مجلة إكليل للدراسات الانسانية
التصنيف الورقي: العدد 25 /آذار/2026
المجلد(7)- العدد(1)-الجزء(2) IASJ–Iraqi Academic Scientific Journals

تأثير الحرب السيبرانية على العلاقات الدولية وآلية مجابتها وفق قواعد القانون الدولي

م . د . عصام علي حسين العبيدي
كلية القانون – جامعة الأمين

الكلمات المفتاحية: الحرب السيبرانية- المسؤولية الدولية- التجسس الرقمي- الفيروسات

الملخص:

تناولت الدراسة البحث تأثير الحرب السيبرانية على العلاقات الدولية في إطار قواعد القانون الدولي، من خلال بيان مفهومها وخصائصها وتمييزها عن الجريمة السيبرانية، وتحليل أبرز صورها كالهجمات التخريبية والتجسس الرقمي، كما تناولت انعكاساتها على موازين القوة، واستقرار النظام الدولي في ظل تصاعد الاعتماد على التكنولوجيا الرقمية، كما تثير الحرب السيبرانية إشكاليات قانونية معقدة تتعلق بإسناد الفعل غير المشروع وتحديد نطاق المسؤولية الدولية، ومدى انطباق أحكام ميثاق الأمم المتحدة وقواعد القانون الدولي العام عليها، وفي ضوء ذلك تبرز الحاجة إلى تطوير آليات قانونية ومؤسسية حديثة قادرة على تعزيز الأمن السيبراني الدولي وضبط سلوك الدول في هذا المجال.

المقدمة

أولاً: التعريف بموضوع البحث

يشهد النظام الدولي المعاصر تحولات عميقة بفعل الثورة الرقمية التي أعادت تشكيل مفاهيم القوة والسيادة والأمن وأفرزت نمطاً جديداً من الصراعات يتجاوز الحدود الجغرافية ويعمل في فضاء غير مرئي هو الفضاء السيبراني، وفي هذا السياق برزت الحرب السيبرانية بوصفها أحد أبرز التحديات التي تواجه العلاقات الدولية لما تنطوي عليه من استخدام منظم للتقنيات الرقمية بقصد الإضرار بالبنى التحتية الحيوية أو التأثير في القرارات السيادية، أو زعزعة الاستقرار السياسي والاقتصادي للدول، ولم يعد الصراع مقصوراً على المواجهة العسكرية التقليدية، بل أصبح الفيروس المعلوماتي وهجمات حجب الخدمات والتسلل إلى الشبكات الحساسة أدوات قد تعادل في أثرها استخدام القوة المسلحة.

وتتميز الحرب السيبرانية بجملة من الخصائص التي تجعلها مختلفة عن الجريمة السيبرانية من حيث طبيعة الفاعل والغاية الاستراتيجية، ومستوى التنظيم، ومدى ارتباطها بالمصالح العليا للدول فهي غالباً ما ترتبط بسياسات دولة أو بدعم مباشر أو غير مباشر منها وتسعى إلى تحقيق

أهداف سياسية أو عسكرية ضمن سياق تنافسي دولي في حين تظل الجريمة السيبرانية في إطار السلوك الإجرامي الفردي أو الجماعي ذي الطابع الربحي أو التخريبي المحدود.

وقد انعكس تصاعد هذا النمط من الصراع بصورة واضحة إذ أصبح التجسس الرقمي والتدخل في الأنظمة الحيوية والعمليات السياسية مصدر توتر دائم بين الدول وأداة لإعادة رسم موازين القوة والتحالفات كما أثار ذلك إشكاليات قانونية معقدة تتعلق بتحديد المسؤولية الدولية عن الهجمات السيبرانية خاصة في ظل صعوبة إسناد الفعل إلى دولة معينة، وتداخل أدوار الفاعلين من غير الدول ومن هنا برزت أهمية تفعيل الآليات المتاحة في إطار ميثاق الأمم المتحدة إلى جانب تطوير آليات حديثة للتعاون الدولي وبناء القدرات الدفاعية ووضع قواعد تنظيمية تكفل الحد من مخاطر هذا النوع من الحروب بما يحقق التوازن بين متطلبات الأمن واحترام قواعد القانون الدولي.

ثانياً: أهداف الدراسة

تسعى الدراسة إلى تحقيق جملة من الأهداف من أبرزها:

1. بيان الإطار المفاهيمي للحرب السيبرانية وتحديد خصائصها المميزة.
2. تحليل صور الحرب السيبرانية وأدواتها المختلفة، لاسيما الهجمات التخريبية والتجسس الرقمي.
3. تقييم مدى انطباق قواعد القانون الدولي، وخاصة أحكام ميثاق الأمم المتحدة، على العمليات السيبرانية.

ثالثاً: أهمية الدراسة

تنبع أهمية هذا الدراسة من التحول الجذري الذي أحدثته التكنولوجيا الرقمية في طبيعة الصراعات الدولية، حيث أصبحت الحرب السيبرانية تمثل أحد أخطر التهديدات التي تواجه الأمن والسلم الدوليين فالفضاء السيبراني أضحى مجالاً استراتيجياً تستخدمه الدول لتحقيق أهداف سياسية وعسكرية واقتصادية دون اللجوء إلى القوة المسلحة التقليدية الأمر الذي يفرض تحديات غير مسبوقة على قواعد القانون الدولي.

رابعاً/ إشكالية الدراسة

تكمن الإشكالية الرئيسة في السؤال التالي: ما مدى قدرة قواعد القانون الدولي على استيعاب ظاهرة الحرب السيبرانية وتنظيم آثارها في العلاقات الدولية؟.

خامساً/ منهج الدراسة

تعتمد الدراسة على **المنهج التحليلي** من خلال دراسة النصوص القانونية الدولية ذات الصلة، وتحليل مضامينها في ضوء التطورات التقنية المعاصرة، كما يستند إلى **المنهج الوصفي** لعرض خصائص الحرب السيبرانية وصورها المختلفة.

سادساً/ خطة الدراسة

نتناول في المبحث الأول **مفهوم الحرب السيبرانية**، في حين نتناول المبحث الثاني **مدى تأثير الحرب السيبرانية على العلاقات الدولية.**

المبحث الأول: مفهوم الحرب السيبرانية

أدى التطور المتسارع في تكنولوجيا المعلومات والاتصالات إلى بروز الفضاء السيبراني كساحة جديدة للصراع الدولي، مما أفرز مفاهيم حديثة تعكس التحولات في طبيعة الحروب المعاصرة، وفي مقدمتها مفهوم الحرب السيبرانية، ولم يعد النزاع يقتصر على المواجهات العسكرية التقليدية فالدول قد بدأت في التجهيز لمواجهة تحديات حروب المستقبل التي تعتمد على التخريب والتدمير من خلال الفضاء السيبراني هذا أصبح جزءاً لا يتجزأ من تكتيكات واستراتيجيات الدول المتقدمة حيث يعتبر التصدي لهذه الحروب أو القيام بها جزءاً حيوياً من استراتيجيات الدفاع للعديد من الدول، فأصبحت الحرب السيبرانية هي حرب تستغل الفضاء الإلكتروني كساحة رئيسية لتحقيق المصالح والتعبير عن القضايا، ويشمل ذلك تفاعلها مع الفضاء العام التقليدي وأصبح هذا التحول مصدر قلق للدول، حيث أصبح للحروب السيبرانية تأثير خطير على النظام العالمي[1]. **بناء على ذلك سوف نقوم بتقسيم المبحث إلى مطلبين، سوف نتحدث في المطلب الأول عن التعريف بالحرب السيبرانية، أما المطلب الثاني سوف نتحدث عن خصائص الحرب السيبرانية وتمييزه عن الجريمة السيبرانية.**

المطلب الأول :التعريف بالحرب السيبرانية

أصبحت النزاعات الدولية المعاصرة تتسم بطابع مختلط حيث تكتسب الحروب اليوم أبعاداً جديدة تتضمن استخدام أدوات الحرب السيبرانية بشكل رئيسي، حيث يتميز النطاق السيبراني في هذه الحروب بتقدم متسارع ومنافسة مكثفة، وذلك نتيجة للتنافس الشديد بين شركات البرمجيات الرائدة، والتعاون بينها وبين شركات تصنيع الأسلحة، وتظهر الهجمات السيبرانية كتحدي حقيقي لا يمكن تجاهله، حيث يمكن أن تكون مدمرة على حد سواء مشابهة لمخاطر الإرهاب والأحداث والكوارث، **بناء على ذلك سوف نقوم بتقسيم المطلب إلى فرعين، سوف نتحدث في الفرع الأول عن تعريف الحرب السيبرانية، اما الفرع الثاني سوف نتحدث عن دوافع الحرب السيبرانية.**

الفرع الأول: تعريف الحرب السيبرانية

يعد مفهوم الحرب السيبرانية (Cyber warfare) مفهوماً جديداً على صعيد النزاعات المسلحة في القرن الحادي والعشرين، فهذه الحرب تشتمل على أساليب ووسائل قتالية عالية من عمليات إلكترونية ترقى إلى مستوى النزاع المسلح أو تستخدم في سياقه، والحرب السيبرانية تهدف إلى الإخلال بتوازن المعلومات والمعرفة لصالح القوات الصديقة، لاسيما في غياب التوازن العسكري، وعليه فإن استخدام التفوق العلمي في الحرب السيبرانية سيغطي النقص في التجهيزات والقوات

العسكرية وبالتالي يمكن تحقيق النصر فيه[2]، وتعرف الحرب السيبرانية بأنها "استعمال الحواسيب كسلاح أو أداة للقيام بأعمال عنف بقصد ترعيب أو تغيير رأي مجموعة أو دولة ما، ويتم استخدامه لأغراض سياسية وأيديولوجية عن طريق استهداف البنية التحتية الحيوية كالطاقة، النقل، الاتصال والخدمات الضرورية (كالطوارئ والشرطة)"[3].

