Int. J. Media. Mas. Com. Vol. 08, No. 01, 86-119 (2026)
DOI: 10.46988/IJMMC.08.01.2026.05
ISSN: 2536-0035
ISBN: 2535-9797
Arab Impact Factor (1.04) (2021).

IJMMC International Journal For Media Mass Communication &

International Journal of Media and Mass Communication المجلة الدولية للإعلام والاتصال الجماهيري

Cybersecurity and its impact on contemporary international relations: challenges and strategies

Dr. Saleh Obaid Al-Rashed[1]

Associate Professor of Political Science and International Relations

Umm Al Quwain University – United Arab Emirates

Email: drsaleh.alrached@uaqu.ac.ae

Received: 12 July 2025 Revised: 24 August 2025 Accepted: 02 October 2025 Published: 01 Jan 2026

Abstract:

Cybersecurity has emerged as a critical issue in the contemporary era, posing significant challenges to states amid rapid technological advancements and growing dependence on the internet and digital technologies across various sectors. Cyberspace has evolved into a new domain for international interaction, directly impacting national and economic security. This evolution has introduced a range of threats, including attacks on critical infrastructure and cyber espionage. Due to the transnational nature of cyberattacks, international cooperation is imperative to counter these threats and safeguard global stability. Such attacks have the potential to escalate tensions between states, particularly when they target vital or economic systems, thereby affecting diplomatic relations and potentially triggering conflict. Consequently, cybersecurity has become an integral component of national and global security strategies. While modern technologies such as artificial intelligence and cloud computing offer economic advantages, they also introduce novel vulnerabilities. Addressing these threats necessitates comprehensive strategies involving collaboration among governments, as well as international and regional organizations. This research aims to analyze the impact of cyberattacks on international relations, evaluate existing global and regional policies, and propose strategic frameworks to enhance international cooperation and protect cyberspace—ultimately contributing to stability in global relations.

Keywords: Cybersecurity, International Relations, Cyber Threats, Cyberwars, Cyberspace, International Law.

IJMMC
International journal For Media Mass Communication &

الأمن السيبراني وتأثيره على العلاقات الدولية المعاصرة: التحديات والاستراتيجيات

د.صالح عبيد الراشد

قسم العلوم السياسية والعلاقات الدولية جامعة ام القيوين –الامارات العربية المتحدة

ملخص البحث:

أضحى الأمن السيبراني من أبرز القضايا الحيوية في العصر الرقمي الراهن، نتيجة للتطور التكنولوجي المتسارع والاعتماد المتزايد على الإنترنت والتقنيات الرقمية في مختلف المجالات، فقد تحول الفضاء السيبراني إلى ساحة جديدة للتفاعلات والصراعات الدولية، تؤثر بشكل مباشر في الأمن الوطني والاقتصادي للدول، ونتيجة للطبيعة العابرة للحدود للهجمات السيبرانية، تواجه الدول تحديات غير تقليدية تتضمن اختراق البنى التحتية الحيوية، والتجسس الإلكتروني، والتدخل في النظم السياسية والاقتصادية.

في هذا السياق، أصبح التعاون الدولي ضرورة ملحّة لمجابهة هذه التهديدات المتصاعدة، والحفاظ على الاستقرار العالمي، فالهجمات السيبرانية لا تقتصر آثارها على الداخل، بل قد تؤدي إلى تصعيد التوترات بين الدول، لا سيما إذا استهدفت أنظمة حيوية أو مؤسسات استراتيجية، مما قد يؤثر سلبًا على العلاقات الدبلوماسية وربما يؤدي إلى أزمات أو صراعات مفتوحة.

وبناءً على ذلك، بات الأمن السيبراني جزءًا لا يتجزأ من استراتيجيات الأمن القومي والدولي، خاصة مع توسع استخدام تقنيات الذكاء الاصطناعي، والحوسبة السحابية، وإنترنت الأشياء، التي تقدم منافع اقتصادية وإدارية، لكنها تفتح في الوقت نفسه آفاقًا جديدة للتهديدات الإلكترونية.

يهدف هذا البحث إلى تحليل تأثير الأمن السيبراني على العلاقات الدولية من خلال وضع إطارًا تحليليًا متكاملًا يتجاوز المقاربات التقنية البحتة، ويُسهم في بناء فهم أعمق لصيغ التعاون والصراع في الفضاء السيبراني، بهدف ضمان أمن الفضاء الرقمي وتعزيز الاستقرار في العلاقات الدولية.

الكلمات المفتاحية :الأمن السيبراني، العلاقات الدولية، التهديدات السيبرانية، الحروب السيبرانية، الفضاء السيبراني، القانون الدولي.

مقدمة:

في ظل التسارع الكبير في وتيرة التطور التكنولوجي، بات الأمن السيبراني أحد أبرز القضايا التي تفرض نفسها بقوة على أجندة العلاقات الدولية المعاصرة، ومع الانتشار الواسع للتكنولوجيا الرقمية، أصبحت الدول والمؤسسات عرضة لتهديدات سيبرانية متزايدة، تمسّ بشكل مباشر استقرارها الأمني والاقتصادي، ويشكّل الأمن السيبراني ميدانًا جديدًا للتحديات الأمنية، في ظل الهجمات الرقمية العابرة للحدود، التي لا تقتصر آثارها على المجال الداخلي، بل تمتد لتؤثر على العلاقات بين الدول، وتثير إشكاليات متعلقة بالسيادة الوطنية والمساءلة القانونية.

تشمل التهديدات السيبرانية جوانب معقدة ومتعددة، منها التجسس الإلكتروني، والهجمات التي تستهدف البنية التحتية الحيوية، فضلًا عن الصراعات الرقمية التي قد تسهم في تصعيد التوترات الدولية، وربما تؤدي إلى نشوب أزمات أو نزاعات مفتوحة، وفي

هذا السياق، تبرز الحاجة إلى دراسة تأثير الأمن السيبراني على العلاقات الدولية من خلال تحليل التحديات التي تواجه الدول في هذا المجال، واستعراض استراتيجيات التعاون الدولي لمكافحة الجرائم السيبرانية، بالإضافة إلى إبراز دور المنظمات الدولية في وضع أطر قانونية تنظّم استخدام الفضاء السيبراني وتحفظ استقراره.

مشكلة البحث:

تشهد العلاقات الدولية في العصر الرقمي تحولًا جذريًا بفعل التهديدات السيبرانية التي أصبحت تمثل أحد أبرز مصادر التهديد غير التقليدي للأمن القومي للدول، بل وللنظام الدولي برمته، وتتبع مشكلة هذا البحث من التنامي المستمر في حجم وخطورة هذه التهديدات، حيث أصبحت الهجمات السيبرانية تُستخدم كأدوات ضغط سياسي واقتصادي، وقد تؤدي أحيانًا إلى زعزعة الاستقرار الداخلي أو حتى التسبب في نزاعات بين الدول، ويزداد تعقيد المشكلة نظرًا للطبيعة غير المرئية واللا مركزية للفضاء السيبراني، مما يُصعّب من تحديد الجهة المسؤولة عن الهجوم، ويعوق الجهود الدولية للرد الجماعي أو حتى لردع المعتدين.

ويُثير هذا الواقع السيبراني المستجد تساؤلات أساسية حول مدى كفاءة السياسات الدولية القائمة في التعامل مع هذا النوع من التهديدات، وإلى أي مدى يمكن للدول تحقيق الانسجام بين مقتضيات السيادة الوطنية ومتطلبات التعاون الدولي لمجابهة الهجمات العابرة للحدود، كما تشمل مشكلة البحث أبعادًا اقتصادية ودبلوماسية معقدة، حيث تؤثر الهجمات السيبرانية بشكل مباشر على الاستثمارات، والتجارة، وثقة الشعوب في الحكومات، فضلًا عن إمكانية استغلالها في صراعات جيوسياسية عبر ما يُعرف بـ"الحروب السيبرانية."

وتُعد مسألة التنسيق القانوني والمؤسسي بين الدول والمنظمات الدولية من أبرز التحديات المطروحة، خاصة في ظل غياب اتفاقيات ملزمة أو قواعد قانونية دولية شاملة تحكم السلوك في الفضاء السيبراني، كما تتفاقم المشكلة بفعل التفاوت الكبير بين قدرات الدول السيبرانية، مما يخلق فجوة في مستويات الحماية ويزيد من هشاشة الأمن العالمي في هذا المجال، ومن هنا، يهدف البحث إلى تسليط الضوء على هذه الإشكالية المعقدة متعددة الأبعاد، ومحاولة تحليل سبل مواجهتها من خلال التعاون الدولي، وتطوير الاستراتيجيات والسياسات التي توازن بين الحرية الرقمية ومتطلبات الأمن.

أهمية البحث:

تأتي أهمية هذا البحث من واقع التهديدات المتصاعدة التي يفرضها الأمن السيبراني على النظام الدولي في ظل التحول الرقمي الشامل الذي يشهده العالم، حيث أصبحت البنى التحتية الحيوية – مثل شبكات الكهرباء، والمياه، والاتصالات، والمصارف، والمطارات – معتمدة بشكل كلي على نظم المعلومات والاتصالات، مما جعلها أهدافًا محتملة للهجمات السيبرانية، وبات الأمن السيبراني يشكل بعدًا استراتيجيًا لا غنى عنه في صياغة سياسات الأمن الوطني للدول، كما أصبح له تأثير مباشر على مخرجات السياسة الخارجية والعلاقات الدولية، في ضوء تصاعد ما يُعرف بـ"الحروب غير التقليدية" في الفضاء الإلكتروني.

ويكتسب البحث أهمية خاصة لكونه يتناول هذا الموضوع من منظور العلاقات الدولية، متجاوزًا المقاربات التقنية البحتة نحو فهم أعمق لتأثير الفضاء السيبراني على ديناميكيات التفاعل بين الدول، بما يشمله ذلك من أبعاد سياسية، واقتصادية، وقانونية،

ودبلوماسية، كما تسهم الدراسة في تسليط الضوء على الفجوة القائمة بين تطور التهديدات السيبرانية وسرعة استجابة الأطر القانونية والمؤسساتية لها، لا سيما في ظل غياب توافق دولي ملزم بشأن القواعد الناظمة للسلوك في الفضاء السيبراني.

علاوة على ذلك، فإن تناول البحث لدور المنظمات الدولية والإقليمية في بناء استراتيجيات جماعية للتصدي للجرائم السيبرانية يسهم في إبراز أهمية العمل الجماعي في مواجهة التهديدات العابرة للحدود، ويعزز من جهود بناء الأمن الرقمي العالمي، كما أن تقديم توصيات عملية مبنية على تحليل الواقع السيبراني المعاصر من شأنه أن يدعم صانعي القرار والباحثين في تطوير استراتيجيات أكثر فاعلية وتكاملًا لحماية الأمن القومي والسيادة الرقمية للدول.

أهداف البحث:

1. تحليل تأثير التهديدات السيبرانية على الأمن الدولي والعلاقات بين الدول.
2. دراسة استراتيجيات التعاون الدولي والإقليمي لمكافحة الجرائم السيبرانية.
3. استكشاف دور المنظمات الدولية والإقليمية في تطوير أطر قانونية لتنظيم الفضاء السيبراني.
4. تقديم توصيات لتعزيز التعاون بين الدول في مواجهة الهجمات السيبرانية وحماية الأمن السيبراني.
5. تحليل التأثيرات الاقتصادية والدبلوماسية للهجمات السيبرانية على الاستقرار الدولي.

حدود البحث:

- **الحدود الزمنية:** يغطي البحث الفترة الزمنية من عام 2000 حتى الوقت الحالي، حيث تزايدت الهجمات السيبرانية في هذه الفترة بشكل ملحوظ.
- **الحدود الجغرافية:** يركز البحث على الدول الكبرى والمنظمات الدولية مثل الأمم المتحدة والاتحاد الأوروبي، مع إشارة إلى بعض الدول النامية التي تعاني من التحديات المتعلقة بالأمن السيبراني.
- **الحدود الموضوعية:** يتناول البحث التهديدات السيبرانية التي تشمل الهجمات على البنية التحتية الحيوية، والتجسس السيبراني، والهجمات الاقتصادية، وتأثير ذلك على العلاقات الدولية والأمن القومي.

فرضيات البحث:

1. الهجمات السيبرانية تمثل تهديدًا حقيقيًا للأمن القومي للدول، وقد تؤدي إلى تصعيد التوترات السياسية والاقتصادية.
2. التعاون الدولي في مجال الأمن السيبراني يمكن أن يكون له دور حاسم في تقليل تأثير هذه الهجمات وضمان استقرار العلاقات الدولية.
3. القوانين والسياسات الدولية الحالية لا تواكب التطور السريع للتكنولوجيا، مما يستدعي تحديث الأطر القانونية والتنظيمية المتعلقة بالأمن السيبراني.

متغيرات البحث:

1. **التهديدات السيبرانية:** تشمل الهجمات على البنية التحتية الحيوية، التجسس السيبراني، والهجمات الاقتصادية.
2. **الأمن السيبراني:** يشمل السياسات، التقنيات، والإجراءات التي تتبناها الدول والمنظمات لحماية الفضاء السيبراني.
3. **التعاون الدولي:** يشير إلى التنسيق بين الدول والمنظمات الدولية في مواجهة التهديدات السيبرانية.
4. **القوانين والتشريعات:** تشمل القوانين الوطنية والدولية المتعلقة بالأمن السيبراني وتطوير أطر تنظيمية لحماية الفضاء السيبراني.

الدراسات السابقة:

عندما بدأتُ رحلة البحث هذه، كان من المهم بمكان أن أستند إلى أعمال الباحثين السابقين الذين مهدوا الطريق في فهم العلاقة المعقدة بين الأمن السيبراني والعلاقات الدولية. لقد قمت بمراجعة متأنية لعدد من الدراسات التي أثرت هذا المجال، ووجدت أن لكل منها إسهامًا فريدًا في بناء التصور العام لمشكلة البحث، مع وجود نقاط التقاء واختلاف مهمة مع مقاربتي الخاصة.

