report outlining norms of behavior in cyberspace.
9. International Telecommunication Union (ITU). (2020). *Global Cybersecurity Index*. ITU Publications.
— A global assessment of states' cybersecurity readiness.
10. Council of Europe. (2001). *Convention on Cybercrime (Budapest Convention)*.
— The first international treaty addressing cybercrime.

11. Iraqi Penal Code No. 111 of 1969 (as amended).
— National legislation relevant to cyber-related offenses.
12. Republic of Iraq. *Draft Cybercrime Law* (various years).
— Draft legal frameworks regulating cybercrime in Iraq.

http://joshuc.edu.iq ISSN: 2079 -7486