وقد جاء تعريف الحرب السيبرانية في قاموس جامعة كامبريدج بأنها "أي نشاط يستخدم الإنترنت لمهاجمة الأجهزة الإلكترونية التابعة لدولة ما بقصد الإضرار بأشياء كأنظمة الاتصالات والنقل وموارد المياه والطاقة، إن استخدام الحرب السيبرانية قد يؤدي إلى زعزعة استقرار الأنظمة المالية، نظام الهاتف أو شبكة الكهرباء، وقد يغير الأمن القومي بشكل جذري بسبب هجوم قد يأتي من أي ومكان"، وفي مناسبة أخرى عرفت بأنها:"الاستعمال الدفاعي أو الهجومي للمعلومات وأنظمتها بقصد تعريض عناصر المعلومات والعمليات القائمة على المعلومات الأنظمة المعلوماتية شبكات الإنترنت التابعة للعدو في الفضاء السيبراني للخطر[4]، وعرفتها مؤسسة راند[5] (RAND) بأنها: "الحرب السيبرانية هي حرب الدول والمنظمات الدولية ضد دول أخرى من أجل تحمير شبكات الكمبيوتر والمعلومات. وهذه الحرب تتم عن طريق الفايروسات، أحسنة طروادة والبرمجيات الخبيثة الأخرى[6].

فالحرب السيبرانية لها من الخصائص ما يميزها عن النزاعات المسلحة التقليدية سواء من حيث ماهيتها أم مضمونها، فبخلاف النزاعات المسلحة التقليدية لايمكن تحديد وقت بدء الحرب السيبرانية أو انتهائها، بل إن فاعلية الحرب السيبرانية تكمن في علم إمكانية تحديد وقت بدءها، لاسيما صعوبة التوصل ومعرفة مصدر الحرب السيبرانية تشكل عامل اختلاف آخر وذلك لعدة أسباب منها، تعدد الجهات الفاعلة في الفضاء السيبراني كالدول والمنظمات والجماعات الحكومية وغير الحكومية والإرهابيين والقراصنة وحتى الأفراد[7].

مما سبق يتبين إن الحرب السيبرانية وإن كانت تنفق كثيرا مع الهجمات السيبرانية، إلا إن ذلك لا يعني عدم وجود ما يميزهما عن بعض، فالحرب السيبرانية نوع أو جزء من الهجمات السيبرانية التي تحدث في أثناء نزاع مسلح دائر أو التي تنتج أثارا مادية أو ما يسمى بالآثار الحركية تشبه وتعادل آثار الهجمات المسلحة التقليدية، بينما الهجمات السيبرانية هي كل نشاط إلكتروني ضار بالدول الأخرى سواء كان في وقت السلم أو في أثناء نزاع مسلح دائر وسواء نتجت عنه أثار مادية جسيمة في الأرواح أم الممتلكات أو لم يؤدي إلا إلى تشويش أنظمة الكمبيوتر فيها مادام كان ذلك لأغراض أمنية وعسكرية وأحدث ارتباك في الحكومة التابعة لتلك الدولة[8].

الفرع الثاني: دوافع الحرب السيبرانية

إن فهم دوافع الحرب السيبرانية يقتضي النظر إليها ضمن سياق أوسع يرتبط بتحولات مفهوم القوة في العلاقات الدولية حيث أصبح التفوق الرقمي جزءاً من القوة الشاملة للدولة إلى جانب القوة العسكرية والاقتصادية والسياسية، فالفضاء السيبراني يوفر للدول والجهات الفاعلة

إمكانية تحقيق مكاسب استراتيجية دون تحمل المخاطر السياسية والقانونية المرتبطة بالحروب التقليدية، كما يسمح بالعمل في منطقة رمادية بين السلم والنزاع المسلح بما يخلق تحديات جديدة أمام القانون الدولي وآليات الردع التقليدية، وتتداخل دوافع الحرب السيبرانية بين أبعاد سياسية وعسكرية واقتصادية بحيث يصعب الفصل بينها بصورة مطلقة، إذ إن العمليات السيبرانية غالباً ما تخدم أهدافاً متعددة في آن واحد، ومع ذلك فإن التحليل العلمي يقتضي تصنيف هذه الدوافع ضمن محاور رئيسية لفهم طبيعتها وآليات عملها وتأثيراتها على الأمن الدولي والاستقرار العالمي[9]، وسوف نشرحها على النحو الآتي:

أولاً: الدو افع السياسية

تعد الدوافع السياسية من أبرز المحركات الأساسية للحرب السيبرانية إذ تمثل البيئة الرقمية مجالاً مثالياً لممارسة النفوذ السياسي وإعادة تشكيل موازين القوة دون الانزلاق إلى مواجهة عسكرية مباشرة، ففي ظل تعقيد العلاقات الدولية المعاصرة وتزايد تكلفة الحروب التقليدية، وجدت الدول في الفضاء السيبراني أداة فعالة لتحقيق أهدافها الاستراتيجية عبر وسائل أقل وضوحاً وأكثر مرونة.

وأحد أهم الدوافع السياسية يتمثل في السعي إلى التأثير في القرار السيادي للدول المنافسة، حيث يمكن للهجمات السيبرانية أن تستهدف المؤسسات الحكومية أو أنظمة الاتصالات أو قواعد البيانات الحساسة بهدف جمع المعلومات أو تعطيل عمل المؤسسات أو خلق حالة من الارتباك السياسي، وتتيح هذه العمليات إمكانية الضغط السياسي غير المباشر، بما يسمح للدول باستخدام القوة دون الإعلان الرسمي عن النزاع، ولايمكن إغفال أن الدوافع السياسية للحرب السيبرانية ترتبط أيضاً بالتنافس بين النماذج السياسية المختلفة، حيث تسعى بعض الدول إلى تعزيز نموذجها السياسي أو إضعاف نماذج منافسة عبر التأثير في الفضاء المعلوماتي العالمي وقد أدى هذا التنافس إلى تصاعد ما يمكن تسميته بصراعات السيادة الرقمية حيث تسعى الدول إلى فرض سيطرتها على البيانات والبنية التحتية الرقمية باعتبارها جزءاً من أمنها القومي[10].

ثانياً_ الدافع العسكري

تحتل الاعتبارات العسكرية موقعاً مركزياً في دوافع الحرب السيبرانية حيث أصبحت القدرات الرقمية جزءاً أساسياً من الاستراتيجيات الدفاعية والهجومية للدول، وقد أدى التطور التكنولوجي إلى إدماج العمليات السيبرانية ضمن العقائد العسكرية الحديثة، بحيث لم تعد مجرد نشاط استخباراتي بل أصبحت سلاحاً قائماً بذاته يمكن استخدامه لتحقيق أهداف عسكرية مباشرة، وأحد أبرز الدوافع العسكرية يتمثل في تحقيق التفوق العملياتي عبر تعطيل أنظمة الخصم قبل بدء العمليات التقليدية، فالهجمات السيبرانية يمكن أن تستهدف شبكات القيادة والسيطرة، وأنظمة الاتصالات العسكرية، وأنظمة الملاحة أو الدفاع الجوي مما يؤدي إلى

إضعاف قدرة الخصم على التنسيق والاستجابة، ويتيح هذا النوع من العمليات تحقيق عنصر المفاجأة وتقليل الخسائر البشرية[11].

كما تمثل الحرب السيبرانية وسيلة فعالة لجمع المعلومات الاستخباراتية حيث يمكن اختراق الأنظمة العسكرية أو الحكومية للحصول على بيانات حساسة حول الخطط العسكرية أو القدرات الدفاعية، وتعد هذه المعلومات عاملاً حاسماً في رسم الاستراتيجيات العسكرية وتحديد نقاط الضعف لدى الخصوم، وتسعى الدول أيضاً إلى استخدام الهجمات السيبرانية كبديل جزئي للقوة المسلحة، خاصة في الحالات التي يكون فيها استخدام القوة التقليدية محفوفاً بالمخاطر السياسية أو القانونية، فالهجمات الرقمية قد تحقق أهدافاً مشابهة للهجمات العسكرية من حيث تعطيل البنية التحتية أو إحداث خسائر اقتصادية، لكنها تقلل من احتمالات التصعيد العسكري المباشر، ومن ناحية أخرى أصبح الردع السيبراني جزءاً من الاستراتيجية العسكرية حيث تقوم الدول بتطوير قدرات هجومية ودفاعية لردع الخصوم عن تنفيذ هجمات رقمية، ويعتمد هذا الردع على القدرة على الكشف المبكر للهجمات والاستجابة السريعة، إضافة إلى امتلاك القدرة على تنفيذ عمليات مضادة[12].