1. إيمان عبد القادر، "أثر الفضاء السيبراني على الأمن القومي العربي خلال الفترة من 2011 حتى 2023(2024) "

ملخص الدراسة :قدمت الباحثة إيمان عبد القادر دراسة قيّمة تركز على تأثير الفضاء السيبراني على الأمن القومي العربي في فترة حساسة وحافلة بالتحولات (2011–2023). صدرت هذه الدراسة مؤخرًا في مجلة "الأمن القومي والإستراتيجية"، وتميزت بمعالجتها المفاهيمية الواضحة لمصطلحات مثل "الفضاء السيبراني"، "الأمن القومي"، و"الأمن السيبراني"، مما رسخ قاعدة نظرية قوية. اعتمدت الباحثة المنهج الوصفي التحليلي، مركزة على تحليل البيانات حول واقع الأمن السيبراني في الدول العربية من جوانبها المؤسسية والبشرية والتقنية، مع إبراز أوجه القصور. وقد توصلت الدراسة إلى وجود فجوة كبيرة بين التهديدات المتزايدة وقدرات الدول العربية على مواجهتها، لافتةً إلى نقص الكوادر البشرية المؤهلة وضرورة برامج التعليم والتدريب المتخصصة.

أوجه الشبه مع بحثي :تتقاطع دراستي مع عمل عبد القادر في **الاهتمام المشترك بتحليل تأثير التهديدات الرقمية على الأمن القومي**، مما يؤكد عالمية هذه القضية. كما أبرزت كلتا الدراستين **تحديات جوهرية مشتركة** مثل نقص الكوادر وضعف القدرات الفنية والتنسيق المؤسسي، مما يوحي بأن هذه التحديات قد تكون بنيوية وعالمية لا تقتصر على منطقة معينة. علاوة على ذلك، فإن اعتمادها على **المنهج الوصفي التحليلي** يتشابه مع الجانب التحليلي والاستقرائي في منهجي.

أوجه الاختلاف مع بحثي :يكمن الاختلاف الجوهري في **النطاق الجغرافي والتحليلي** .فدراسة عبد القادر انحصرت في السياق العربي، بينما تتوسع دراستي لتشمل العلاقات الدولية بمفهومها الشامل، مما يتيح لي فهم التفاعلات الجيوسياسية الأوسع. بينما ركزت دراستها على التهديدات الداخلية والهيكلية التي تواجه الدول العربية، تميل دراستي إلى **التركيز على الجانب التفاعلي الدولي**، من حيث علاقات التعاون والتنافس، ومسألة الصراع السيبراني كامتداد للصراعات السياسية التقليدية. الأهم من ذلك، أن

دراستي تتبنى **إطارًا نظريًا أوسع** يستند إلى نظريات العلاقات الدولية، مثل الأمن الجماعي والحرب غير المتماثلة، متجاوزةً مفهوم الأمن القومي كونه الأساس الوحيد.

أهميتها لبحثي الحالي :تُقدم دراسة إيمان عبد القادر **قاعدة بيانات وملاحظات ميدانية قيمة** عن واقع الأمن السيبراني في الدول العربية، والتي تُشكل حالة دراسية جزئية يمكن الاستفادة منها في إطار الفضاء الدولي الأوسع الذي أتناوله. كما أنها تُسلط الضوء على الفجوة بين السياسات الوطنية للدول النامية والأطر القانونية والمؤسسية الدولية، وهي نقطة محورية في بحثي الذي يسعى إلى تحليل التفاعل بين الهجمات السيبرانية والعلاقات بين الدول، بما يشمله ذلك من تهديدات وتحديات وفرص تعاون.

2. توماس ريد، "الحرب السيبرانية لن تحدث(2012/2013) (Cyber War Will Not Take Place) "

ملخص الدراسة :تُعد هذه الدراسة لتوماس ريد، التي نُشرت في Journal of Strategic Studies، من الأعمال الرائدة التي قدمت منظورًا نقديًا جريئًا لمفهوم "الحرب السيبرانية" السائد. يتحدى ريد الفكرة القائلة بأن الهجمات السيبرانية يمكن أن ترقى إلى مستوى الحرب الحقيقية بالمعنى التقليدي الذي يتضمن القتل والتدمير المادي الواسع. بدلاً من ذلك، يقترح تصنيف الأنشطة السيبرانية ضمن أربع فئات رئيسية :**التجسس، التخريب، السرقة، والردع** .ويرى أن هذه الأنشطة، وإن كانت قادرة على زعزعة الاستقرار وإحداث أضرار كبيرة، إلا أنها تفتقر إلى العنف المميت الذي يميز الحرب التقليدية، ويجب فهمها كأدوات سياسية واقتصادية وليست عسكرية بحتة.

أوجه الشبه مع بحثي :تتفق دراسة ريد مع بحثي في **تحديد الفضاء السيبراني كساحة للتفاعلات الدولية** التي تؤثر على الأمن والعلاقات بين الدول. كما أنها تتقاطع في أهمية **التحليل الدقيق للتهديدات السيبرانية** وفهم طبيعتها المعقدة.

أوجه الاختلاف مع بحثي :يكمن الاختلاف الجوهري في **الموقف من مفهوم "الحرب السيبرانية** ."فبينما يقلل ريد من احتمالية حدوث حرب سيبرانية شاملة، فإن بحثي يشير إلى "الحروب السيبرانية" كأحد الأبعاد المحتملة للتهديدات التي تؤثر على العلاقات الدولية (كما ورد في الكلمات المفتاحية ومشكلة البحث)، مما يفتح مجالًا للنقاش والتحليل المستفيض في دراستي.

أهميتها لبحثي الحالي :تُقدم دراسة ريد مساهمة حيوية لبحثي من خلال **تعميق النقاش المفاهيمي حول "الحرب السيبرانية** ." فهي ستدفعني إلى التفكير النقدي في تعريف هذا المصطلح ضمن سياق بحثي، وما إذا كنت سأتبنى تعريفًا أوسع أو أضيق. كما أنها تُضيف **بعدًا نظريًا مهمًا** يمكن أن يكون نقطة انطلاق لمناقشة كيفية تصنيف الأنشطة السيبرانية وتأثيرها على العلاقات بين الدول، مما يُثري الإطار النظري لبحثي ويُظهر وعيًا بالنقاشات الأكاديمية المعقدة في هذا المجال.

3. جوزيف ناي الابن، "القوة السيبرانية (Cyber Power) "من أعمال متعددة، بدءًا من (2010)

ملخص الدراسة :يُعد جوزيف ناي الابن، وهو أحد أبرز المنظرين في العلاقات الدولية ومبتكر مفهوم "القوة الناعمة"، من أوائل من وسّعوا تحليلاتهم لتشمل مفهوم "القوة السيبرانية". يرى ناي أن القوة السيبرانية تمثل قدرة الدول على التأثير في سلوك الآخرين من خلال التحكم في الفضاء السيبراني أو استغلاله. يميز بين القوة الهجومية والدفاعية في هذا الفضاء، ويُناقش كيف يمكن

للدول توظيف هذه القوة لتحقيق أهدافها السياسية والاقتصادية. يُبرز ناي أن القوة السيبرانية تُزيد من تعقيد ديناميكيات القوة التقليدية في العلاقات الدولية وتُعيد تشكيل توازن القوى العالمي. كما يُشدد بقوة على أهمية التعاون الدولي لإدارة هذه القوة المتنامية وتقليل مخاطرها.

أوجه الشبه مع بحثي :تتفق أعمال ناي مع بحثي في التأكيد على أن **الفضاء السيبراني يمثل مصدرًا جديدًا ومهمًا للقوة والتأثير** في العلاقات الدولية. كلا الدراستين تُبرزان **أهمية التعاون الدولي** كضرورة ملحة لمواجهة التحديات السيبرانية والحفاظ على الاستقرار. كما أن منظور ناي الشامل الذي يربط القوة السيبرانية بأبعاد سياسية واقتصادية يتوافق تمامًا مع مقاربتي الواسعة للموضوع.

أوجه الاختلاف مع بحثي :يركز ناي بشكل أساسي على **مفهوم "القوة السيبرانية" كأداة للدول** وتأثيرها على توازن القوى، بينما يتناول بحثي "الأمن السيبراني" كقضية أوسع وتشمل تحديات واستراتيجيات وسياسات. كما أن ناي يقدم إطارًا نظريًا عامًا، في حين أن بحثي سيتعمق في التحليل العملي للتهديدات، الاستراتيجيات، والسياسات المحددة.

أهميتها لبحثي الحالي :تُقدم أعمال جوزيف ناي مساهمة نظرية قوية لبحثي من خلال **تعزيز الإطار المفاهيمي الخاص بالقوة في السياق السيبراني** .ستساعدني على مناقشة كيفية تأثير القدرات السيبرانية على توازن القوى وديناميكيات العلاقات بين الدول. كما أنها تُقدم دعمًا أكاديميًا لفرضيتي حول **أهمية التعاون الدولي** في مواجهة التهديدات السيبرانية، وتُسهم في ربط مفهوم الأمن السيبراني بمفهوم القوة في العلاقات الدولية، مما يضيف عمقًا تحليليًا كبيرًا.

منهج البحث:

يعتمد هذا البحث على **منهجية متكاملة** تجمع بين مقاربات بحثية متنوعة. تهدف هذه المنهجية المتعددة الأبعاد إلى استكشاف الظاهرة من زوايا مختلفة، بدءًا من جذورها التاريخية وصولًا إلى تحليلها المعاصر، مع مقارنة السياسات والاستراتيجيات المتبعة.

1-المنهج التحليلي :سيكون المنهج التحليلي حجر الزاوية في فهم آثار الهجمات السيبرانية على الساحة الدولية.و سيتم الغوص في تفاصيل **الهجمات السيبرانية البارزة** التي شهدها العالم منذ عام 2000، مع التركيز على تلك التي استهدفت البنى التحتية الحيوية للدول أو مؤسساتها الاستراتيجية. سيتضمن ذلك تحليلًا دقيقًا لأنواع الهجمات (مثل هجمات برامج الفدية واسعة النطاق، عمليات التجسس السيبراني على المؤسسات الحكومية، أو التدخلات الرقمية في العمليات الانتخابية)، محاولة تحديد الجهات الفاعلة المحتملة، وتقييم حجم الخسائر والتداعيات المترتبة عليها. ولتحقيق ذلك، سيتم الاعتماد على مجموعة واسعة من **المصادر الموثوقة**؛ من التقارير الرسمية الصادرة عن الهيئات الحكومية والمنظمات الدولية الرائدة (كالأمم المتحدة والناتو والاتحاد الأوروبي)، إلى الدراسات المتخصصة التي تنشرها مراكز الأبحاث الأمنية المرموقة) مثل تقارير Crowd Strike و Mandiant وFireEye....)، بالإضافة إلى البيانات المتاحة للجمهور من قواعد بيانات الهجمات السيبرانية المتاحة

2-المنهج الاستقرائي :لتعميم الاستنتاجات الفردية وبناء فهم شامل للظاهرة، سيتم توظيف المنهج الاستقرائي. يهدف هذا المنهج إلى استكشاف **الأنماط والاتجاهات العامة** التي تحكم التفاعل السيبراني الدولي من خلال مراجعة معمقة للأدبيات الأكاديمية

والتقارير البحثية المعاصرة. سيتم تحليل هذه المصادر لتحديد كيف تتطور طبيعة التهديدات السيبرانية، وما هي الاستجابات المشتركة للدول والمنظيمات، وكيف تتشكل الأطر القانونية والمعيارية الدولية. الهدف الأسمى هو بلورة صورة متكاملة تمكن من تحديد المبادئ والقواعد التي تحكم هذا الفضاء المتغير باستمرار.

3-المنهج المقارن :لا غنى عن المنهج المقارن لفهم التباينات والتقاربات في مقاربات الدول والمنظمات الدولية تجاه الأمن السيبراني. سيتم إجراء مقارنة بين **الاستراتيجيات الوطنية للأمن السيبراني** والأطر القانونية المعتمدة من قبل مجموعة مختارة من القوى السيبرانية الكبرى (مثل الولايات المتحدة، الصين، وروسيا)، إلى جانب عدد من المنظمات الدولية والإقليمية ذات الثقل (كالأمم المتحدة، الناتو، الاتحاد الأوروبي، ومجموعة العشرين). ستركز هذه المقارنة على نقاط جوهرية مثل كيفية تعريف الهجمات السيبرانية في تشريعاتها، آليات الردع والاستجابة المتبعة، تدابير بناء الثقة السيبرانية، ومبادرات التعاون المشترك وتبادل المعلومات، بالإضافة إلى دور القطاع الخاص في تعزيز الدفاعات السيبرانية. يرمي هذا التحليل المقارن إلى تسليط الضوء على أفضل الممارسات الممكنة، وكشف الفجوات القائمة في التعاون الدولي، وتقييم الفعالية الشاملة للاستراتيجيات المتبعة عالميًا.

4-المنهج التاريخي :لفهم السياق التطوري للأمن السيبراني في العلاقات الدولية، سيتم تبني المنهج التاريخي. سيتتبع هذا المنهج مسار تطور الأمن السيبراني كقضية محورية على الأجندة الدولية، بدءًا من اللحظات الأولى لظهور التهديدات السيبرانية وتصنيفها، مرورًا بتبني الاستراتيجيات الوطنية والدولية الأولى لمواجهتها، وصولًا إلى النقاشات الراهنة حول تطبيق قواعد القانون الدولي على الفضاء السيبراني. هذا المسار الزمني سيمكننا من إدراك كيف أسهمت **الأحداث المفصلية** (مثل الهجمات السيبرانية الكبرى، مؤتمرات القمة الدولية، وتأسيس فرق الاستجابة السيبرانية .....) في تشكيل التصورات والسياسات تجاه الأمن السيبراني، وكيف أثرت على العلاقات الدولية ؟

IJMMC
International journal For Media
Mass Communication &

المبحث الأول

الإطار المفاهيمي للأمن السيبراني والعلاقات الدولية

تمهيد وتقسيم:

مما لا شك فيه أن الفضاء السيبراني أصبح جزءًا لا يتجزأ من حياتنا اليومية، ويؤثر بشكل كبير على جميع المجالات، بما في ذلك العلاقات الدولية، إن التطور التكنولوجي السريع واستخدام الإنترنت في جميع أنحاء العالم قد خلق بيئة جديدة من التفاعلات بين الدول، سواء على المستوى الاقتصادي أو الأمني أو الدبلوماسي، في هذا السياق، نشأ مفهوم "الأمن السيبراني" باعتباره عنصراً أساسياً في استراتيجيات الدول للحفاظ على استقرارها وأمنها في مواجهة التهديدات الرقمية.

الأمن السيبراني لا يقتصر فقط على حماية الأنظمة الإلكترونية للشركات والأفراد، بل يشمل أيضًا الدفاع ضد الهجمات السيبرانية التي قد تهدد الأمن القومي للدول، هذه التهديدات يمكن أن تؤدي إلى تقويض الأنظمة الحكومية أو العسكرية أو البنية التحتية الحيوية لدولة معينة، من هنا تبرز العلاقة القوية بين الأمن السيبراني والعلاقات الدولية، حيث أصبح الفضاء السيبراني ميدانًا جديدًا للمنافسة والصراع بين الدول.

وفي هذا المبحث، سيتم تناول الإطار المفاهيمي الذي يحدد الأمن السيبراني وكيفية تأثيره على العلاقات الدولية، من خلال دراسة مفهوم الأمن السيبراني في المطلب الأول، وتحليل تأثير الفضاء السيبراني على العلاقات الدولية في المطلب الثاني.

- **المطلب الأول: مفهوم الأمن السيبراني:**
- **المطلب الثاني: العلاقات الدولية في ظل الفضاء السيبراني:**

المطلب الأول

مفهوم الأمن السيبراني

لفهم التحديات التي يواجهها الأمن السيبراني، يجب أولًا تحديد مفهومي "الأمن السيبراني" لغة واصطلاحًا، ثم التطرق إلى تطور هذا المفهوم عبر الزمن، وأخيرًا استعراض العناصر والمكونات الأساسية التي يتكون منها الأمن السيبراني، سيتم تناول هذه النقاط بالتفصيل في هذا المطلب لتوضيح أهمية الأمن السيبراني في العصر الرقمي الذي نعيشه اليوم.

1. تعريف الأمن السيبراني لغة واصطلاحًا:

تعود كلمة "سايبر (Cyber) "إلى الأصل اليوناني"Kybernetes" ، التي تعني "القيادة" أو "التحكم عن بُعد"، تم استخدام هذا المصطلح لأول مرة في الأدب العلمي الكلاسيكي للإشارة إلى القدرة على التحكم في الأنظمة عن بُعد، يعود الفضل في إدخال مصطلح "السيبرانية" في مجال العلوم الحديثة إلى عالم الرياضيات نوربرت وينر، الذي استخدمه في عام 1948 أثناء دراسته لعلم "السيبرانية" في مجال الأنظمة التكيفية، وقد تطور هذا المفهوم ليشمل دراسة كيفية تفاعل الإنسان مع الآلات بشكل منظم ومنضبط(Wiener, Norbert, 1948, p. 7).

في سياق الأمن السيبراني، يمكن تعريف مصطلح "سايبر" على أنه يشير إلى "الفضاء الرقمي" أو "البيئة الإلكترونية" التي تشمل جميع الشبكات والأنظمة التي ترتبط بها الأجهزة الإلكترونية، وهو ما يعكس التركيز على حماية المعلومات والنظم في هذا الفضاء الإلكتروني، لا تقتصر أهمية "السايبر" فقط على النظم التقنية، بل تشمل أيضًا الوسائل التي من خلالها تتم الحماية أو الهجوم على هذه الأنظمة، مثل التشفير، مكافحة الفيروسات، والجدران النارية، وكلها تقنيات تساهم في الحفاظ على سلامة البيانات وحمايتها من الوصول غير المصرح به(البعلبكي، منير, 2004, p. 243).

وبينما يُستخدم مصطلح "سايبر" بشكل واسع في العديد من المجالات التقنية والعلمية، فإن تطبيقه في مجال الأمن السيبراني يرتبط بشكل أساسي بالأنظمة الإلكترونية والشبكات التي تحتفظ بالبيانات أو تدير العمليات الحساسة، سواء في المؤسسات الحكومية أو الشركات الخاصة أو الأفراد، هذه الأنظمة تتطلب مستوى عالٍ من الحماية لضمان سرية المعلومات وسلامتها وإتاحتها في الوقت المناسب(وزارة الدفاع الأمريكية, 2010, ص 8)

.

وفي الاصطلاح، يُعرّف الأمن السيبراني على أنه "حماية الأنظمة والشبكات والبرمجيات من الهجمات الرقمية التي تهدف إلى الوصول غير المصرح به إلى البيانات أو تغييرها أو تدميرها أو تعطيل العمليات"، فالأمن السيبراني يشمل مجموعة من السياسات، التقنيات، والإجراءات التي تهدف إلى حماية المعلومات والبنى التحتية الإلكترونية من مجموعة متنوعة من المخاطر الرقمية، بما في ذلك الهجمات الإلكترونية (Melzer, Nils, 2001, p. 5).

يُعرف بعض المتخصصين في المجال مثل "شين (Shin) "الأمن السيبراني بأنه "استخدام الطيف الإلكتروني لتخزين، تعديل، وتبادل البيانات بشكل آمن، ضمن الأنظمة المتصلة بشبكات الإنترنت"، في هذا الإطار، يكتسب الأمن السيبراني أهمية خاصة

في حماية البيانات وحمايتها من التلاعب أو السرقة عبر الأنظمة والشبكات الإلكترونية التي تزداد تعقيدًا بشكل مستمر. وبالتالي، فإن الأمن السيبراني يعتمد بشكل أساسي على حماية البيانات المخزنة والمنقولة بين الأنظمة، ويدير المعلومات بطريقة تضمن توافرها دون تدخل خارجي غير مصرح به (Shin, Beomchul, 2011, p. 99–140).

من جانب آخر، يتوسع مفهوم الأمن السيبراني ليشمل أمن الأنظمة المتصلة بالشبكات، حيث يتعامل مع العناصر المادية (مثل الأجهزة) والبرمجيات (مثل التطبيقات)، يشمل ذلك الأجهزة الذكية، أنظمة التحكم الصناعية، الإنترنت من الأشياء(IoT) ، وجميع الأنظمة الإلكترونية التي تتعامل مع البيانات في العصر الرقمي (Andress, Jason, & Winterfeld, Steve, 2011, p. 2).

ومن التعريفات الأخرى التي تبرز في السياق القانوني والأمني هو أن الأمن السيبراني يهدف إلى "حماية الأنظمة والشبكات من المخاطر الرقمية التي قد تؤدي إلى تعطيل العمليات أو سرقة المعلومات الحساسة"، فبجانب الحماية التقنية من الهجمات، يتطلب الأمر وجود استراتيجيات دفاعية تشرك مؤسسات متعددة لضمان الالتزام بالقوانين والأطر التنظيمية المحلية والدولية (Giles, Kenneth, 2017, p. 23–24).

2. تطور مفهوم الأمن السيبراني عبر الزمن:

شهد مفهوم الأمن السيبراني تطورًا كبيرًا منذ نشأته في سبعينيات القرن العشرين، حيث بدأت التهديدات بسيطة بسبب محدودية التكنولوجيا، إلا أن ظهور أول فيروس حاسوبي في الثمانينيات، وانتشار الإنترنت في التسعينيات، أديا إلى تصاعد التحديات الأمنية وتعقيدها، ومع دخول الألفية الجديدة، أصبح الأمن السيبراني ضرورة حتمية لحماية البيانات والأنظمة من الهجمات الإلكترونية المتطورة، تطورت الأدوات والتشريعات لمواكبة هذا التهديد، وأصبح الأمن الرقمي جزءًا لا يتجزأ من الأمن القومي، اليوم، يمثل الأمن السيبراني خط الدفاع الأول ضد التهديدات التي تمس استقرار الدول وأمنها الاقتصادي والاجتماعي والسياسي (الفتلاوي، أحمد, 2016، ص 619: 623).

3. عناصر ومكونات الأمن السيبراني (مثل سرية المعلومات، سلامتها، وتوافرها):

يتكوّن الأمن السيبراني من ثلاثة عناصر رئيسية: **سرية المعلومات** لحمايتها من الوصول غير المصرح به، **سلامة المعلومات** لضمان عدم التلاعب أو التغيير غير المشروع، و**توافر المعلومات** لضمان وصول المستخدمين إليها عند الحاجة، تُشكل هذه المبادئ جوهر حماية الأنظمة والبيانات الرقمية.

من خلال هذه الدراسة، يتضح للباحث إن تناول مفهوم الأمن السيبراني من مختلف زواياه اللغوية والاصطلاحية والتاريخية لا ينبغي أن يُنظر إليه كعرض نظري مجرد، بل يُعد مدخلًا ضروريًا لفهم الطبيعة المعقدة والديناميكية للبيئة الرقمية الحديثة، وما تفرضه من تحديات متنامية على أمن الدول والأفراد على حد سواء، لقد بدا واضحًا من تتبع تطور المفهوم أن الأمن السيبراني لم يعد حكرًا على النطاق التقني الصرف، بل أضحى مفهومًا مركبًا يشتبك مع قضايا استراتيجية، قانونية، اقتصادية، بل وسياسية، مما يضع الباحث أمام مسؤولية فهمٍ شمولي يزاوج بين الجوانب التقنية والبُعد الإنساني والتنظيمي لهذه الظاهرة.

من هنا، فإن العودة إلى الجذور اللغوية لكلمة "سايبر" وربطها بفكرة "التحكم عن بعد" ليست ترفًا لغويًا، بل تؤكد منذ نشأته البعد السيادي والسيادي الذي يحكم هذا الفضاء غير المادي، إن "التحكم" هنا لا يقتصر على الجوانب الميكانيكية أو البرمجية، بل يتجاوز ذلك ليشمل من يتحكم في تدفق المعلومات، وفي من يمتلك أدوات الردع والهجوم، وبالتالي من يفرض إرادته في هذا الفضاء السيبراني.

وقد بدا للباحث من خلال استعراض التعريفات المتعددة، سواء الأكاديمية أو التنظيمية، أن ثمة قصورًا في استيعاب حقيقة التهديدات السيبرانية المتسارعة في تعريفات سابقة كانت تركز على حماية "النظام" أكثر من تركيزها على حماية "الإنسان، وهذا ما يدعو إلى تبني منظور أكثر شمولًا يعترف بأهمية البنية التحتية الرقمية، لكنه لا يُغفل أثر الهجمات السيبرانية على الحياة اليومية للمواطنين، وعلى الأمن الإنساني في أوسع معانيه.

كما يلفت الباحث النظر إلى أن تأخر الاعتراف الرسمي والدولي بخطورة التهديدات السيبرانية حتى مطلع الألفية الجديدة إنما يعكس قصورًا في الاستجابة الاستراتيجية المبكرة، الأمر الذي سمح لجهات غير حكومية، بل وحتى أفراد، بامتلاك أدوات سيبرانية قادرة على زعزعة استقرار مؤسسات عريقة أو التأثير على نتائج انتخابية في دول كبرى، كما حدث في عدة محطات انتخابية في العقدين الأخيرين.

ومن هذا المنطلق، فإن الباحث يرى أن تطور مفهوم الأمن السيبراني لا ينبغي أن يُدرس بمعزل عن التحولات الجيوسياسية التي شهدها العالم منذ التسعينيات، وخاصة بعد سقوط الاتحاد السوفيتي، إذ انتقل العالم من صراع نووي معلن إلى صراع غير مرئي في الفضاء السيبراني، حيث تُخاض المعارك باستخدام الشفرات والفيروسات والبرمجيات الخبيثة، لا بالصواريخ والدبابات، وهو ما يتطلب إعادة النظر في مفاهيم السيادة الوطنية والحرب والدفاع.

أما من حيث العناصر الثلاثة التي يُبنى عليها الأمن السيبراني (السرية، السلامة، التوافر)، فإن الباحث يعتبرها بمثابة مثلث ذهبي لا يمكن أن تتحقق الحماية الرقمية الفعالة دون مراعاة توازن دقيق بينها، فالتركيز المفرط على سرية المعلومات مثلًا قد يؤدي إلى قيود تعيق التوافر أو كفاءة الأداء، في حين أن التغاضي عن سلامة البيانات قد يفتح الباب أمام التلاعب بنتائج حساسة، كما هو الحال في الأنظمة البنكية أو الصحية، من هنا تأتي أهمية التفكير في الأمن السيبراني بمنطق "الموازنة" لا بمنطق "المغالبة."