المطلب الثاني :خصائص الحرب السيبرانية وتمييزه عن الجريمة السيبرانية

يشهد الفضاء الرقمي تزايداً ملحوظاً في الأنشطة العدائية التي تتنوع بين أعمال ذات طابع إجرامي بحت وأخرى ترتقي إلى مستوى الصراع السيبراني بين الدول الأمر الذي يثير إشكالية التمييز بين الحرب السيبرانية والجريمة السيبرانية رغم تشابه الوسائل التقنية المستخدمة في كل منهما، فالحرب السيبرانية ترتبط غالباً بأهداف استراتيجية وسياسية أو عسكرية تسعى إلى تحقيق تأثيرات واسعة النطاق تمس الأمن القومي أو الاستقرار الدولي، بينما تنحصر الجريمة السيبرانية في تحقيق منافع شخصية أو مالية ضمن إطار جنائي تقليدي، **لذلك سوف نقسم المطلب إلى فرعين، سوف نتحدث في الفرع الأول عن خصائص الحرب السيبرانية، اما الفرع الثاني سوف نتحدث عن تمييز الحرب السيبرانية عن الجريمة السيبرانية.**

الفرع الأول :خصائص الحرب السيبرانية

تعد الحرب السيبرانية من أبرز مظاهر التحول في طبيعة الصراعات المعاصرة إذ تعكس انتقال النزاعات من ساحات المواجهة التقليدية إلى فضاء رقمي مفتوح تتداخل فيه الأبعاد التقنية والاستراتيجية والقانونية والسياسية وقد أفرز التطور التكنولوجي المتسارع بيئة جديدة للصراع تقوم على استغلال الشبكات المعلوماتية والبنى التحتية الرقمية لتحقيق أهداف قد تعجز الوسائل العسكرية التقليدية عن تحقيقها بالكلفة نفسها أو بالدرجة ذاتها من المرونة، ولعل أهم ما يميز الحرب السيبرانية هو تعدد خصائصها التي تجعلها تختلف جوهرياً عن أنماط الحروب التقليدية سواء من حيث طبيعة الفاعلين أو أدوات الصراع أو نطاق التأثير أو آليات الردع والمسؤولية القانونية[13]، ومن أبرز هذه الخصائص ما يلي:

1_ غياب ساحة القتال التقليدية

من أبرز خصائص الحرب السيبرانية أنها تدور في فضاء غير مادي حيث يتم تنفيذ العمليات عبر شبكات رقمية دون الحاجة إلى وجود مادي مباشر في أرض المعركة، فالفضاء السيبراني لايخضع للحدود الجغرافية التقليدية، مما يسمح بتنفيذ الهجمات عن بعد وفي أي وقت، ويؤدي ذلك إلى صعوبة تحديد مسرح العمليات بالمعنى التقليدي للحرب، وتمنح هذه الطبيعة الافتراضية الجهات الفاعلة قدرة كبيرة على المناورة والاختفاء، إذ يمكن تنفيذ الهجوم من دولة معينة بينما يتم توجيه أثره نحو دولة أخرى عبر عدة مسارات رقمية معقدة، كما أن غياب الحدود الجغرافية الواضحة يخلق تحديات أمام تطبيق قواعد القانون الدولي التقليدي التي بنيت على مفهوم الإقليم والسيادة المكانية، فالهجوم السيبراني قد يمر عبر خوادم متعددة في دول مختلفة مما يجعل تحديد الاختصاص القانوني أو المسؤولية الدولية أمراً بالغ التعقيد[14].

ثانياً_ صعوبة تحديد مصدر الهجوم والفاعل

تعد صعوبة تحديد الجهة المسؤولة عن الهجمات السيبرانية من أهم خصائص الحرب السيبرانية، إذ يمكن للمهاجمين استخدام تقنيات متقدمة لإخفاء هويتهم مثل توجيه الهجمات عبر شبكات وسيطة أو استخدام أدوات تشفير متطورة، ويؤدي هذا الغموض إلى خلق ما يسمى بمنطقة الظل أو المنطقة الرمادية بين السلم والحرب، حيث تستطيع الدول تنفيذ عمليات هجومية دون الاعتراف بها رسمياً، وتؤثر هذه الخاصية في مفهوم الردع، إذ يصبح من الصعب الرد على هجوم ما دون التأكد من هوية المهاجم مما قد يؤدي إلى تصعيد غير محسوب أو إلى الامتناع عن الرد خشية الخطأ في التقدير، كما تسمح هذه الخاصية باستخدام وكلاء أو جهات غير حكومية لتنفيذ الهجمات، الأمر الذي يزيد من تعقيد المشهد الأمني[15].

ثالثاً_ انخفاض الكلفة مقارنة بالحروب التقليدية

تتميز الحرب السيبرانية بانخفاض كلفتها الاقتصادية والعسكرية مقارنة بالحروب التقليدية التي تتطلب موارد بشرية ومادية ضخمة، فالهجمات السيبرانية قد تنفذ بواسطة فرق صغيرة من الخبراء التقنيين باستخدام أدوات رقمية متاحة نسبياً، ما يجعلها وسيلة جذابة للدول ذات القدرات العسكرية المحدودة أو حتى للجهات غير الحكومية وقد أدى انخفاض الكلفة إلى انتشار واسع للهجمات السيبرانية، إذ أصبحت وسيلة فعالة لتحقيق تأثيرات استراتيجية دون الحاجة إلى استثمارات ضخمة في الأسلحة التقليدية، كما أن القدرة على إلحاق أضرار كبيرة بالبنية التحتية الحيوية للخصم باستخدام وسائل رقمية فقط تعزز من جاذبية هذا النوع من الصراع[16].

رابعاً_ السرعة الفائقة في التنفيذ والتأثير

تتميز العمليات السيبرانية بسرعة التنفيذ والقدرة على إحداث تأثيرات فورية، حيث يمكن للهجوم أن ينتشر خلال ثوان عبر الشبكات الرقمية، مما يجعل الاستجابة الدفاعية أكثر

تعقيداً، فالأنظمة الحيوية مثل شبكات الطاقة أو الاتصالات قد تتعرض للتعطيل المفاجئ نتيجة هجوم واحد، وهو ما قد يؤدي إلى اضطرابات واسعة النطاق، وتؤثر هذه السرعة أيضاً في عملية اتخاذ القرار السياسي والعسكري، إذ يتعين على الدول الاستجابة بسرعة كبيرة دون توفر الوقت الكافي للتحقق الكامل من طبيعة الهجوم أو مصدره، مما يزيد من مخاطر التصعيد غير المقصود[17].

خامساً_ الطابع غير الدموي المباشر

من الخصائص الجوهرية للحرب السيبرانية تداخل الأهداف المدنية والعسكرية حيث تعتمد البنية التحتية العسكرية الحديثة بشكل كبير على الشبكات المدنية، مثل الإنترنت وأنظمة الاتصالات التجارية، وهذا التداخل يجعل من الصعب الفصل بين الأهداف المشروعة عسكرياً والأهداف المدنية التي يحميها القانون الدولي الإنساني، كما أن الهجمات السيبرانية قد تستهدف قطاعات مدنية حيوية مثل الطاقة والمياه والنقل، بهدف تحقيق تأثيرات استراتيجية غير مباشرة على القدرات العسكرية أو على الاستقرار الداخلي للدولة ويثير هذا التداخل تحديات قانونية تتعلق بمبدأ التمييز والتناسب في النزاعات المسلحة[18].

وتتيح الحرب السيبرانية للدول إمكانية إنكار مسؤوليتها عن الهجمات، مما يجعلها أداة مثالية لإدارة الصراعات منخفضة الحدة، فالهجمات الرقمية قد تنفذ دون إعلان رسمي للحرب الأمر الذي يسمح للدول بممارسة الضغط الاستراتيجي دون تجاوز العتبة القانونية للنزاع المسلح، ويؤدي ذلك إلى ظهور نمط جديد من الصراعات المستمرة منخفضة الشدة، حيث تتبادل الدول الهجمات السيبرانية بشكل غير معلن، في إطار منافسة استراتيجية طويلة الأمد وهذا الواقع يعكس تحولاً في مفهوم الحرب ذاته حيث لم يعد النزاع يبدأ بإعلان رسمي أو ينتهي باتفاقية سلام واضحة.