إن هذه العناصر، على الرغم من وضوحها، تواجه تحديات معقدة في الواقع العملي، حيث إن الكثير من الهجمات السيبرانية أصبحت تستهدف العنصر البشري بوصفه الحلقة الأضعف في سلسلة الأمن المعلوماتي، وليس الأنظمة التقنية فحسب، ويؤكد الباحث هنا على ضرورة إدماج البعد الثقافي والتوعوي ضمن استراتيجيات الأمن السيبراني، لا سيما في البيئات التي تفتقر إلى الوعي الكافي بمخاطر الاستخدام غير الآمن للتكنولوجيا،

وفي ضوء ما سبق، يوصي الباحث بضرورة الانتقال من الرؤية التقنية الضيقة إلى رؤية أكثر تكاملًا، تنظر إلى الأمن السيبراني بوصفه قضية تتقاطع فيها الاعتبارات التكنولوجية مع الأبعاد الأخلاقية والسياسية والاجتماعية، وتستلزم تعاونًا دوليًا صريحًا لمواجهة المخاطر العابرة للحدود، والتي لم تعد تقف عند حدود التهديد، بل باتت جزءًا من صميم الصراع الدولي على النفوذ والسيطرة والمعلومات.

المطلب الثاني

العلاقات الدولية في ظل الفضاء السيبراني

تُعد مفاهيم السيادة الوطنية من أبرز تلك المفاهيم التي تعرضت لتحديات كبيرة بفعل الفضاء السيبراني، ومن خلال هذا المطلب سنتناول دراسة تأثير الفضاء السيبراني على مفاهيم السيادة الوطنية، ودور الفاعلين الجدد مثل الشركات التقنية ومجموعات الهاكرز في العلاقات الدولية، بالإضافة إلى كيفية تأثير الأمن السيبراني على التعاون والصراع بين الدول.

1. تأثير الفضاء السيبراني على مفاهيم السيادة الوطنية:

مع التقدم التكنولوجي السريع في الفضاء السيبراني، ظهرت تهديدات أمنية جديدة تهدد استقرار السيادة الوطنية للدول، فبفضل الأسلحة السيبرانية التي أصبحت جزءًا من الترسانة الحديثة، يمكن للدول استخدام هذه الأدوات لتحقيق أهداف سياسية أو عسكرية عبر الهجمات السيبرانية، ونتيجة لذلك، أصبحت الهجمات السيبرانية تنقسم إلى نوعين رئيسيين: الأول هو "الهجمات الاصطلاحية(syntactic attacks) "، التي تستهدف الأنظمة من خلال البرمجيات الضارة مثل الفيروسات والبرمجيات الخبيثة، والثاني هو "الهجمات الدلالية(semantic attacks) "، التي تستهدف البنية التحتية لتكنولوجيا المعلومات وتقوم بتغيير البيانات بشكل غير ظاهر(خليفة، إيهاب, 2020، ص 46: 78).

تؤدي هذه التهديدات إلى إحداث اضطرابات في الأنظمة الرقمية والعمليات التقنية اليومية، مما يضع قضايا الأمن السيبراني على رأس أولويات السياسات الوطنية والدولية، ولذلك، تسعى الحكومات إلى تطوير استراتيجيات فعالة لمواجهة هذه التهديدات الحديثة، كما أدى ظهور الفضاء السيبراني إلى تغيير حسابات القوة الوطنية، حيث أصبح هذا المجال يساهم في إعادة توزيع القوة والضعف بين الدول والمنظمات العالمية.

أكد ديفيد هيلد في كتابه "Globalization Transformation" أن تهديدات الأمن في عصر العولمة تتأثر بالتطورات التكنولوجية، حيث ساهمت التكنولوجيا العسكرية في تحسين القدرات الحربية، كما جعلت أنظمة الاتصالات الحديثة إدارة العمليات العسكرية أكثر فعالية، وزادت العولمة من صعوبة سيطرة الدول على مصادر الأسلحة (خليل، حازم محمد, 2023، ص 23–54).

2. دور الفاعلين الجدد في العلاقات الدولية (مثل الشركات التقنية، مجموعات الهاكرز):

لقد شهدت العلاقات الدولية تحولًا كبيرًا في السنوات الأخيرة نتيجة لدور الفاعلين الجدد الذين ظهروا على الساحة الدولية، بما في ذلك الشركات التقنية الكبرى ومجموعات الهاكرز، التي أصبح لها تأثير متزايد في السياسة الدولية والأمن السيبراني، لم تعد الدول وحدها هي القوى الرئيسية المؤثرة في الساحة الدولية، بل أصبح للجهات غير الحكومية دور متزايد في تشكيل التحولات السياسية والاقتصادية (ماجد، محمد, 2021، ص 154–167).

وتلعب الشركات التقنية دورًا أساسيًا في تطوير وتوزيع التكنولوجيا الحديثة، مما يعزز من مكانتها كفاعلين دوليين، على سبيل المثال، أصبحت الشركات التقنية هي المسؤولة عن تطوير البنية التحتية للإنترنت، وهو ما يجعلها تتحكم في تدفق البيانات،

وبالتالي تصبح في موقع يتيح لها مراقبة أو التأثير على سلوك الأفراد والشركات والحكومات، هذا التحكم في تدفق المعلومات يجعل هذه الشركات جزءًا أساسيًا من عملية تشكيل الرأي العام، كما يمكن أن تكون أداة قوية في استراتيجيات القوى الناعمة التي تستخدمها الدول لتحقيق أهدافها السياسية والاقتصادية(Geers, Kenneth, 2015, p. 67–88).

من جهة أخرى، تعد مجموعات الهاكرز، سواء كانت تابعة لدول معينة أو مجموعات غير حكومية، من الفاعلين الجدد الذين يمكنهم التأثير بشكل كبير على العلاقات الدولية، فعلى الرغم من أن مجموعات الهاكرز تعتبر غير رسمية من حيث الهوية، إلا أن تأثيرها في السياسة الدولية والأمن السيبراني لا يمكن تجاهله، هناك العديد من الحالات التي شهدنا فيها مجموعات الهاكرز تنفذ هجمات سيبرانية على دول أخرى أو على كيانات دولية بهدف تحقيق أهداف سياسية أو اقتصادية (Bradshaw, Samantha, 2015, p. 13–21).

إن هذه التحولات تتطلب من الدول أن تعدل استراتيجياتها الأمنية والسياسية لمواكبة التحديات الجديدة، ففي الماضي، كانت الدولة هي القوة الوحيدة القادرة على حماية الأمن القومي وتشكيل السياسة الدولية، لكن اليوم أصبحت الشركات التقنية الكبرى ومجموعات الهاكرز لاعبًا رئيسيًا في هذه المعادلة، لذلك، أصبح من الضروري أن تتعاون الدول بشكل وثيق مع هذه الشركات لضمان حماية المعلومات الوطنية من التهديدات السيبرانية المتزايدة (De Falco, Marco, 2012, p. 51–69).

بالإضافة إلى ذلك، فإن ظهور الفاعلين الجدد يعزز من الحاجة إلى تنظيمات وقوانين دولية أكثر فعالية لمواكبة التحديات المعاصرة، على سبيل المثال، من الضروري أن يتم وضع أطر قانونية تحكم كيفية تعامل الدول مع الهجمات السيبرانية التي قد تتسبب فيها مجموعات الهاكرز أو حتى الشركات التقنية التي قد تُستغل لأغراض سياسية، ومن ثم، يجب أن تكون هناك اتفاقيات دولية لحماية الأمن السيبراني، وتحديد المسؤوليات القانونية لتلك الأطراف الفاعلة، وضمان أن تكون هناك آليات رادعة ضد الهجمات السيبرانية(زروقة، إسماعيل, 2018ص 109– 113).

3. تأثير الأمن السيبراني على التعاون والصراع بين الدول:

شكّل الأمن السيبراني عنصرًا محوريًا في طبيعة العلاقات الدولية الحديثة، حيث لم يعد التعاون والصراع بين الدول يقتصر على الأبعاد العسكرية أو الاقتصادية فقط، بل أصبح الفضاء السيبراني ساحةً جديدة للمواجهة والتأثير المتبادل، منذ الهجوم السيبراني على أنبوب النفط السوفيتي عام 1982، الذي يُعد من أوائل الأمثلة على استخدام التكنولوجيا لتحقيق أهداف استراتيجية، تطورت الهجمات السيبرانية لتصبح أكثر تعقيدًا وتنظيمًا. فقد استُخدمت لأغراض التجسس، تعطيل البنية التحتية، والتأثير في العمليات السياسية كما حدث في الانتخابات الأمريكية عام 2016م (Banks, William, 2021, p. 15–21).

كما أظهرت الهجمات السيبرانية على وزارات الدفاع الأمريكية في أواخر التسعينيات، ثم استخدام فيروس "ستكسنت" ضد المنشآت النووية الإيرانية، أن هذه الهجمات يمكن أن تكون أداة فعالة لتقويض قدرات الخصوم دون الدخول في صراع عسكري مباشر (Curlee, Kathleen, 2021, p. 56–78) ، كذلك، فإن الهجوم على إستونيا عام 2007 والهجمات المتزامنة مع الحرب

الروسية الجورجية عام 2008، أكدتا أن الهجمات السيبرانية باتت تُستخدم كمقدمة أو مرافقة للعمليات العسكرية التقليدية (Adewale, Lukman, 2020, p. 23–45).

في مواجهة هذه التهديدات، برزت الحاجة إلى التعاون الدولي، خاصة من خلال تبادل الخبرات والمعلومات، فقد قامت الأمم المتحدة بدور بارز في هذا الإطار، من خلال دعم اتفاقيات دولية مثل اتفاقية بودابست لمكافحة الجرائم السيبرانية، وتعزيز الحوار بين الدول لسن تشريعات مشتركة وتنظيم ورش عمل متخصصة(Gomes, Marcelo, 2019, p. 43–62) .

في هذا المطلب، سعتُ لتسليط الضوء على التحولات الكبيرة التي أحدثها الفضاء السيبراني في العلاقات الدولية، وكيف أن هذه التحولات تفرض تحديات جديدة على مفاهيم السيادة الوطنية، فقد بيّنتُ كيف أن الهجمات السيبرانية أصبحت جزءًا من الصراع الدولي، مما أثر بشكل مباشر على استقرار الدول وزعزعة أمنها السيبراني، إلى جانب ذلك، تناولتُ الدور المتزايد للفاعلين الجدد مثل الشركات التقنية ومجموعات الهاكرز، مشيرًا إلى أن هذا التحول في الديناميكيات الدولية يفرض على الدول إعادة تقييم استراتيجياتها الأمنية والتعاون بشكل أكثر فعالية.

كما برزت أهمية الأطر القانونية الدولية لمواكبة هذه التحديات، حيث أكدت على ضرورة وضع اتفاقيات رادعة ضد الهجمات السيبرانية وحماية البيانات من الاستغلال السياسي، لقد أظهرتُ أن الفضاء السيبراني لم يعد مجرد مجال تقني بل أصبح ساحة جديدة للمواجهة والتأثير في السياسات الدولية، وقد أشرتُ إلى الأمثلة الواقعية على تطور استخدام الهجمات السيبرانية كأداة فعالة في تحقيق أهداف سياسية واستراتيجية، ما يجعل التعاون بين الدول أمرًا لا غنى عنه.

يتضح من العرض السابق أن الفضاء السيبراني قد أصبح بالفعل عاملاً محوريًا في تشكيل العلاقات الدولية، وليس مجرد مجال تقني محدود، صحيح أن السيادة الوطنية تواجه تحديات كبيرة في ظل الهجمات السيبرانية المتزايدة، لكن من المهم أيضًا الاعتراف بأن هذه التهديدات قد تفتح المجال لإعادة تقييم مفهوم السيادة بشكل أوسع، من الممكن أن يُعاد تعريف السيادة في سياق جديد حيث لا تقتصر على السيادة الجغرافية فقط، بل تتوسع لتشمل الفضاء السيبراني كجزء من السيادة الرقمية.

إضافة إلى ذلك، يمكن القول بأن الدور المتزايد للشركات التقنية ومجموعات الهاكرز في الساحة الدولية يطرح تحديات أكبر من مجرد الهجمات السيبرانية التقليدية، فالشركات الكبرى، التي تتحكم في تدفق المعلومات والتكنولوجيا، قد تجد نفسها في موضع فاعل أوسع من الحكومات نفسها في بعض الحالات، مما يطرح سؤالًا كبيرًا حول السلطة السياسية الفعلية: هل تقتصر السلطة على الدول فقط، أم أن هذه الشركات أصبحت تشارك في صياغة السياسات الدولية وتوجهاتها؟ هذا التداخل بين القطاع الخاص والحكومات يطرح أيضًا تساؤلات قانونية أخلاقية حول الحوكمة والحقوق الرقمية.

كما أن دور مجموعات الهاكرز، سواء أكانت مدعومة من دول أو غير حكومية، يفتح المجال لمفهوم "الحروب غير التقليدية، ولكن السؤال الأهم الذي يطرح نفسه هنا هو: كيف يمكن للدول أن تعزز أمنها السيبراني في ظل تعدد الفاعلين وغياب إطار قانوني عالمي شامل ينظم هذه الهجمات، خاصة في ظل عدم وجود قوانين دولية واضحة ومتماسكة فيما يتعلق بالحروب السيبرانية؟

من الجدير بالذكر أن هذا التحول نحو الفضاء السيبراني يتطلب أيضًا تطوير استراتيجيات تعاون دولي أقوى، فحتى في الحالات التي تشارك فيها دول معينة في الهجمات السيبرانية أو تحاول التأثير في سياسات الدول الأخرى من خلال الفضاء

الرقمي، يصبح من الضروري على الدول أن تتبنى استراتيجيات أمنية منسقة وأن تبني آليات تشريعية فعالة لمواجهة هذا النوع من الحروب الحديثة.

وبذلك، يمكن القول إن الفضاء السيبراني أصبح ساحة جديدة للمواجهة والتأثير في العلاقات الدولية، وهذا يتطلب إعادة صياغة السياسات الدولية بشكل يعكس التحديات الجديدة التي تفرضها التهديدات السيبرانية على الأمن السيادي والاقتصادي للدول.

IJMMC
International journal For Media
Mass Communication &

المبحث الثاني

التحديات التي يفرضها الأمن السيبراني على العلاقات الدولية

تمهيد وتقسيم:

في ظل التطور المتسارع لتكنولوجيا المعلومات والاتصالات، أصبحت قضايا الأمن السيبراني تمثل تحديًا كبيرًا في العلاقات الدولية، لم تعد تهديدات الأمن السيبراني مقتصرة على الأفراد أو المؤسسات المحلية، بل أصبحت تهدد الأمن القومي للدول وتؤثر بشكل مباشر على استقرار العلاقات الدولية، حيث تتنوع التحديات التي تفرضها هذه الظاهرة بين التحديات التقنية والقانونية من جهة، والتحديات السياسية والاستراتيجية من جهة أخرى، مما يستدعي التعاون الدولي وتطوير آليات لمواجهة هذه المخاطر بشكل مشترك.

التحديات التقنية والقانونية تتعلق بصعوبة تحديد هوية مرتكبي الجرائم السيبرانية، والنقص الكبير في التشريعات الدولية الموحدة لمكافحة هذه الجرائم، بالإضافة إلى تطور أساليب الهجمات السيبرانية بشكل مستمر مثل هجمات برامج الفدية وحجب الخدمة، ما يجعل عملية التصدي لها أكثر تعقيدًا.

من جهة أخرى، تُضيف التحديات السياسية والاستراتيجية بعدًا معقدًا لهذه القضية، إذ يتم استغلال الفضاء السيبراني كأداة في الصراعات السياسية والدبلوماسية بين الدول، هذه التحديات تؤثر على قدرة المجتمع الدولي على وضع استراتيجيات فعالة لمكافحة هذه الجرائم والتهديدات.

في هذا المبحث، سنسلط الضوء على أبرز التحديات التي يفرضها الأمن السيبراني على العلاقات الدولية، حيث يتم تناول التحديات التقنية والقانونية في المطلب الأول، ثم نتناول التحديات السياسية والاستراتيجية في المطلب الثاني.

- **المطلب الأول: التحديات التقنية والقانونية:**
- **المطلب الثاني: التحديات السياسية والاستراتيجية:**

المطلب الأول

التحديات التقنية والقانونية

يعد التصدي للجرائم السيبرانية مهمة صعبة نظرًا للعديد من الأسباب، التي تتراوح بين صعوبة تحديد هوية مرتكبي الجرائم، ونقص التشريعات الدولية الموحدة لمكافحة هذه الجرائم، وصولاً إلى التطور المستمر في أساليب الهجمات السيبرانية، سنناقش في هذا المطلب التحديات الرئيسية التي تواجه مكافحة الجرائم السيبرانية، مع التركيز على هذه الجوانب الثلاثة الأساسية.

1 – صعوبة تحديد هوية مرتكبي الجرائم السيبرانية:

تعد صعوبة تحديد هوية مرتكبي الجرائم السيبرانية من أبرز التحديات التقنية التي تواجه مكافحة هذه الجرائم، على عكس الجرائم التقليدية التي يتم فيها تحديد هوية الجاني من خلال الأدلة المادية والشهادات المباشرة، فإن الجرائم السيبرانية تنطوي على تعقيدات تقنية تجعل من الصعب تحديد هوية مرتكبيها، في العالم الرقمي، يمكن للجرائم أن تتم عبر الإنترنت باستخدام هويات مزورة أو عبر تقنيات تحايل تجعل من الصعب ربط الجريمة بمجرم معين (عصام محمد، أماني، 2022، ص 168–180).

علاوة على ذلك، يمكن للمهاجمين أن يقوموا بتقسيم الهجمات إلى العديد من الأجزاء الصغيرة التي يصعب ربطها ببعضها البعض، مما يزيد من تعقيد التحقيقات، في بعض الحالات، يمكن أن تكون الهجمات السيبرانية على الإنترنت قد تمت من خلال عدد من المهاجمين المتعاونين من مختلف أنحاء العالم، مما يجعل التعاون الدولي أمرًا بالغ الأهمية في تحديد هوية الجناة وملاحقتهم (Tarpova, Simona, 2022, pp. 3–8).

2 – نقص التشريعات الدولية الموحدة لمكافحة الجرائم السيبرانية:

من بين أكبر التحديات القانونية في مكافحة الجرائم السيبرانية، هو نقص التشريعات الدولية الموحدة التي تعالج هذه الجرائم بشكل شامل، على الرغم من الجهود التي تبذلها الدول والمنظمات الدولية مثل الأمم المتحدة، إلا أن التشريعات المتعلقة بالجرائم السيبرانية تتفاوت بشكل كبير من دولة إلى أخرى، مما يخلق فجوات قانونية صعبة في محاربة هذا النوع من الجرائم على مستوى العالم.

3 – تطور أساليب الهجمات السيبرانية باستمرار:

تُعد الهجمات السيبرانية من أخطر التهديدات التي تواجه العالم الرقمي اليوم، ويكمن التحدي الأكبر في التطور المستمر لأساليب هذه الهجمات، فلم تعد تقتصر على الفيروسات التقليدية، بل ظهرت هجمات أكثر تعقيدًا مثل برامج الفدية (Ransomware)التي تشفر بيانات الضحية مقابل فدية مالية، وهجمات حجب الخدمة الموزعة (DDoS) التي تُستخدم فيها شبكات من الأجهزة المُخترقة لإيقاف خدمات إلكترونية بالكامل، هذا التطور السريع يجعل من الصعب على المؤسسات مواكبة التهديدات الأمنية المستجدة (Isnarti, Rika, 2016, pp. 13–24).

وفي ظل هذا التعقيد، أصبح لزامًا على الحكومات والمؤسسات تحديث أنظمتها الدفاعية باستمرار، فالمهاجمون باتوا يستخدمون تقنيات متقدمة كالتعلم الآلي والذكاء الاصطناعي لتطوير أساليب هجومية أكثر دقة، ويستدعي ذلك استراتيجيات أمنية

مرنة ومتكاملة، إلى جانب تعزيز التعاون الدولي وسن تشريعات موحدة، لضمان التصدي الفعّال لهذا النوع من الجرائم العابرة للحدود (Baezner, Marie, 2018, pp. 34–52).

وبذلك، تم تسليط الضوء على التحديات الرئيسية التي تواجه مكافحة الجرائم السيبرانية، ومن خلاله حاولتُ إظهار الأبعاد التقنية والقانونية لهذه القضايا، لقد ناقشتُ صعوبة تحديد هوية مرتكبي الجرائم السيبرانية، التي تعد واحدة من أكبر العوائق التقنية، حيث يؤدي استخدام التقنيات الحديثة والهوية المزورة إلى تعقيد التحقيقات، كما أبرزتُ أيضًا نقص التشريعات الدولية الموحدة التي تشكل تحديًا قانونيًا كبيرًا، إذ تساهم الفجوات التشريعية في تعقيد مواجهة الجرائم السيبرانية على المستوى العالمي، أما فيما يتعلق بتطور أساليب الهجمات السيبرانية، فقد تناولتُ كيف أن المهاجمين يطورون أدواتهم باستمرار باستخدام تقنيات متقدمة مثل الذكاء الاصطناعي والتعلم الآلي، مما يزيد من صعوبة التصدي لهذه الهجمات.

من خلال مناقشة التحديات التقنية والقانونية التي تواجه مكافحة الجرائم السيبرانية، أرى أن الحاجة إلى التعاون الدولي المستمر وتحديث الأنظمة الدفاعية تمثل جوانب محورية لا غنى عنها لمواجهة هذه التحديات بفعالية، وكباحث، أرى أن الجرائم السيبرانية ليست مجرد تهديدات معزولة تقتصر على حدود دولة معينة، بل هي تهديدات عابرة للحدود، تتطلب استجابة منسقة ومتكاملة بين الدول كافة، والقطاعين العام والخاص على حد سواء.

إن **التعاون الدولي المستمر** لا يقتصر فقط على تبادل المعلومات والممارسات الفضلى بين الدول، بل يجب أن يمتد إلى تطوير آليات قانونية وتكنولوجية مشتركة تتسم بالمرونة والقدرة على التكيف مع التطورات السريعة في الفضاء الرقمي، نحن بحاجة إلى بنية قانونية دولية تشجع على التعاون السريع في ملاحقة المجرمين، على غرار المعاهدات التي أبرمت لمكافحة الإرهاب الدولي، ولكن الأمر يتطلب أن تكون هذه الاتفاقيات أكثر تحديدًا في التعامل مع الأبعاد المتغيرة للتهديدات السيبرانية.

أما فيما يتعلق بـ **تحديث الأنظمة الدفاعية**، فإن الأمر لا يقتصر على مجرد تعزيز الأدوات التقنية، بل يتطلب **ثقافة أمنية مستدامة** في المؤسسات الحكومية والخاصة، كلما تقدمنا في تكنولوجيا المعلومات، زادت التهديدات التي نواجهها، من هجمات برامج الفدية إلى الهجمات التي تستخدم الذكاء الاصطناعي، لهذا، من الضروري ليس فقط توفير الأدوات التقنية الحديثة، بل أيضًا تدريب الكوادر البشرية على استخدامها بفعالية.

أخيرًا، **تعزيز التشريعات الدولية** يعد أمرًا ضروريًا في مواجهة هذه الجرائم العابرة للحدود، إن تعدد الأنظمة القانونية بين الدول، وغياب قوانين موحدة تلزم الجميع، يشكل عقبة كبيرة في التصدي الفعال للجرائم السيبرانية، ومع تطور الجرائم، يجب أن تكون التشريعات أكثر مرونة وقادرة على التكيف مع الأبعاد التقنية المتجددة، فالعجز عن تعزيز هذه التشريعات يؤدي إلى ترك ثغرات يستغلها المجرمون،

في النهاية، من خلال هذا المطلب، أرغب في التأكيد على أن **التعاون والتحديث المستمر** ليسا فقط خيارًا، بل ضرورة لنجاح مكافحة الجرائم السيبرانية، وهو ما يتطلب أن تواكب التشريعات والممارسات الدولية التطورات التكنولوجية المتسارعة.

المطلب الثاني

التحديات السياسية والاستراتيجية

يُعد التحدي السياسي والاستراتيجي الأبرز في الفضاء السيبراني هو تحقيق التوازن بين الأمن القومي والحريات الرقمية في ظل تصاعد التهديدات السيبرانية والهجمات على البنية التحتية الحيوية.

تستعرض هذه التحديات السياسية والاستراتيجية الأبعاد المتعددة لاستخدام الفضاء السيبراني في العصر الحديث، وتأثيراته على العلاقات الدولية والأمن الوطني.

1. استخدام الفضاء السيبراني كأداة للتجسس والصراع بين الدول:

الفضاء السيبراني قد تحول إلى ساحة جديدة للتجسس بين الدول، وأصبح يشكل أحد أدوات الصراع السياسي والجيوسياسي في العلاقات الدولية، في هذا السياق، يتم استخدام التقنيات الرقمية الحديثة لسرقة المعلومات الحساسة من الحكومات والشركات والأفراد، وهو ما يخلق تحديات كبيرة للدول التي تسعى للحفاظ على أمنها القومي، هذا النوع من الصراع السيبراني أصبح يشكل تهديدًا كبيرًا للأمن الوطني، حيث يمكن أن تؤدي الهجمات السيبرانية إلى اختراق نظم الدفاع وأجهزة الاستخبارات، وبالتالي تدمير القدرات العسكرية والتقنية لدولة ما (خليفة، إيهاب، 2020، ص 46–78).

علاوة على ذلك، تحاول بعض الدول استغلال الفضاء السيبراني كأداة لتقويض استقرار الدول المنافسة أو المعادية، على سبيل المثال، قد تقوم بعض الحكومات بزرع برامج خبيثة في شبكات حكومية أو مؤسسات مالية في دول أخرى، بهدف تعطيل العمل بها أو التأثير على الاقتصاد الوطني، لا تقتصر الهجمات السيبرانية على سرقة البيانات العسكرية فقط، بل تشمل أيضًا محاولة التأثير في الرأي العام والسياسة الداخلية للدول المستهدفة، حملات التضليل المعلوماتي عبر الإنترنت تعد واحدة من أبرز أشكال هذا الصراع السيبراني، حيث يمكن أن تقوم دول بتوزيع الأخبار الكاذبة أو تحريف الحقائق بهدف زعزعة استقرار الحكومات أو التأثير في الانتخابات (Cardash, Sharon, 2021, pp. 42–61).

2. تأثير الهجمات السيبرانية على البنية التحتية الحيوية للدول:

تُعد الهجمات السيبرانية على البنية التحتية الحيوية من أخطر التهديدات التي تواجه الدول، إذ قد تؤدي إلى تعطيل شبكات الكهرباء، والاتصالات، والرعاية الصحية، والأنظمة المالية، هذه الهجمات لا تضر فقط بالخدمات الأساسية، بل تهدد أيضًا الأمن القومي والاستقرار الاقتصادي، كما يمكن أن تستغلها جهات معادية أو جماعات إرهابية لتحقيق أهداف تخريبية (Schulze, Matthias, 2020, pp. 48–66).

3. صعوبة تحقيق التوازن بين الأمن القومي وحماية الحريات الرقمية:

تحقيق التوازن بين الأمن القومي وحماية الحريات الرقمية يُعد من أكثر التحديات تعقيدًا في العصر الرقمي، فبينما تسعى الدول إلى تعزيز أمنها السيبراني لمواجهة التهديدات الإلكترونية، قد تؤدي بعض السياسات الأمنية إلى المساس بحقوق الأفراد، مثل الخصوصية وحرية التعبير، ويتطلب ذلك صياغة سياسات دقيقة تراعي احتياجات الأمن وتحترم الحقوق الأساسية (Eze, Friday Ikechukwu, 2019, pp. 84–91).