الفرع الثاني:تمييز الحرب السيبرانية عن الجريمة السيبرانية

أدى التطور المتسارع في التكنولوجيا الرقمية وانتشار الاعتماد على الشبكات المعلوماتية إلى ظهور أنماط جديدة من الأنشطة العدائية في الفضاء السيبراني، مما أوجد تحديات مفاهيمية وقانونية تتعلق بتمييز الحرب السيبرانية عن الجريمة السيبرانية، خاصة في ظل تشابه الأدوات التقنية المستخدمة في كلا المجالين، فالهجمات السيبرانية قد تتخذ أشكالاً متعددة تتراوح بين أنشطة إجرامية تقليدية تستهدف تحقيق مكاسب مالية، وعمليات استراتيجية واسعة النطاق ترمي إلى تحقيق أهداف سياسية أو عسكرية أو اقتصادية للدول، ويعد هذا التمييز ذا أهمية خاصة من الناحية القانونية والاستراتيجية لأنه يحدد الإطار القانوني الواجب التطبيق سواء كان قانوناً جنائياً وطنياً أو قواعد القانون الدولي الإنساني وقانون النزاعات المسلحة، وعلى الرغم من وجود تداخل بين الحرب السيبرانية والجريمة السيبرانية من حيث الوسائل التقنية

المستخدمة إلا أن الاختلافات بينهما تظهر بوضوح عند تحليل طبيعة الفاعلين، والأهداف[19]، والنتائج القانونية المترتبة على كل منهما، ومن أبرز الاختلافات:

1_ الاختلاف في طبيعة الفاعلين والجهات المنفذة

من أبرز معايير التمييز بين الحرب السيبرانية والجريمة السيبرانية طبيعة الجهات الفاعلة التي تقف وراء الهجمات، فالحرب السيبرانية ترتبط في الغالب بالدول أو الجهات المرتبطة بها سواء بشكل مباشر أو غير مباشر حيث تستخدم كأداة ضمن الاستراتيجيات الوطنية لتحقيق أهداف سياسية أو عسكرية أو اقتصادية، وقد تتولى تنفيذ العمليات وحدات عسكرية متخصصة في الفضاء السيبراني أو أجهزة استخباراتية تعمل ضمن إطار مؤسسي رسمي، في المقابل ترتبط الجريمة السيبرانية غالباً بأفراد أو جماعات إجرامية منظمة تسعى لتحقيق مكاسب شخصية أو مالية، مثل سرقة البيانات أو الاحتيال الإلكتروني أو هجمات الفدية الرقمية. وتخضع هذه الأنشطة عادة للقانون الجنائي الوطني أو الاتفاقيات الدولية المتعلقة بمكافحة الجرائم الإلكترونية[20].

2_ الاختلاف في الأهداف والدو افع

تختلف دوافع الحرب السيبرانية عن الجريمة السيبرانية بشكل جوهري، فالحرب السيبرانية تسعى إلى تحقيق أهداف استراتيجية تتعلق بالأمن القومي أو النفوذ السياسي أو التفوق العسكري، مثل تعطيل البنية التحتية الحيوية للخصم أو جمع معلومات استخباراتية حساسة أو التأثير في العمليات السياسية للدول الأخرى، أما الجريمة السيبرانية فتهدف غالباً إلى تحقيق مكاسب مالية أو شخصية، مثل ابتزاز الضحايا أو سرقة الحسابات المصرفية أو الاتجار غير المشروع بالبيانات، وعلى الرغم من أن بعض الهجمات الإجرامية قد تكون واسعة النطاق، إلا أنها تظل في إطار تحقيق الربح وليس تغيير موازين القوى السياسية أو العسكرية[21].

3_ القانون المنظم

الحرب السيبرانية قد تخضع لقواعد القانون الدولي العام، بما في ذلك ميثاق الأمم المتحدة وقواعد استخدام القوة، إضافة إلى القانون الدولي الإنساني إذا وصلت العمليات إلى مستوى النزاع المسلح، ويثير ذلك تساؤلات حول مشروعية الرد العسكري أو تطبيق حق الدفاع الشرعي، أما الجريمة السيبرانية فتخضع للقوانين الجنائية الوطنية والاتفاقيات الدولية المتعلقة بمكافحة الجرائم الإلكترونية، مثل اتفاقية بودابست بشأن الجرائم المعلوماتية، ويكون الهدف من تطبيق هذه القوانين هو محاسبة الأفراد المسؤولين ومعاقبتهم وفق الإجراءات الجنائية[22].

كما تتسم الحرب السيبرانية بدرجة عالية من التنظيم والتخطيط الاستراتيجي، حيث يتم تصميم العمليات ضمن رؤية طويلة الأمد تتكامل مع السياسات الخارجية والعسكرية للدولة، وتشمل هذه العمليات مراحل متعددة مثل الاستطلاع الرقمي، واختبار الثغرات، وزرع البرمجيات الخبيثة، وانتظار اللحظة المناسبة لتنفيذ الهجو، في المقابل قد تكون الجريمة السيبرانية أقل

تنظيماً، خاصة عندما تنفذ من قبل أفراد أو مجموعات صغيرة. ومع ذلك، فإن بعض الشبكات الإجرامية الحديثة أصبحت تمتلك مستويات تنظيمية متقدمة، مما يزيد من صعوبة التمييز بينها وبين العمليات المدعومة من الدول[23].

المبحث الثاني:مدى تأثير الحرب السيبرانية على العلاقات الدولية

لقد بات الفضاء السيبراني ميداناً خامساً للصراع إلى جانب البر والبحر والجو والفضاء الخارجي وهو ميدان يتسم بخصائص مغايرة للميادين التقليدية من حيث صعوبة تحديد مصدر الهجوم وإمكانية الإنكار وانخفاض الكلفة المادية واتساع نطاق التأثير هذه الخصائص جعلت الحرب السيبرانية أداة جذابة للدول لتحقيق أهداف سياسية أو اقتصادية أو عسكرية دون الدخول في مواجهة مسلحة مباشرة، الأمر الذي انعكس بصورة مباشرة على طبيعة العلاقات الدولية، سواء من حيث أنماط التحالف أو مفاهيم الردع أو قواعد المسؤولية الدولية. **بناء على ذلك سوف نقوم بتقسيم المبحث إلى مطلبين، سوف نتحدث في المطلب الأول عن صور الحرب السيبرانية، أما المطلب الثاني سوف نتحدث عن حدود المسؤولية الدولية عن الحرب السيبرانية واليات مجابتها.**

المطلب الأول: صور الحرب السيبرانية

أفرز التطور التقني المتسارع أنماطاً متعددة للحرب السيبرانية تجاوزت الإطار التقليدي للصراع المسلح، لتشمل صوراً متنوعة من الهجمات الرقمية التي تستهدف البنى التحتية الحيوية، والأنظمة العسكرية، والمؤسسات المالية والبيانات الاستراتيجية للدول، وتتنوع هذه الصور بين التجسس الإلكتروني والهجمات التخريبية وحملات التضليل الإعلامي، وصولاً إلى شل المرافق العامة بما يجعل الفضاء السيبراني ساحة صراع مفتوحة ذات تأثير عابر للحدود، **بناء على ذلك سوف نقوم بتقسيم المطلب إلى فرعين، سوف نتحدث في الفرع الأول عن الفيروسات وهجمات حجب الخدمات، أما الفرع الثاني سوف نتحدث عن التجسس الرقمي.**

الفرع الأول: الفيروسات وهجمات حجب الخدمات

يعد استخدام الفيروسات الإلكترونية وهجمات حجب الخدمات من أبرز الأدوات التي تجسد الطبيعة الهجومية للحرب السيبرانية، إذ تمثل هذه الوسائل انتقالاً واضحاً من مجرد الاختراق إلى إحداث ضرر فعلي ومباشر بالبنى التحتية الرقمية، وما يرتبط بها من مرافق حيوية تمس الأمن الوطني والاستقرار الاقتصادي والاجتماعي للدول، فالحرب السيبرانية بوصفها شكلاً حديثاً من أشكال النزاع تعتمد على أدوات تقنية منخفضة الكلفة نسبياً مقارنة بالأسلحة التقليدية لكنها قادرة على إحداث آثار قد تعادل في خطورتها نتائج العمليات العسكرية المباشرة[24].

أولاً_ الفيروسات كأداة هجومية في الفضاء السيبراني

تمثل الفيروسات أحد أقدم وأخطر أشكال البرمجيات الخبيثة التي استخدمت في سياق الصراعات السيبرانية، والفيروس في جوهره برنامج يصمم للتسلل إلى نظام معلوماتي دون علم المستخدم ثم يتكاثر أو ينفذ أوامر مبرمجة مسبقاً قد تشمل تدمير البيانات أو تعطيل الأنظمة أو التجسس أو فتح أبواب خلفية تتيح السيطرة الكاملة على الشبكة المستهدفة غير أن التطور التقني أفرز أنماطاً أكثر تعقيداً من الفيروسات مثل الديدان الإلكترونية (Worms) وأحصنة طروادة (Trojans) وبرمجيات الفدية (Ransomware) التي أصبحت أدوات رئيسية في النزاعات السيبرانية المعاصرة، وقد شكل هجوم Stuxnet نقطة تحول مفصلية في إدراك المجتمع الدولي لإمكانات الفيروسات كسلاح سيبراني استراتيجي[25].