في المقابل، تثير إجراءات مثل مراقبة البيانات وحظر بعض المواقع قلقًا متزايدًا بشأن توسع صلاحيات الحكومات في الفضاء الرقمي، لذا، يجب تطوير تقنيات قانونية وتقنية تضمن الشفافية والمساءلة، وتمنع استخدام الأمن السيبراني كذريعة لتقييد الحريات (Graham, David, 2019, pp. 43–56).

من خلال هذا المطلب، **يتضح للباحث** إن التحديات السياسية والاستراتيجية التي أُثيرت في هذا المطلب تعد من أكثر الأبعاد تعقيدًا في الفضاء السيبراني، وهذا يبرز بشكل جلي من خلال تأثيراتها على الأمن القومي والعلاقات الدولية، كباحث، أعتقد أن هناك مسألتين يجب أن تُعطى لهما أولوية أكبر عند تناول هذه القضايا :**التطور السريع في استخدام الفضاء السيبراني كأداة للصراع بين الدول**، و**التحدي المتمثل في تحقيق التوازن بين الأمن القومي والحريات الرقمية**.

أولًا، أود أن أؤكد على **الاستراتيجية المتطورة لاستخدام الفضاء السيبراني كأداة للتجسس والصراع**، ما نراه اليوم من هجمات سيبرانية تهدف إلى **الاختراق والسرقة** أو حتى **إحداث فوضى سياسية** يتطلب استجابة منسقة ومتكاملة بين دول العالم، فمفهوم **الحرب السيبرانية** بات واقعًا لا مفر منه، ويجب أن نواكب هذا الواقع بتعزيز **البحث والتطوير في الأدوات الدفاعية السيبرانية**، لكن ما يثير القلق بالنسبة لي هو **استغلال الفضاء السيبراني كأداة للتأثير على سياسات الدول الداخلية**، وخاصة عبر **حملات التضليل** أو التلاعب بالرأي العام، وهو ما يساهم في إضعاف النظم الديمقراطية، هذا التوجه يعكس ضرورة التفكير في **استراتيجيات دفاعية محورية** ضد هذه الأنماط الهجومية، والتي قد تتجاوز الحدود التقليدية للصراع بين الدول.

ثانيًا، يُعتبر **التأثير على البنية التحتية الحيوية** للدول من أخطر الآثار السلبية للهجمات السيبرانية، وهذا ما يجعل **حماية تلك البنى** أولوية، لكن من جانب آخر، **التأثير على الحياة اليومية** قد يكون متزايدًا، ويجب أن يعي المسؤولون في مختلف الدول أن تأثير الهجمات السيبرانية يمكن أن يتعدى **المجال العسكري والاقتصادي** إلى تأثيرات **اجتماعية وثقافية** تتعلق برفاهية الأفراد، وهذا هو التحدي الأعمق في الأمن السيبراني.

أما فيما يتعلق **بالتوازن بين الأمن القومي وحماية الحريات الرقمية**، أرى أن هذه القضية تُثير العديد من الأسئلة الفلسفية والعملية، من جهة، من الضروري تعزيز **الأمن السيبراني** لحماية الأنظمة الحيوية من الهجمات، ولكن من جهة أخرى، يجب أن تكون هناك **ضوابط قانونية** واضحة تحكم السياسات الأمنية، تضمن الحفاظ على **الحقوق الفردية**، فما يزعجني هنا هو **استغلال التحديات الأمنية كذريعة لتقليص الحريات**، مثل انتهاك الخصوصية أو تقييد حرية التعبير، لذلك، من واجبنا كباحثين وكتقنيين وضع حلول تشريعية مبتكرة تضمن **الشفافية والمساءلة** في السياسات الأمنية، وتبقي **الحريات الرقمية مصونة** في ظل تزايد التهديدات.

من خلال هذا المطلب، أرى أن **الإجابة على هذه التحديات** ليست في مجرد تعزيز الأدوات الدفاعية أو تطوير التشريعات، بل في **إيجاد توازن دقيق بين حماية الأمن السيبراني وحماية الحقوق**، كما أنه من المهم أن تبادر الدول إلى التعاون الفعّال في هذا السياق، ويجب أن تكون سياساتها السيبرانية **دولية ومتوافقة** مع معايير حقوق الإنسان، مع **الاستفادة من التقنيات الحديثة** بشكل يضمن الحفاظ على الأمن الشخصي والعالمي في آن واحد.

IJMMC
International journal For Media
Mass Communication &

المبحث الثالث

استراتيجيات تعزيز الأمن السيبراني في العلاقات الدولية

تمهيد وتقسيم:

يُعد التعاون الدولي وتطوير السياسات الوطنية والإقليمية من أبرز استراتيجيات تعزيز الأمن السيبراني، ويهدف هذا المبحث إلى دراسة الجهود الدولية والإقليمية التي تسهم في مواجهة التهديدات السيبرانية المتزايدة.

- **المطلب الأول: التعاون الدولي في مجال الأمن السيبراني**
- **المطلب الثاني: الاستراتيجيات الوطنية والإقليمية**

المطلب الأول

التعاون الدولي في مجال الأمن السيبراني

تلعب المنظمات الدولية دورًا حاسمًا في توجيه وتنسيق الجهود العالمية لمكافحة الجرائم السيبرانية، من خلال وضع معايير مشتركة وتعزيز التعاون بين الدول، كما يُعد تبادل المعلومات والخبرات التقنية بين الدول عنصرًا أساسيًا لمواجهة التهديدات السيبرانية المتطورة، خاصة مع تفاوت القدرات التقنية بين الدول (جيلالي، دلالي، 2021، ص 18–32).

إضافة إلى ذلك، ظهرت العديد من الاتفاقيات والمعاهدات الدولية التي تهدف إلى وضع أسس للتعاون بين الدول في مجال الأمن السيبراني، لضمان الاستجابة الفعالة ضد التهديدات السيبرانية، وتُعد هذه الاتفاقيات من الأدوات الأساسية التي تضمن التنسيق بين الحكومات وتحديد المسؤوليات القانونية، وتساهم في تعزيز التعاون التقني والمعلوماتي بين الدول في هذا المجال الحيوي (خميس، لبني، 2020، ص 145–152).

في هذا السياق، يتناول هذا المطلب أهمية التعاون الدولي في مجال الأمن السيبراني، مع التركيز على دور المنظمات الدولية في وضع المعايير، أهمية تبادل المعلومات والخبرات، والنماذج المبدعة للاتفاقيات والمعاهدات الدولية التي تمثل أساس التعاون بين الدول لمكافحة الجرائم السيبرانية وضمان الأمن الرقمي.

1. دور المنظمات الدولية (مثل الأمم المتحدة، والاتحاد الدولي للاتصالات) في وضع معايير الأمن السيبراني:

تعد الجريمة السيبرانية تحديًا متزايدًا في العصر الرقمي، وقد أدركت الأمم المتحدة ضرورة التصدي لهذه الجرائم العالمية، في عام 1950، أوصى المجلس الاقتصادي والاجتماعي التابع للأمم المتحدة بأن تكون المنظمة الدولية جزءًا رئيسيًا في رسم سياسة لمنع الجريمة وتحقيق العدالة الجنائية الدولية، هذا التوجه تحقق عندما أنشأت الأمم المتحدة "اللجنة الاستشارية لخبراء منع الجريمة"، التي تهدف إلى وضع السياسات الدولية المتعلقة بالجريمة، بما في ذلك الجرائم السيبرانية (Edelman, David, 2013, pp. 201–255).

وبشأن جهود الاتحاد الدولي للاتصالات، فإن الاحتياجات الأمنية العالمية في مجال تكنولوجيا المعلومات تتطلب استراتيجيات قوية، وهو ما يعزز دور الاتحاد الدولي للاتصالات(ITU) ، منذ تأسيسه في 1865، أصبح الاتحاد لاعبًا رئيسيًا في تعزيز الأمن السيبراني من خلال تطوير استراتيجيات دولية شاملة، أبرز هذه الجهود هو إطلاق دليل الاستراتيجية الوطنية للأمن السيبراني الذي يقدم لدول العالم إطارًا لتطوير سياسات فعالة في هذا المجال، ويشمل الجوانب التقنية والقانونية (Clark, David, 2014, pp. 54–67).

وعن دور المعهد الوطني للمعايير والتكنولوجيا، فإن المعهد الوطني للمعايير والتكنولوجيا (NIST) في الولايات المتحدة يعد من الرواد في تطوير معايير الأمن السيبراني، أطلق المعهد في 2014 إطارًا شاملاً للأمن السيبراني، يتضمن خمسة عناصر رئيسية: التحديد، الحماية، الكشف، الاستجابة، والتعافي، يساعد هذا الإطار المؤسسات على تقييم المخاطر وتحسين استراتيجيات الأمان السيبراني (Buzan, Barry, 2009, pp. 121–134).

2. أهمية تبادل المعلومات والخبرات بين الدول لمكافحة الجرائم السيبرانية:

تبادل المعلومات هو من الأسس الرئيسية التي يقوم عليها التعاون الدولي في مجال مكافحة الجرائم السيبرانية، في العديد من الحالات، تكون المعلومات حول الهجمات السيبرانية والمهاجمين متاحة فقط في الدول التي تعرضت لهذه الهجمات، ولكن نظرًا للطبيعة العابرة للحدود للجرائم السيبرانية، فإن مشاركة هذه المعلومات مع **الدول الأخرى** أمر حيوي لمكافحة هذه الجرائم بشكل فعال (Segal, Adam, 2022, pp. 98–112).

إلى جانب التعاون بين الدول والحكومات، يجب أيضًا تعزيز التعاون بين **القطاعين العام والخاص** في مجال **الأمن السيبراني**، الشركات الكبيرة، خاصة في القطاعات الحيوية مثل **الطاقة**، و**المالية**، و**الاتصالات**، تمتلك معلومات وبيانات حيوية يمكن أن تكون مفيدة في التصدي للجرائم السيبرانية، من خلال تبادل **البيانات** و**التجارب** مع الحكومات والوكالات الأمنية، يمكن للقطاع الخاص أن يلعب دورًا كبيرًا في تعزيز **الأمن السيبراني** عالميًا (Muller, Benedikt, 2014, pp. 33–67).

3. نماذج للاتفاقيات والمعاهدات الدولية في مجال الأمن السيبراني:

فيما يلي بعض النماذج البارزة للاتفاقيات والمعاهدات الدولية في مجال الأمن السيبراني التي تسعى إلى تعزيز التعاون بين الدول لمكافحة التهديدات السيبرانية وحماية البنية التحتية الرقمية:

1 – اتفاقية بودابست:

تعد **اتفاقية بودابست** واحدة من أهم المعاهدات الدولية في مجال الأمن السيبراني، التي تم تبنيها في **عام 2001** من قبل **مجلس أوروبا**، وهي أول معاهدة دولية ملزمة قانونًا تهدف إلى مكافحة **الجريمة السيبرانية**، تهدف الاتفاقية إلى تزويد الدول الأعضاء بإطار قانوني فعال للتعاون في التحقيقات والملاحقات القضائية المرتبطة بالجرائم الإلكترونية، تغطي الاتفاقية مجموعة واسعة من الأنشطة، بما في ذلك القرصنة، والاحتيال الإلكتروني، وانتهاك حقوق الملكية الفكرية عبر الإنترنت، والجرائم المتعلقة بالمحتوى غير القانوني على الإنترنت، والاعتداءات على الشبكات (Wenger, Andreas, 2022, pp. 211–230).

2 – اتفاقية مالابو (اتفاقية الاتحاد الإفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية):

اتفاقية مالابو أو **اتفاقية الاتحاد الإفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية** (هي معاهدة تم اعتمادها في **2014**من قبل **الاتحاد الإفريقي**، تهدف الاتفاقية إلى تعزيز **الأمن السيبراني** في **الدول الإفريقية** وحماية **البيانات الشخصية** في إطار **عالمي**، وتعتبر خطوة رئيسية نحو تأمين الفضاء السيبراني في قارة إفريقيا.

تنص الاتفاقية على تجريم عدد من الأنشطة السيبرانية مثل **القرصنة**، **الاحتيال الإلكتروني**، و**التهديدات المتقدمة**، بالإضافة إلى تقديم إطار لحماية **الخصوصية** و**البيانات الشخصية**، كما تدعو الاتفاقية الدول الأعضاء إلى إنشاء **هيئات حماية البيانات الشخصية** لضمان معالجة البيانات بطريقة آمنة وقانونية.

3 – الإطار الإقليمي للاتحاد الدولي للاتصالات (ITU) بشأن الأمن السيبراني:

يعد **الاتحاد الدولي للاتصالات** (ITU)من المنظمات الدولية الرائدة في مجال وضع **المعايير** والتوجيهات المتعلقة بالأمن السيبراني، في هذا الإطار، قام الاتحاد بتطوير عدد من المبادرات والاتفاقيات التي تهدف إلى تعزيز التعاون الدولي في مواجهة

التهديدات السيبرانية، على سبيل المثال، تم إطلاق **الإطار الإقليمي للأمن السيبراني** في **منطقة آسيا والهادئ** والذي يسعى إلى تعزيز القدرات الإقليمية في مجال الأمن السيبراني وتنسيق الجهود بين الدول الأعضاء (هادي، سهيلة، 2017، ص 12–19).

وبذلك يتبين للباحث أن المنظمات الدولية مثل الأمم المتحدة والاتحاد الدولي للاتصالات تساهم في وضع المعايير وتنسيق الجهود، يُعد تبادل المعلومات والخبرات بين الدول عنصرًا أساسيًا في التصدي للجرائم السيبرانية، كذلك، تُعتبر الاتفاقيات الدولية مثل اتفاقية بودابست ومالابو أدوات حيوية لتوجيه التعاون بين الدول في مواجهة التهديدات الرقمية المتزايدة.

المطلب الثاني

الاستراتيجيات الوطنية والإقليمية

تتمثل أهمية هذا المطلب في ضرورة أن تتبنى الدول استراتيجيات وطنية محكمة لتعزيز القدرات السيبرانية، بالإضافة إلى تعزيز التعاون الإقليمي من خلال اتفاقيات متعددة الأطراف أو ثنائية، بهدف تأمين الفضاء السيبراني وتعزيز قدرة الدول على مواجهة التهديدات المتزايدة، ويشمل ذلك التركيز على التدريب والتأهيل المستمر لبناء كوادر قادرة على التصدي لتلك التهديدات.

1. وضع استراتيجيات وطنية شاملة للأمن السيبراني:

تناولت اتفاقية بودابست الخاصة بالجريمة السيبرانية العديد من التدابير الضرورية التي يجب أن تتخذها الدول على الصعيد الوطني لضمان الأمن السيبراني وحماية الفضاء الإلكتروني، يركز الجزء الثاني من هذه الاتفاقية على الإجراءات اللازمة على الصعيد الوطني، حيث يتم تقسيمها إلى قسمين رئيسيين: الأول يتعلق بالقانون الجنائي الموضوعي، في حين أن الثاني يتناول الجوانب المتعلقة بالحوكمة، الوقاية من الفساد، ومكافحته، وفي هذه الدراسة، سيتم التركيز على القسم الأول الذي يتناول الجوانب الموضوعية للجرائم المعلوماتية، حيث يتناول المواد من (2) إلى (13) من الاتفاقية.

أولاً: الجرائم ضد سرية وسلامة وإتاحة البيانات والنظم المعلوماتية

تعد الجرائم المرتكبة ضد سرية البيانات وسلامة النظم المعلوماتية من أخطر الجرائم التي تهدد الأفراد والمجتمعات والدول في العصر الرقمي، وقد تناولت اتفاقية بودابست لمكافحة الجرائم الإلكترونية، التي تم تبنيها في عام 2001 تحت إشراف مجلس أوروبا، العديد من هذه الجرائم التي تهدد الأمن السيبراني، وتتضمن خمس جرائم رئيسية تستهدف سرية البيانات وسلامة النظم المعلوماتية (بطيخ، حاتم، 2021، ص 34).

أولاً، جريمة النفاذ (الولوج) غير المشروع، التي تتضمن دخول الأفراد أو البرامج إلى الأنظمة المعلوماتية دون إذن بهدف سرقة البيانات أو إحداث أضرار، هذه الجريمة تشكل تهديدًا خطيرًا للنظم الأمنية وتهدد بكشف أو سرقة معلومات حساسة، ثانيًا، جريمة الاعتراض غير المشروع للبيانات، حيث يتم اعتراض البيانات المرسلة عبر الشبكات أو الأنظمة باستخدام تقنيات غير قانونية، مما يعرض سرية المعلومات للخطر (أحمد، هلالي عبد اللاه، 2011، ص 56).

أما ثالثًا، فتتعلق جريمة الاعتداء على سلامة البيانات، التي تشمل محو أو تعطيل أو التلاعب بالبيانات بشكل ضار، هذه الجريمة قد تؤدي إلى ضياع أو تلاعب في بيانات حساسة، مما يعرض المؤسسات لخطر فقدان معلومات أساسية، رابعًا، جريمة الاعتداء على سلامة النظام، التي تشمل تعطيل الأنظمة المعلوماتية أو إدخال بيانات ضارة لعرقلة عمل النظام، وأخيرًا، جريمة إساءة استخدام أجهزة الحاسب، التي تشمل استخدام البرمجيات الضارة أو أدوات القرصنة في ارتكاب الجرائم الإلكترونية (أحمد، هلالي عبد اللاه، 1997، ص 48).

ثانيًا: الجرائم المعلوماتية المتصلة بالحاسب الآلي

تناولت اتفاقية بودابست العديد من الجرائم التي ترتبط بتقنيات الحاسب الآلي، والتي تشكل تهديدًا مباشرًا للأمن السيبراني، من أبرز هذه الجرائم (جمال الدين، هيه، 2023، ص 190–201):

1. **جريمة التزوير المعلوماتي:** تجريم التلاعب بالبيانات الإلكترونية بهدف إحداث تغييرات تظهر كأنها صحيحة، لكن في الواقع هي مزورة، يشمل ذلك إدخال أو محو أو طمس بيانات بهدف إنشاء معلومات كاذبة.
2. **جريمة الاحتيال المعلوماتي:** تجريم الأفعال التي تؤدي لتحقيق منافع غير مشروعة باستخدام تقنيات الحاسب، مثل الاحتيال المصرفي أو التلاعب بالأسواق المالية، مما يهدد الاقتصاد الرقمي وأمن المعاملات المالية

ثالثًا: الجرائم المتصلة بالمحتوى

الجرائم المتصلة بالمحتوى غير المشروع، مثل إنتاج أو نشر المواد الإباحية للأطفال، تشكل تهديدًا كبيرًا للأمن السيبراني، حيث تهدد البنية الأخلاقية والاجتماعية للمجتمعات، بما يشمل الأضرار النفسية للأطفال واستغلالهم بطريقة غير قانونية عبر الإنترنت.

رابعًا: الجرائم المتعلقة بالاعتداءات على الملكية الفكرية

الاعتداءات على حقوق الملكية الفكرية عبر الإنترنت أصبحت من الجرائم المتزايدة في الفضاء السيبراني، تُعنى المادة العاشرة من الاتفاقية بالجرائم التي تتعلق بالتعدي على حقوق الملكية الفكرية، مثل نسخ أو توزيع الأعمال المحمية بحقوق الطبع والنشر دون إذن عبر الأنظمة المعلوماتية، تعتبر هذه الجرائم تحديًا كبيرًا في ظل الانتشار الواسع للإنترنت ووسائل التواصل الاجتماعي، حيث يمكن توزيع المحتوى المحمي بشكل سريع وغير قانوني (عودة، نبيل، 2022، ص 18–31).

خامسًا: مسئولية الأشخاص المعنوية

تُعد مسئولية الأشخاص المعنوية، مثل الشركات والمؤسسات، أحد أبرز الموضوعات التي تناولتها اتفاقية بودابست، يهدف هذا المبدأ إلى ضمان محاسبة المؤسسات عن الجرائم التي تُرتكب لمصلحتها، سواء كانت تلك الجرائم جنائية أو مدنية أو إدارية، وفقًا للمادة الثانية عشرة من الاتفاقية، تشترط الدول الأعضاء اتخاذ التدابير التشريعية اللازمة لمحاسبة الأشخاص المعنوية التي ترتكب أو تُسهّل الجرائم الإلكترونية، هذا المبدأ يكتسب أهمية بالغة في العصر الرقمي، حيث لا تقتصر الجريمة السيبرانية على الأفراد فقط بل تشمل أيضًا المنظمات التي قد تساهم بشكل مباشر أو غير مباشر في تنفيذ تلك الجرائم (علي، مرعي، 2022، ص 32–55).

2. تعزيز القدرات الوطنية في مجال الأمن السيبراني

في ضوء التحديات المستمرة والمتزايدة في مجال الأمن السيبراني، يصبح تعزيز القدرات الوطنية أحد الأولويات الأساسية للدول، يتطلب هذا تعزيز وتطوير التقنيات، التشريعات، والتدريب المتخصص، وذلك لضمان مواجهة تهديدات الجرائم السيبرانية بفعالية، الأمن السيبراني ليس مسألة محلية فحسب، بل يتعدى الحدود الوطنية ليشمل تهديدات قد تضر بالدول الأخرى، هذا الواقع يحتم على الدول أن تكون لديها البنية التحتية الكفيلة لمواجهة هذه التهديدات وحماية المعلومات الحساسة (الميموني، أحمد، 2020، ص 13–19).

1–تطوير البنية التحتية الرقمية

تعد البنية التحتية الرقمية من العوامل الحيوية التي تساهم في تعزيز الأمن السيبراني الوطني، يتطلب هذا تطوير الأنظمة والشبكات بشكل مستمر لكي تكون قادرة على التعامل مع التهديدات السيبرانية المتزايدة، البنية التحتية الرقمية تشمل الشبكات الداخلية للمؤسسات الحكومية والشركات الخاصة، بالإضافة إلى الأنظمة السحابية التي أصبحت أكثر عرضة للهجمات، من المهم تحديث هذه الأنظمة بشكل دوري وتزويدها بالتقنيات اللازمة لمكافحة البرمجيات الخبيثة والفيروسات (القحطاني، محمد، 2020، ص 23).

2-التشريعات والسياسات الوطنية للأمن السيبراني

تعتبر التشريعات والسياسات الوطنية ركيزة أساسية في مكافحة الجرائم السيبرانية، لا بد من أن تواكب القوانين الوطنية التطورات التكنولوجية المستمرة التي تظهر بشكل متسارع، التشريعات الوطنية يجب أن تشمل قوانين تتعلق بالقرصنة الإلكترونية، الاحتيال الرقمي، وتهديدات أخرى تستهدف المعلومات الحساسة والأنظمة الإلكترونية، يعتبر قانون حماية البيانات الشخصية، مثل اللائحة العامة لحماية البيانات(GDPR) ، نموذجًا مهمًا يُحتذى به في العديد من البلدان (فاتح، حارك، 2022، ص 78-99).

3. التعاون الدولي والإقليمي لمكافحة الجرائم السيبرانية

في عالم مترابط تكنولوجيًا، لم تعد الجرائم السيبرانية مقتصرة على نطاق الحدود الوطنية فقط، بل أصبحت هذه الجرائم تتخطى الحدود الجغرافية، مما يتطلب تعاونًا دوليًا مستمرًا لمكافحتها، يتمثل هذا التعاون في تبادل المعلومات حول الهجمات السيبرانية، المهاجمين، والأساليب المستخدمة في الهجمات (Warren, P., Kaivanto, K., & Prince, D., 2018, pp. 21-30).

من أبرز الأمثلة على التعاون الدولي في هذا المجال هي اتفاقية بودابست لمكافحة الجريمة السيبرانية، التي تسهم في تعزيز التعاون بين الدول الأعضاء لتبادل المعلومات والتنسيق في التحقيقات، إضافة إلى ذلك، تعزز الاتفاقيات الإقليمية، مثل الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، التعاون بين الدول العربية لمواجهة التهديدات السيبرانية التي تهدد الأمن الرقمي للدول (Robinson, M., Jones, K., & Janicke, H., 2015, pp. 70-94)

تمثل الاتفاقيات الإقليمية أداة هامة في تعزيز التعاون بين الدول لمكافحة الجرائم السيبرانية، الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، على سبيل المثال، توفر إطارًا قانونيًا موحدًا يسمح للدول العربية بتبادل المعلومات وتنسيق جهودها لمكافحة الجرائم الإلكترونية، تهدف هذه الاتفاقية إلى توحيد التشريعات، تجريم الأفعال المرتبطة بتقنيات المعلومات، وتعزيز التعاون القضائي بين الدول الأطراف (Pagallo, U., 2015, pp. 407-425).

من خلال التعاون الإقليمي، يمكن تبادل أفضل الممارسات، وتقديم التدريب المشترك، وتعزيز الاستجابة السريعة للهجمات السيبرانية التي تؤثر على أكثر من دولة في نفس الوقت، يساهم هذا التعاون في تطوير استراتيجيات مشتركة وموحدة لمكافحة الجرائم السيبرانية، ويعزز من أمن الفضاء الإلكتروني على المستوى الإقليمي (Panait, I., 2015, p. 130).

وبذلك تسهم هذه الاستراتيجيات في تعزيز القدرات السيبرانية لمواجهة التهديدات المتزايدة، يشمل ذلك تطوير التشريعات، تعزيز التعاون الدولي والإقليمي، وتبادل المعلومات لضمان حماية الفضاء السيبراني والبنية التحتية الرقمية، وبالتالي تعزيز الأمن الرقمي على المستويين الوطني والإقليمي.

الخاتمة

في الختام، يمكن القول إن الأمن السيبراني لم يعد مجرد مسألة تقنية أو محلية، بل أصبح عنصراً أساسياً في العلاقات الدولية، حيث يرتبط بشكل وثيق بالأمن الوطني، الاستقرار الاقتصادي، والسياسي في مختلف أنحاء العالم، تطور الفضاء السيبراني أصبح يشكل تحديات غير مسبوقة على مستوى الحكومات والشركات والمجتمعات، خاصة مع تنامي التهديدات السيبرانية التي يمكن أن تؤثر بشكل كبير على البنية التحتية الحيوية، لذا فإن دراسة هذه الظاهرة، وفهم تأثيراتها، وتحديد سبل مواجهة التهديدات السيبرانية تكتسب أهمية متزايدة.

وسنتناول هنا أبرز النتائج التي تم الوصول إليها من خلال هذا البحث، كما سنقدم توصيات عملية لتعزيز الأمن السيبراني في العلاقات الدولية، مع اقتراح مواضيع لبحوث مستقبلية قد تسهم في تطوير هذا المجال الحيوي.

- **أهم النتائج التي توصل إليها البحث:**

من خلال البحث، تم التأكيد على أن **الأمن السيبراني** أصبح أحد العوامل الأساسية في العلاقات الدولية المعاصرة، حيث يعكس تأثير التهديدات السيبرانية على **الأمن الوطني**، **الاقتصاد**، و**الاستقرار السياسي**، كما أوضح البحث أن التهديدات السيبرانية ليست مقتصرة على **الهجمات التقليدية** مثل الفيروسات، بل تتضمن أيضًا الهجمات على **البنية التحتية الحيوية** مثل الطاقة، الصحة، والنقل، ما يجعل تأثيرها على العلاقات الدولية بالغ الخطورة.