وتكمن خطورة الفيروسات في سياق الحرب السيبرانية في عدة عناصر مترابطة أولها قدرتها على التخفي لفترات طويلة داخل الأنظمة المستهدفة ما يسمح بجمع معلومات حساسة أو انتظار لحظة مناسبة لتنفيذ الهجوم ثانيها صعوبة إسناد الهجوم إلى جهة معينة بسبب إمكانية تمرير الفيروس عبر شبكات متعددة أو استخدام خوادم في دول مختلفة وهو ما يعقد مسألة المسؤولية الدولية، ثالثها إمكانية توجيه الفيروسات لاستهداف قطاعات حيوية مثل الطاقة والمياه، والنقل والمصارف والمستشفيات بما يخلق حالة من الفوضى المجتمعية تتجاوز الأثر التقني إلى بعد سياسي وأمني واسع، كما أن برمجيات الفدية تمثل وجهاً آخر من أوجه استخدام الفيروسات في الحرب السيبرانية، إذ تستخدم لتعطيل مؤسسات حكومية أو بنوك أو مرافق صحية عبر تشفير بياناتها والمطالبة بفدية مالية وقد شهدت السنوات الأخيرة هجمات واسعة النطاق استهدفت مؤسسات عامة في دول متعددة وأدت إلى تعطيل الخدمات الحيوية لساعات أو أيام بل أحياناً لأسابيع، وفي سياق النزاعات المسلحة يمكن توظيف هذه الهجمات لشل قدرة الدولة على إدارة مواردها أو تقديم الخدمات الأساسية لمواطنيها[26].

ثانياً_ هجمات حجب الخدمات (DoS و DDoS) كأداة لشلّ البنى التحتية الرقمية

تمثل هجمات حجب الخدمات أحد أكثر أشكال الهجوم السيبراني انتشاراً وتأثيراً في سياق الحرب الرقمية ويقصد بها استهداف خادم أو شبكة أو موقع إلكتروني عبر إغراقه بعدد هائل من الطلبات أو البيانات بحيث يصبح غير قادر على الاستجابة للمستخدمين الشرعيين، وعندما يتم تنفيذ الهجوم عبر شبكة واسعة من الأجهزة المخترقة حول العالم، يعرف باسم هجوم حجب الخدمة الموزع (DDoS)[27] ، تعتمد هذه الهجمات على ما يعرف بشبكات "البوت نت" (Botnets) وهي مجموعة من الأجهزة المصابة ببرمجيات خبيثة، يتم التحكم بها عن بعد لإطلاق الهجوم في وقت واحد، وتكمن خطورة هذه الآلية في أن الأجهزة المستخدمة قد تكون حواسيب شخصية أو كاميرات مراقبة أو أجهزة إنترنت الأشياء ما يجعل اكتشاف مصدر الهجوم أمراً بالغ الصعوبة، إن هجمات حجب الخدمات، وإن كانت لاتحدث دماراً مادياً مباشراً في الغالب، إلا أنها قادرة على

إحداث أثر نفسي وسياسي عميق من خلال إظهار عجز الدولة عن حماية بنيتها الرقمية، كما يمكن استخدامها تمهيداً لهجمات أكثر تعقيداً، إذ يمكن أن تشكل وسيلة لتشتيت الانتباه بينما يجري تنفيذ اختراقات أخرى في الخلفية[28].

الفرع الثاني: التجسس الرقمي

يمثل التجسس الرقمي أحد أكثر صور الحرب السيبرانية تعقيداً وخطورة، لكونه يجمع بين الطابع السري التقليدي لعمليات الاستخبارات وبين الأدوات التقنية الحديثة التي تتيح اختراق الحدود الجغرافية والسيادية دون الحاجة إلى وجود مادي داخل إقليم الدولة المستهدفة، وإذا كانت الحروب التقليدية تعتمد على القوة الظاهرة، فإن التجسس الرقمي يعتمد على الخفاء وعلى القدرة على التسلل غير المرئي إلى شبكات الدولة ومؤسساتها الحيوية بغية الحصول على معلومات استراتيجية تمكن الطرف المهاجم من تحقيق تفوق سياسي أو عسكري أو اقتصادي[29].

ويقصد بالتجسس الرقمي استخدام وسائل تقنية لاختراق أنظمة المعلومات أو اعتراض الاتصالات أو زرع برمجيات خبيثة بهدف جمع معلومات سرية أو حساسة دون علم الجهة المستهدفة، ويتميز هذا النمط من التجسس بعدة خصائص تجعله أداة فعالة في الحرب السيبرانية أولى هذه الخصائص هي الطابع العابر للحدود، إذ يمكن تنفيذ العملية من دولة إلى أخرى عبر شبكة الإنترنت دون المرور بإجراءات مادية أو لوجستية معقدة، وثانيها، صعوبة الإسناد حيث يمكن للجهة المنفذة أن تستخدم خوادم وسيطة أو شبكات افتراضية أو مجموعات قرصنة كغطاء لإخفاء هويتها الحقيقية، وثالثها القدرة على الاستمرارية، إذ قد يبقى المخترق داخل النظام المستهدف لفترة طويلة دون اكتشاف، جامعاً المعلومات بشكل تدريجي، ومن أبرز الأمثلة التي كشفت عن حجم هذا النمط من التجسس ما أعلنه المتعاقد السابق مع وكالة الأمن القومي الأمريكية Edward Snowden[30] عام 2013، حين كشف عن برامج مراقبة واسعة النطاق تنفذها National Security Agency، تضمنت جمع بيانات الاتصالات من داخل وخارج United States وقد أثارت تلك التسريبات نقاشاً عالمياً حول حدود الأمن القومي وحقوق الخصوصية، وأظهرت أن التجسس الرقمي لم يعد موجهاً فقط إلى الخصوم التقليديين، بل يشمل نطاقاً واسعاً من الأفراد والمؤسسات[31].

وتتعدد الأدوات المستخدمة في التجسس الرقمي، وتتطور باستمرار تبعاً للتقدم التكنولوجي، ومن أهمها برمجيات التجسس (Spyware) التي تزرع في أجهزة الحاسوب أو الهواتف الذكية لجمع البيانات وإرسالها إلى الجهة المهاجمة، وقد كشفت تقارير دولية عن استخدام برنامج " "Pegasus الذي طورته شركة NSO Group، لاستهداف صحفيين وناشطين ومسؤولين في دول متعددة، مما أبرز البعد السياسي لهذا النوع من العمليات، كما يستخدم أسلوب "التصيد الاحتيالي" (Phishing)لإقناع الضحايا بالكشف عن بياناتهم السرية عبر رسائل بريد إلكتروني

مزيفة أو مواقع وهمية تحاكي المواقع الرسمية ويعد هذا الأسلوب من أكثر الوسائل انتشاراً نظراً لاعتماده على العامل البشري بوصفه الحلقة الأضعف في منظومة الأمن السيبراني، كذلك تلجأ بعض الجهات إلى استغلال الثغرات في البرمجيات وأنظمة التشغيل للوصول إلى الشبكات المستهدفة دون الحاجة إلى تفاعل المستخدم[32].

ولايقتصر أثر التجسس الرقمي على جمع المعلومات فحسب، بل يمتد إلى إعادة تشكيل موازين القوى بين الدول، فالحصول على معلومات عسكرية سرية قد يمنح الدولة المهاجمة قدرة على تطوير استراتيجيات دفاعية أو هجومية أكثر دقة، كما أن سرقة الأسرار الصناعية أو براءات الاختراع قد تؤثر في التنافس الاقتصادي العالمي، وتختصر سنوات من البحث والتطوير[33].

وفي السياق العسكري قد يؤدي التجسس الرقمي إلى كشف مواقع القواعد العسكرية أو أنظمة الدفاع الجوي أو خطط التحرك ما يجعل الدولة المستهدفة في وضع هش أمام أي مواجهة محتملة، أما في المجال السياسي، فقد يستخدم التجسس للحصول على معلومات تستغل في الضغط الدبلوماسي أو في التأثير على العمليات الانتخابية وهو ما أثير في تقارير حول تدخلات سيبرانية في انتخابات عدة دول، كما أن التجسس الرقمي قد يكون تمهيداً لهجمات تخريبية لاحقة إذ إن اختراق الشبكة وجمع المعلومات عنها يعد خطوة أولى لفهم بنيتها وتحديد نقاط ضعفها تمهيداً لتعطيلها أو تدميرها عند الحاجة ومن ثم فإن التجسس لاينفصل عن بقية صور الحرب السيبرانية بل يعد في كثير من الأحيان المرحلة التحضيرية لها ويتجاوز التجسس الرقمي الإطار القانوني ليطرح تساؤلات أخلاقية عميقة حول حدود المراقبة المشروعة، ففي ظل التطور التكنولوجي أصبحت القدرة على جمع البيانات وتحليلها شبه غير محدودة ما يهدد بتحويل المجتمعات إلى فضاءات مراقبة دائمة كما أن استخدام هذه الأدوات في سياق النزاعات السياسية قد يقوض الثقة بين الدول، ويؤدي إلى سباق تسلح رقمي يفاقم التوتر الدولي[34].

إن التجسس الرقمي يمثل إحدى الركائز الأساسية للحرب السيبرانية المعاصرة، لكونه يجمع بين الطابع الاستخباراتي التقليدي والقدرات التقنية الحديثة التي تتيح اختراق الأنظمة وجمع المعلومات على نطاق غير مسبوق، وتكمن خطورته في طبيعته الخفية، واتساع نطاق تأثيره ليشمل المجالات العسكرية والسياسية والاقتصادية والاجتماعية كما إن غياب إطار قانوني دولي واضح ينظم هذا السلوك يزيد من تعقيد المشهد، ويجعل من الفضاء السيبراني ساحة مفتوحة لصراعات غير مرئية قد تسبق أو ترافق النزاعات المسلحة التقليدية، ومن ثم فإن فهم التجسس الرقمي وتحليل أبعاده يمثل خطوة أساسية في بناء تصور قانوني وأمني متكامل لمواجهة تحديات الحرب السيبرانية في العصر الحديث[35].