وقد تم تسليط الضوء على أن **الفضاء السيبراني** يتسم بطبيعته **العابرة للحدود**، ما يجعل من الصعب تحديد المسؤولية القانونية بوضوح، مما يزيد من تعقيد التعاون الدولي لمكافحة هذه التهديدات، كما تبين أن التعاون بين **الدول الكبرى** و**المنظمات الدولية** مثل **الأمم المتحدة** و**الاتحاد الأوروبي** يعد أمرًا حيويًا في إيجاد حلول فعّالة لهذه التهديدات عبر إنشاء **إطار قانوني موحد** يمكن أن يشمل جميع الدول، علاوة على ذلك، أثبت البحث أن **الأسلحة السيبرانية** أصبحت جزءًا من **استراتيجيات الحروب الحديثة**، مما يساهم في تصعيد التوترات بين الدول الكبرى.

- **تقديم توصيات عملية لتعزيز الأمن السيبراني في العلاقات الدولية:**

تطوير إطار قانوني دولي موحد: ينبغي على الدول والمنظمات الدولية العمل معًا لتطوير **اتفاقيات قانونية دولية** ملزمة تتعلق بالأمن السيبراني، مثل تعزيز اتفاقية **بودابست لمكافحة الجريمة السيبرانية** وتحديثها لتشمل التهديدات الجديدة مثل **الأسلحة السيبرانية** والهجمات على البنية التحتية الحيوية.

تعزيز التعاون الدولي: يجب تعزيز التعاون بين الدول في مجال **مشاركة المعلومات** حول التهديدات السيبرانية، خاصة في حالات **الهجمات العابرة للحدود**، يمكن تحقيق ذلك من خلال **مراكز تعاون سيبراني** تعمل على مدار الساعة، مثل شبكة الطوارئ 7/24 التي توفر مساعدة فورية في التحقيقات السيبرانية.

تعليم وتدريب الخبراء: من الضروري زيادة الاستثمارات في **التعليم والتدريب** في مجال الأمن السيبراني، يجب أن يكون هناك برامج أكاديمية متخصصة ومبادرات تدريبية لرفع **الوعي السيبراني** لدى الأفراد والشركات على حد سواء، بالإضافة إلى تدريب الحكومات على الرد السريع في حالات الهجمات السيبرانية.

تقوية القطاع الخاص: على الدول أن تعزز التعاون بين **القطاعين العام والخاص** لتحسين مستوى الأمن السيبراني، يجب على الشركات الكبرى في **قطاع التكنولوجيا** التعاون مع الحكومات لتبادل المعلومات حول التهديدات السيبرانية وتطوير أدوات متقدمة للحماية.

التعاون الإقليمي: من الأهمية بمكان أن تشارك **المنظمات الإقليمية** مثل **الاتحاد الأفريقي** و**الجامعة العربية** في وضع آليات عمل للتعاون في مجال الأمن السيبراني بين الدول الأعضاء لتطوير الأطر القانونية والتقنية في مكافحة الجرائم السيبرانية.

- **اقتراح موضوعات لبحوث مستقبلية في مجال الأمن السيبراني:**

دور الذكاء الاصطناعي في الأمن السيبراني: دراسة كيفية استخدام تقنيات الذكاء الاصطناعي في التصدي للهجمات السيبرانية وتحليلها بشكل أسرع وأكثر دقة.

تأثير الحروب السيبرانية على السياسة الدولية: دراسة تطور **الأسلحة السيبرانية** وتداعياتها على العلاقات السياسية بين الدول، وكيفية تحديد مسؤولية الهجمات السيبرانية في أوقات النزاع العسكري.

الأمن السيبراني في الاقتصادات النامية: دراسة التحديات التي تواجه الدول النامية في تعزيز **الأمن السيبراني**، وكيفية مساعدتها في تطوير **القدرات المحلية** لحماية الفضاء الرقمي.

حماية الخصوصية في الفضاء السيبراني: بحث تأثير الهجمات السيبرانية على **الخصوصية** و**حقوق الأفراد** في الفضاء السيبراني، واقتراح آليات قانونية جديدة لحمايتها.

التعاون الدولي في مواجهة الهجمات السيبرانية العابرة للحدود: دراسة استراتيجيات التعاون بين الدول المختلفة في التصدي للهجمات السيبرانية التي تتجاوز الحدود الوطنية وتؤثر على الأمن العالمي.

قائمة المراجع

أولا: قائمة المراجع باللغة العربية:

- أحمد، هلالي عبد اللاه. .(1997) *تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي*. دار النهضة العربية.
- أحمد، هلالي عبد اللاه. .(2011) *اتفاقية بودابست لمكافحة جرائم المعلوماتية: معلقا عليها*. دار النهضة العربية.
- البعلبكي، منير. .(2004) *المورد: قاموس إنجليزي عربي*. بيروت: دار العلم للملايين.
- الفتلاوي، أحمد. .(2016) *الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر*. *مجلة المحقق الحلي للعلوم القانونية والسياسية*، السنة 8، العدد 4.
- القحطاني، محمد. .(2020) *قدرات القرصنة السيبرانية الإيرانية*. مركز الملك فيصل للبحوث والدراسات الإسلامية، الرياض.
- الميموني، أحمد. .(2020) *الجبهة النشطة: تداعيات المواجهة السيبرانية بين إيران وإسرائيل*. *مجلة الدراسات الإيرانية*، السنة الرابعة، العدد 12، المعهد الدولي للدراسات الإيرانية، الرياض، أكتوبر.
- بطيخ، حاتم. .(2021) *تطور السياسة التشريعية في مجال مكافحة جرائم تقنية المعلومات: دراسة تحليلية مقارنة*. *مجلة الدراسات القانونية والاقتصادية*، جامعة السادات، مجلد 5، العدد 1، أغسطس.
- جمال الدين، هيه. .(2023) *الأمن السيبراني والتحول في النظام الدولي*. *مجلة كلية الاقتصاد والعلوم السياسية*، المجلد 24، العدد الأول، جامعة القاهرة، يناير.
- جيلالي، دلالي. .(2021) *رهانات الأمن السيبراني الوطني في ظل التحول الرقمي: قراءة في التأصيل المعرفي واستراتيجية المواجهة التشريعية*. *مجلة كلية القانون الكويتية العالمية*، السنة العاشرة، العدد الأول، الكويت.
- خليفة، إيهاب. .(2020) *الحرب السيبرانية: الاستعداد لقيادة المعارك العسكرية في الميدان الخامس*. القاهرة: مركز المستقبل للأبحاث والدراسات المتقدمة.
- خليل، حازم محمد. .(2023) *استغلال الفضاء السيبراني في الحروب غير التقليدية: دراسة في الوكالة السيبرانية والإرهاب السيبراني*. *مجلة كلية الدراسات الاقتصادية والعلوم السياسية*، المجلد 8، العدد 15، جامعة الإسكندرية.
- خميس، لبني. .(2020) *أثر السيبرانية في تطور القوة*. *مجلة حمورابي*، العدد 33، كلية العلوم السياسية، جامعة النهرين، بغداد.
- زروقة، إسماعيل. .(2018) *الفضاء السيبراني والتحول في مفاهيم القوة والصراع*. *مجلة العلوم القانونية والسياسية*، المجلد 10، العدد 1، جامعة محمد بوضياف، الجزائر.
- عصام محمد، أماني. .(2022) *استخدام روسيا للقوة السيبرانية في إدارة تفاعلاتها الدولية*. *مجلة كلية الاقتصاد والعلوم السياسية*، المجلد 22، جامعة القاهرة، أكتوبر.
- علي، مرعي. .(2022) *الحرب السيبرانية ومتطلبات الأمن القومي الجديدة*. المركز الديمقراطي العربي للدراسات الاستراتيجية والسياسية والاقتصادية، برلين.
- عودة، نبيل. .(2022) *العمليات السيبرانية في الحرب الروسية الأوكرانية: طبيعتها وأنماطها*. مركز الشرق للأبحاث الاستراتيجية، إسطنبول، سبتمبر.

- فاتح، حارك. .(2022) *الفضاء السيبراني والتحول في شكل الحروب: دراسة حالة روسيا*. رسالة ماجستير، كلية العلوم السياسية، جامعة القسطنطينية، الجزائر.
- ماجد، محمد. .(2021) *الأبعاد التنموية والاستراتيجية للأمن السيبراني ودوره في دعم الاقتصادات الرقمية والمشفرة. سلسلة قضايا التخطيط والتنمية*، العدد 326، معهد التخطيط القومي، القاهرة، أغسطس.
- هادي، سهيلة. .(2017) *الحروب الإلكترونية في ظل عصر المعلومات. رؤى استراتيجية*، المجلد الرابع، العدد 14، مركز الإمارات للدراسات والبحوث الاستراتيجية، يونيو.
- وزارة الدفاع الأمريكية. .(2010) *قاموس المصطلحات العسكرية الأمريكي*.

ثانيا: قائمة المراجع باللغة الأجنبية:

- Melzer, Nils (2001). *Cyber Warfare and International Law*. IDEAS for Peace and Security, Under Researches.
- Adewale, Lukman. (2020). *Cyber Theater: A Fifth Domain of International Politics: Africa and The Rest of The World in The Cyberspace*. National Institute for Policy and Strategic Studies, Nigeria.
- Andress, Jason, & Winterfeld, Steve (2011). *What is cyber warfare?* In Rogers, R. (Ed.), *Cyber Warfare: Techniques, Tactics, and Tools for Security Practitioners*. New York: Elsevier Inc.
- Baezner, Marie. (2018). *Cyber and Information Warfare in The Ukrainian Conflict*. Center for Security Studies, Zurich.
- Banks, William. (2021). *Cyber Attribution and State Responsibility*. International Law Studies, Vol. 97, Stockton Center for International Law, Naval War College, Rhode Island, USA.
- Bradshaw, Samantha. (2015). *Combatting Cyber Threats: CSIRTs and Fostering International Cooperation on Cybersecurity*. Global Commission on Internet Governance, Vol. 23, Chatham House.
- Buzan, Barry. (2009). *The evolution of international security studies*. Cambridge University Press, New York.
- Cardash, Sharon. (2021). *Cyber Domain Conflict in the 21st Century*. The Whitehead Journal of Diplomacy and International Relations, Vol. 82, Seton Hall University, New Jersey, USA.
- Clark, David. (2014). *At the nexus of cyber security and public policy*. The National Academies Press, Washington DC.
- Curlee, Kathleen. (2021, April). *Cyber warfare: A weapon of mass destruction*. Journal of International Relations, 23, Sigma Iota Rho National Honor Society for International Studies, Philadelphia, USA.
- De Falco, Marco. (2012). *Stuxnet Facts Report: A Technical and Strategic Analysis*. NATO Publications, Tallinn, Estonia.
- Edelman, David. (2013). *Cyber attacks in international relations* (PhD Thesis, The University of Oxford).
- Eze, Friday Ikechukwu. (2019). *Cyber as an instrument of foreign policy* (Master's Thesis, University of Manitoba, Canada).
- Gamero, Alexander. (2022). *Cyber Conflicts in International Relations: Framework and Case Studies*, in *Explorations in Cyber International Relations*, Vol. 73. Massachusetts Institute of Technology & Harvard University.
- Geers, Kenneth. (2015). *Cyber War in Perspective: Russian Aggression Against Ukraine*. NATO Publications, Tallinn, Estonia.

- Giles, Kenneth. (2017). *Cyber War in Perspective: Russian Aggression against Ukraine*. Tallinn, Australia: CCDCOE/NATO Cooperative Cyber Defense Centre of Excellence.
- Gomes, Marcelo. (2019). *Cyber Security: A Case Study of Brazil* (Master's Thesis, National Defense College, Pakistan).
- Graham, David. (2019). *Cyber threats and the law of war*. Journal of National Security Law and Policy, 87, Center on National Security, Georgetown University, Washington DC.
- Isnarti, Rika. (2016). *A Comparison of Neorealism, Liberalism, and Constructivism in Analyzing Cyber War*. Andalas Journal of International Studies, Vol. 5, Andalas University, Indonesia.
- Muller, Benedikt. (2014). *Cyberspace and international relations: Theory, prospect and challenges*. Springer, Berlin.
- Pagallo, U. (2015). *Cyber force and the role of sovereign states in informational warfare*. Philosophy & Technology, 28(3).
- Panait, I. (2015). *The hybrid war concept-arguments for and versus*. Research and Science Today, no. 3.
- Robinson, M., Jones, K., & Janicke, H. (2015). *Cyber warfare: Issues and challenges*. Computers & Security, 49.
- Schulze, Matthias. (2020). *Cyber Escalation: The Conflict Dyad USA/Iran as a Test Case*. German Institute for International and Security Affairs Publications, Berlin, December.
- Segal, Adam. (2022). *Confronting reality in cyberspace: Foreign policy for a fragmented internet*. Council on Foreign Relations, Washington DC.
- Shin, Beomchul (2011). *The cyber warfare and the right of self-defense: Legal perspectives and the case of United States*. IFAVS, 109(1).
- Tarpova, Simona. (2022). *Russia's War on Ukraine: Timeline of Cyber-Attacks*. European Parliament Research Service, European Parliament, Brussels.
- Warren, P., Kaivanto, K., & Prince, D. (2018). *Could a cyber-attack cause a systemic impact in the financial sector?* Bank of England Quarterly Bulletin, 58(4).
- Wenger, Andreas. (2022). *Cyber security politics: Socio-technological transformations and political fragmentation*. Center for Security Studies, Swiss Federal Institute of Technology, Zurich.
- Wiener, Norbert (1948). *Cybernetics: Or Control and Communication in the Animal and the Machine* (2nd ed.). Cambridge, Massachusetts: The MIT Press.