المطلب الثاني: حدود المسؤولية الدولية عن الحرب السيبرانية واليات مجابتها

أفرزت الحرب السيبرانية تحديات قانونية معقدة تتصل بتحديد نطاق المسؤولية الدولية عن الأفعال الضارة التي تقع عبر الفضاء الرقمي ولاسيما في ظل صعوبة إسناد الهجمات إلى دولة

بعينها وتداخل أدوار الفاعلين من غير الدول، وقد أثار ذلك تساؤلات جوهرية حول مدى انطباق قواعد القانون الدولي العام وميثاق الأمم المتحدة وقواعد المسؤولية الدولية عن الأفعال غير المشروعة على العمليات السيبرانية كما برزت الحاجة إلى تطوير آليات فعالة لمجابهة هذه التهديدات سواء عبر التعاون الدولي، أو بناء القدرات الدفاعية أو وضع أطر تنظيمية جديدة تعزز الأمن والاستقرار في الفضاء السيبراني، **بناء على ذلك سوف نقوم بتقسيم المطلب إلى فرعين، سوف نتحدث في الفرع الأول عن حدود المسؤولية الدولية وفق الآليات المتاحة في ميثاق الأمم المتحدة، أما الفرع الثاني سوف نتحدث عن الآليات الحديثة في مواجهة الحرب السيبرانية.**

الفرع الأول: حدود المسؤولية الدولية وفق الآليات المتاحة في ميثاق الأمم المتحدة

أفرز التحول الرقمي العميق في بنية الدولة والمجتمع تحديات غير مسبوقة أمام قواعد القانون الدولي العام، ولاسيما في ما يتعلق بتحديد نطاق المسؤولية الدولية عن الأفعال غير المشروعة التي ترتكب عبر الفضاء السيبراني، فالحرب السيبرانية بما تنطوي عليه من أدوات غير تقليدية وآثار قد تكون غير مادية أو غير فورية، تضع منظومة ميثاق الأمم المتحدة أمام اختبار حقيقي لقدرتها على استيعاب هذا النمط الجديد من النزاعات[36]، ويغدو السؤال الجوهري هو: إلى أي مدى تسمح الآليات المتاحة في الميثاق بتحميل الدولة المسؤولية عن هجوم سيبراني؟ وما حدود هذه المسؤولية في ظل صعوبة الإسناد، وتعدد الفاعلين، وطبيعة الأثر الناجم عن الهجوم؟

أولاً_ مبدأ حظر استخدام القوة وتطبيقه على الهجمات السيبرانية

تنص المادة (4/2) من الميثاق على حظر التهديد باستعمال القوة أو استخدامها ضد سلامة الأراضي أو الاستقلال السياسي لأي دولة[37]، ويثور التساؤل حول ما إذا كانت الهجمات السيبرانية تندرج ضمن مفهوم "القوة" الوارد في النص.

في الفقه الدولي المعاصر اتجه جانب معتبر إلى اعتبار أن الهجوم السيبراني قد يرقى إلى مستوى استخدام القوة إذا ترتب عليه أثر يعادل في خطورته الأثر الناجم عن استخدام القوة العسكرية التقليدية، كتعطيل شبكة كهرباء وطنية أو إحداث انفجار في منشأة صناعية، أو شلّ أنظمة دفاعية حيوية، فالعبرة ليست بوسيلة الهجوم وإنما بنتيجته وآثاره الواقعية، وعلى هذا الأساس فإن هجوماً سيبرانياً يؤدي إلى تدمير بنية تحتية حيوية أو إلى خسائر بشرية يمكن أن يُصنف باعتباره استخداماً للقوة المحظورة دولياًن أما إذا اقتصر الهجوم على اختراق موقع إلكتروني أو تسريب بيانات دون إحداث ضرر مادي جسيم، فقد يعد عملاً غير مشروع أو تدخلاً في الشؤون الداخلية، لكنه لايرقى بالضرورة إلى مستوى استخدام القوة غير أن تحديد الحد الفاصل بين الفعل غير المشروع واستخدام القوة يظل مسألة تقديرية تفتقر إلى معيار دولي ملزم وهذا الغموض يمثل أحد أبرز حدود المسؤولية الدولية في المجال السيبراني، إذ قد تدفع الدولة

المسؤولة بعدم انطباق وصف "القوة" على سلوكها، خاصة إذا كان الضرر غير مباشر أو تدريجياً[38].

ثانياً_ حق الدفاع الشرعي في مواجهة الهجمات السيبرانية

ينص ميثاق الأمم المتحدة على الحق الطبيعي للدول في الدفاع عن نفسها إذا وقع هجوم مسلح عليها[39]، وهنا يبرز إشكال مزدوج: متى يعد الهجوم السيبراني "هجوماً مسلحاً"؟ وما نطاق الرد المشروع في هذه الحالة؟ إذا أدى الهجوم السيبراني إلى أضرار جسيمة تماثل آثار القصف أو العمليات العسكرية التقليدية فإن الاتجاه الغالب في الفقه يرى إمكانية اعتباره هجوماً مسلحاً يجيز ممارسة حق الدفاع الشرعي شريطة احترام مبدأي الضرورة والتناسب، أما الهجمات ذات الطابع التجسسي أو التعطيلي المحدود، فقد لاتستوفي هذا الشرط، وتكمن الصعوبة في أن الهجوم السيبراني قد يكون خفياً أو متدرجاً ما يجعل تحديد لحظة "وقوع الهجوم المسلح" أمراً معقداً، كما أن الرد قد لا يكون بالضرورة سيبرانياً، إذ قد تلجأ الدولة إلى وسائل تقليدية، وهو ما يثير تساؤلات حول مدى مشروعية استخدام القوة العسكرية رداً على هجوم رقمي[40].

ثالثاً_ مسؤولية الدولة عن الأفعال السيبرانية وإشكالية الإسناد

يخول الفصل السابع من الميثاق United Nations Security Council سلطة اتخاذ تدابير في حال وجود تهديد للسلم أو إخلال به أو وقوع عدوان ويمكن نظرياً اعتبار الهجمات السيبرانية واسعة النطاق التي تهدد الاستقرار الدولي ضمن هذا الإطار غير أن تفعيل هذه الآلية يصطدم باعتبارات سياسية ولاسيما حق النقض (الفيتو) الذي تتمتع به الدول الدائمة العضوية، فإذا كانت الدولة المتهمة بالهجوم عضواً دائماً فقد تعرقل أي قرار يدينها أو يفرض عليها تدابير عقابية، وهنا تتجلى حدود فعالية الميثاق في ضبط النزاعات السيبرانية إذ يبقى التطبيق العملي رهين التوازنات السياسية، كما أن توصيف الهجوم السيبراني كتهديد للسلم يتطلب توافقاً دولياً على خطورته، وهو أمر غير متحقق دائماً، بسبب اختلاف وجهات النظر حول طبيعة هذه الهجمات وحدودها[41].

وترتكز المسؤولية الدولية وفق قواعد القانون الدولي العرفي على توافر فعل غير مشروع منسوب إلى دولة وحدوث ضرر وقيام علاقة سببية بينهما، وفي المجال السيبراني تمثل مسألة الإسناد التحدي الأكبر، فالهجوم قد يُنفذ عبر خوادم في دول متعددة، أو بواسطة جماعات غير حكومية أو من خلال أفراد يعملون بشكل غير رسمي ولكي تحمل الدولة المسؤولية يجب إثبات أن الفعل نُفذ من قبل أجهزتها الرسمية أو من قبل أشخاص أو كيانات تعمل بتوجيهها أو تحت سيطرتها الفعلية غير أن الطبيعة التقنية للهجمات السيبرانية تتيح للدولة إنكار صلتها بها أو الادعاء بأن الفاعل مجموعة مستقلة وقد اتجهت بعض الدول إلى اعتماد معايير مرنة للإسناد، تستند إلى القرائن التقنية والسياق السياسي، إلا إن غياب هيئة قضائية دولية مختصة بالنزاعات السيبرانية يجعل هذه المعايير غير موحدة[42].

وتتحدد حدود المسؤولية الدولية عن الحرب السيبرانية في ضوء قدرة قواعد ميثاق الأمم المتحدة على استيعاب هذا النمط الجديد من الصراع، فبينما يوفر الميثاق مبادئ عامة قابلة للتطبيق، كحظر استخدام القوة وحق الدفاع الشرعي ومبدأ عدم التدخل فإن التطبيق العملي يواجه تحديات تتعلق بتوصيف الفعل وإسناده، وإثبات الضرر وتفعيل آليات الرد الجماعي ومن ثم فإن المسؤولية الدولية في المجال السيبراني تظل رهينة تطوير اجتهاد دولي متراكم يسعى إلى ملاءمة النصوص التقليدية مع واقع رقمي متغير، بما يحقق التوازن بين حماية السيادة وضمان السلم والأمن الدوليين[43].

الفرع الثاني: الآليات الحديثة في مواجهة الحرب السيبرانية

يعد الفضاء السيبراني أحد أهم ميادين التفاعل الدولي ليس فقط بوصفه مجالاً للتواصل وتبادل المعرفة، وإنما باعتباره ساحة صراع تتقاطع فيها الاعتبارات الأمنية والعسكرية والاقتصادية والسياسية ومع تصاعد وتيرة الهجمات السيبرانية وتنوع أدواتها برزت الحاجة إلى تطوير آليات حديثة ومتعددة المستويات لمواجهة هذا النمط المعقد من التهديدات ولم تعد المقاربة الأمنية التقليدية كافية بل بات التصدي للحرب السيبرانية يتطلب تكاملاً بين التدابير التقنية والأطر القانونية والاستراتيجيات المؤسسية، وآليات التعاون الدولي، إضافة إلى بناء قدرات بشرية متخصصة[44].

أولاً_ تعزيز منظومات الدفاع السيبراني

تشكل الآليات التقنية خط الدفاع الأول في مواجهة الهجمات السيبرانية وتتمثل هذه الآليات في تطوير أنظمة متقدمة لرصد الاختراقات، وتحليل البرمجيات الخبيثة، والاستجابة الفورية للحوادث الرقمية وقد اعتمدت العديد من الدول استراتيجيات وطنية للأمن السيبراني ترتكز على إنشاء مراكز متخصصة لرصد التهديدات تعرف عادة بفرق الاستجابة لطوارئ الحاسوب (CERT) تتولى متابعة الهجمات وتحليلها والتنسيق بين المؤسسات العامة والخاصة[45].

ومن أبرز التطورات التقنية في هذا المجال توظيف تقنيات الذكاء الاصطناعي والتعلم الآلي لتحليل كميات ضخمة من البيانات ورصد الأنماط غير الطبيعية في حركة الشبكات بما يسمح بالكشف المبكر عن الهجمات قبل أن تتفاقم آثارها كما أدخلت تقنيات التشفير المتقدم لحماية البيانات الحساسة، خاصة في القطاعات الحيوية مثل المصارف والطاقة والدفاع، وتتضمن الآليات التقنية الحديثة كذلك اعتماد مفهوم "الأمن السيبراني الاستباقي"، الذي يقوم على اختبار الأنظمة بانتظام عبر محاكاة هجمات فعلية (اختبارات الاختراق) بهدف اكتشاف الثغرات قبل استغلالها من قبل جهات معادية، كما اتجهت بعض الدول إلى تطوير قدرات الردع السيبراني من خلال إظهار قدرتها على تنفيذ عمليات مضادة بما يشكل رسالة ردعية للخصوم المحتملين[46].

ثانياً_ التعاون الدولي وتنسيق الجهود الجماعية

أثبتت التجربة أن مواجهة الحرب السيبرانية لايمكن أن تتم بمعزل عن التعاون الدولي نظراً للطابع العالمي للشبكات الرقمية وقد برزت مبادرات متعددة في هذا السياق من بينها اتفاقيات دولية لتجريم الجرائم السيبرانية وتعزيز تبادل المعلومات بين الدول، وتعد اتفاقية بودابست بشأن الجرائم المعلوماتية، التي أُبرمت في إطار الاتحاد الأوروبي من أبرز الصكوك الدولية في هذا المجال، إذ وضعت إطاراً للتعاون القضائي وتبادل الأدلة الرقمية، كما شهدت السنوات الأخيرة جهوداً داخل الأمم المتحدة لصياغة معايير سلوك مسؤولة للدول في الفضاء السيبراني عبر فرق خبراء حكوميين ومجموعات عمل مفتوحة العضوية، وفي الإطار الدفاعي أولى (الناتو) أهمية خاصة للأمن السيبراني، واعتبر الهجمات السيبرانية الجسيمة ضمن نطاق الدفاع الجماعي في حالات معينة، كما أنشأ مركزاً للتميز في الدفاع السيبراني يعنى بالبحث والتدريب وتطوير العقيدة السيبرانية ويظهر هذا الاتجاه أن الأمن السيبراني لم يعد شأناً تقنياً فحسب، بل أصبح جزءاً من منظومة الأمن الجماعي والتحالفات الاستراتيجية[47].

ثالثاً_ تطوير مفهوم الردع السيبراني

في ظل غياب قواعد دولية ملزمة تحدد بدقة حدود السلوك في الفضاء السيبراني، اتجهت بعض الدول إلى تبني استراتيجيات ردع تقوم على مزيج من الدفاع القوي والقدرة على الرد، ويقوم الردع السيبراني على إقناع الخصم بأن تكلفة الهجوم ستكون أعلى من مكاسبه المحتملة غير أن الردع في المجال السيبراني يواجه تحديات، أبرزها صعوبة الإسناد، ما قد يُضعف مصداقية التهديد بالرد، كما أن طبيعة الفضاء الرقمي تسمح بوجود فاعلين غير حكوميين، ما يعقد معادلة الردع التقليدية[48].

سابعاً_ الحوكمة الرقمية والمعايير الدولية

أدرك المجتمع الدولي أن ضبط الفضاء السيبراني يتطلب تطوير معايير سلوك طوعية تُرسخ مبدأ المسؤولية المشتركة وقد جرى التأكيد في عدة تقارير أممية على ضرورة احترام السيادة، وعدم استهداف البنى التحتية الحيوية في أوقات السلم وتعزيز الثقة المتبادلة عبر تبادل المعلومات غير أن هذه المعايير ما زالت في طور التطور ولم تتحول بعد إلى قواعد ملزمة، وهو ما يجعل الآليات الحديثة لمواجهة الحرب السيبرانية قائمة على مزيج من الالتزامات القانونية الصلبة والمعايير الطوعية والتفاهمات السياسية[49].

ويتضح أن مواجهة الحرب السيبرانية تتطلب مقاربة شاملة تتجاوز الحلول التقنية البحتة، لتشمل الأبعاد القانونية والمؤسسية والدولية والبشرية، فالآليات الحديثة تتوزع بين تعزيز القدرات الدفاعية، وتطوير التشريعات الوطنية، وتفعيل التعاون الدولي، وحماية البنى التحتية الحيوية، وبناء الردع السيبراني. غير أن فعالية هذه الآليات تظل رهينة الإرادة السياسية والتنسيق الدولي، في ظل بيئة رقمية متغيرة وسريعة التطور، ومن ثم فإن التحدي لا يكمن فقط

في صد الهجمات بل في بناء منظومة أمن سيبراني متكاملة قادرة على التكيف مع طبيعة الصراع الرقمي المتجددة، وتحقيق التوازن بين مقتضيات الأمن واحترام مبادئ القانون الدولي.

الهوامش:

---

(1) خالد وليد محمود، الهجمات عبر الانترنت ساحة الصراع الالكتروني الجديدة، المركز العربي للأبحاث ودراسة السياسات، الدوحة، 2013، ص 4.

(2) زهراء عماد كلنتر، المسؤولية الدولية الناشئة عن الهجمات السيبرانية، مكتبة القانون المقارن، العراق، 2021، ص18.

(3) آية طارق عبد الهادي، الأمن السيبراني والخصوصية في الفضاء الرقمي، المتحدة للنشر والتوزيع، الإمارات العربية المتحدة، 2023، ص21.

(4) دحان حزام القريطي، الأمن السيبراني وحماية أمن المعلومات، دار الفكر الجامعي، مصر، 2021، ص55.

(5) مؤسسة راند (مؤسسة الأبحاث والتطوير) هي منظمة غير ربحية تأسست عام 1948 من قبل شركة الطائرات دوغلاس لتقديم تحليلات وأبحاث للقوات المسلحة الأمريكية.

(6) إسماعيل محمود الرزاز، لحماية القانونية من الهجمات والجرائم السيبرانية، مركز المحمود لتوزيع الكتب القانونية، مصر، 2023، ص28.

(7) دحان حزام القريطي، الأمن السيبراني وحماية أمن المعلومات، مرجع سابق، ص58.

(8) نورة شلوش، القرصنة الإلكترونية في الفضاء السيبراني "التهديد المتصاعد لأمن الدول"، مجلة بابل للدراسات الإنسانية، العدد 2، العراق، 2018، ص191.

(9) خالد الغنامي، الحروب السيبرانية وساحة الصراع الجديدة، منشور بتاريخ 1-6-2025 على الرابط التالي https://www.majalla.com/node/326267/، تاريخ الزيارة 1-2-2026.

(10) نسيب نجيب، الحرب السيبرانية من منظور القانون الدولي الإنساني، المجلة النقدية للقانون والعلوم السياسية، المجلد16، العدد4، الجزائر، 2021، ص225.

(11) الخنادق، الحرب الالكترونية والسيبرانية: تنوع اشكال والهدف واحد، منشور بتاريخ 9-11-2021 على الرابط التالي https://www.alkhanadeq.com/post.php?id=1682، تاريخ الزيارة 1-2-2026.

(12) أنغام عبد الرضا العكابي، توظيف الحروب السيبرانية في تطوير مفهوم القوة للدول الكبرى، مجلة قضايا سياسية، العدد3، 2024، ص430.

(13) وفاء بوكابوس، تحول القوة في العلاقات الدولية: دراسة في انتقال القوة من التقليدية إلى الحديثة، ط1، المركز الديمقراطي العربي للدراسات الاستراتيجية والسياسية والاقتصادية، المانيا، 2019، ص69.

(14) خضر مصباح اسماعيل، أساسيات أمن المعلومات والحاسوب، ط1، دار حامد للنشر والتوزيع، الأردن، 2019، ص60.

[15] أنغام عبد الرضا العكابي، توظيف الحروب السيبرانية في تطوير مفهوم القوة للدول الكبرى، مرجع سابق، ص432.

[16] علي زياد العلى، على حسين حميد، تكتيكات الحروب الحديثة: الأمن السيبراني والحروب المعززة والهجينة، ط1، العربي للنشر والتوزيع، القاهرة، 2023، ص 24.

[17] عبد الوهاب كريم حميد، الأمن السيبراني – القيود والتحديات في ضوء القانون الدولي، مجلة العقد الاجتماعي، العدد 0، أربيل، 2021، ص 310.

[18] حازم محمد خليل، استغلال الفضاء السيبراني في الحروب غير التقليدية: دراسة في الوكالة السيبرانية والإرهاب السيبراني، المجلة العلمية لكلية الدراسات الاقتصادية والعلوم السياسية، المجلد 8، العدد 15، 2023، ص 302.

[19] ايمن احمد الحديدى، الأمن السيبراني في ظل الانفجار المعرفي، ط1، دار اليازوردي للنشر والتوزيع، الأردن، 2022، ص 41.

[20] ماجد عزيز إسكندر، التوظيف السياسي للهجمات السيبرانية ومخاطرها على الأمن القومي، ط1، مركز الإمارات للدراسات والبحوث الاستراتيجية، 2023، ص 28.

[21] نبراس إبراهيم مسلم، الجرائم السيبرانية وأثرها على الأمن السيبراني، مجلة القادسية للقانون والعلوم السياسية، العدد 1، العراق، 2021، ص365

[22] سميرة بيطام، تطور الجريمة السيبرانية والآليات القانونية للتصدي لها في ظل التحولات الجيوسياسية، مجلة كلية القانون والعلوم السياسية، العدد 22، العراق، 2023، ص55.

[23] حسين محمد الغول، جرائم شبكة الانترنت والمسؤولية الجزائية الناشئة عنها، منشورات زين الحقوقية، بيروت، 2017، ص132.

[24] بلقاسم القفصي، الفيروسات الحاسوبية وأثرها على الأمن السيبراني، منشور بتاريخ 14-3-2025 على الرابط التالي https://www.fikran.com/read-blog/69901_، تاريخ الزيارة 1-2-2026.

[25] ماجد الحنيطي،"تكنولوجيا الصراعات الدولية المعاصرة"، شركة الان ناشرون وموزعون، الأردن، 2021، ص75.

[26] محمد الجنون، الحرب السيبرانية.. كل ما تود معرفته عن معارك تدار "بلا رصاص"، منشور بتاريخ 6-9-2025 على الرابط التالي https://www.alaraby.com/news/ ، تاريخ الزيارة 1-2-2026.

[27] جيم هولدسوورث، ما المقصود بالهجوم الموزع لحجب الخدمة (DDoS)؟، منشور بتاريخ 15-10-2025 على الرابط التالي https://www.ibm.com/sa-ar/think/topics/ddos، تاريخ الزيارة 1-2-2026.

[28] ماثيو كوسينسكي، ما المقصود بهجوم موزع لحجب الخدمة (DDoS)، منشور بتاريخ 16-8-2025 على الرابط التالي https://me.kaspersky.com/resource-center/threats/ddos-attacks ، تاريخ الزيارة 1-2-2026.

[29] إيهاب خليفة، الحرب السيبرانية الاستعداد لقيادة المعارك العسكرية في الميدان الخامس، دار العربي للنشر والتوزيع، مصر، 2021، ص125.

(30) أمريكي ومتعاقد تقني وعميل موظف لدى وكالة المخابرات المركزية، عمل كمتعاقد مع وكالة الأمن القومي قبل أن يسرب تفاصيل برنامج التجسس بريسم إلى الصحافة، في يونيو 2013 سرب سنودن مواد مصنفة على أنها سرية للغاية من وكالة الأمن القومي، منها برنامج بريسم إلى صحيفة الغارديان وصحيفة الواشنطن بوست، في 21 يونيو 2013 وجه له القضاء الأمريكي رسميا تهمة التجسس وسرقة ممتلكات حكومية ونقل معلومات تتعلق بالدفاع الوطني دون إذن والنقل المتعمد لمعلومات مخابرات سرية لشخص غير مسموح له بالاطلاع عليها.

(31) عبير علي حسين الورفلي، جرائم التجسس الالكتروني للمعلومات الشخصية في إطار اتفاقية بودابست بشأن (18) الجريمة الالكترونية، مجلة أبحاث بكلية الآداب، جامعة سرت، العدد15 ،2023، ص 134.

(32) فارس العمارات، الأمن السيبراني، المفهوم وتحديات العصر، دار الحليج للنشر والتوزيع، الأردن، 2022، ص150.

(33) علي العلي، تكتيكات الحروب الحديثة.. الأمن السيبراني والحروب المعززة والهجينة، دار العربي للنشر والتوزيع، مصر، 2022، ص50.

(34) محمد محمود زيتون، القوة السيبرانية أداة للتأثير والسيطرة في الفضاء السيبراني والعلاقات الدولية، المجلة العربية للنشر العلمي، العدد77، الاردن، 2025، ص209.

(35) سامية بوشوشة، التجسس الإلكتروني وطرق مكافحته، مجلة العلوم الاجتماعية والإنسانية، المجلد16، العدد1، الجزائر، 2023، ص55.

(36) إيهاب خليفة، ما هو موقف ميثاق الأمم المتحدة من استخدام القوة السيبرانية في التفاعلات الدولية؟، منشور بتاريخ 24-10-2019 على الرابط التالي https://futureuae.com/ar-AE/Mainpage/Item/5051/، تاريخ الزيارة 1-2026.

(37) نص المادة (2/4) من ميثاق الأمم المتحدة على ما يلي: يمتنع أعضاء الهيئة جميعاً في علاقاتهم الدولية عن التهديد باستعمال القوة أو استخدامها ضد سلامة الأراضي أو الاستقلال السياسي لأية دولة أو على أي وجه آخر لا يتفق ومقاصد "الأمم المتحدة"..

(38) محمد جبار جدوع العبدلي، الحروب الوقائية السيبرانية وفقاً لقواعد القانون الدولي، مجلة تكريت للحقوق، المجلد9، العدد4، العراق، 2025، ص160.

(39) المادة (51) من ميثاق الأمم المتحدة والتي نصت على ما يلي: ليس في هذا الميثاق ما يضعف أو ينتقص الحق الطبيعي للدول، فرادى أو جماعات، في الدفاع عن أنفسهم إذا اعتدت قوة مسلحة على أحد أعضاء "الأمم المتحدة" وذلك إلى أن يتخذ مجلس الأمن التدابير اللازمة لحفظ السلم والأمن الدولي، والتدابير التي اتخذها الأعضاء استعمالاً لحق الدفاع عن النفس تبلغ إلى المجلس فورا، ولا تؤثر تلك التدابير بأي حال فيما للمجلس - بمقتضى سلطته ومسؤولياته المستمرة من أحكام هذا الميثاق - من الحق في أن يتخذ في أي وقت ما يرى ضرورة لاتخاذه من الأعمال لحفظ السلم والأمن الدولي أو إعادته إلى نصابه.

(40) عبد الحليم مرزوقي، الدفاع الشرعي ضد فعل العدوان في اطار القانون الدولي، مجلة الاجتهاد القضائي، جامعة محمد خيضر بسكرة، المجلد 14، العدد 29، الجزائر، 2022، ص251.

(41) تيم مورر وارثر نيلسون، التهديد السيبراني العالمي، مجلة التمويل والتنمية، العدد (58)، صندق النقد الدولي، واشنطن، 2021، ص25.

(42) أحمد عبيس نعمة الفتلاوي، الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مجلة المحقق الحلي للعلوم القانونية والسياسية، العدد 4، السنة 8، كلية جامعة بابل، العراق، 2016، ص14

(43) كاميران عزيز حسن، الجهود الدولية في مواجهة الجرائم السيبرانية، ط1، منشورات الحلبي الحقوقية للنشر والتوزيع، بيروت، لبنان، 2021، ص 32.

(44) جيلالي شويرب، مفهوم الحروب السيبرانية والأمن السيبراني، مجلة الحقوق والحريات، مج11، ع1، 2023، ص 178.

(45) رحموني محمد، منظمة الشرطة الجنائية الدولية (الانتربول) آلية لمكافحة الجريمة المنظمة، مجلة آفاق علمية، المجلد 11، العدد 4، 2019، ص 74 – 75.

(46) عبد الله نوار شعت، التعاون الدولي في مكافحة الجريمة المنظمة والارهاب الدولي، ط1، مكتبة الوفاء القانونية، الاسكندرية، 2016، ص 296.

(47) عبد الحسين سلمان العبوسي، مكافحة الارهاب في ضوء آليات القانون الدولي . دراسة مقارنة، ط1، دار السنهوري، بيروت، 2023 ،ص 192.

(48) رغدة البهي، الردع السيبراني: المفهوم والإشكاليات والمتطلبات، منشور بتاريخ 21-2-2017 على الرابط التالي https://democraticac.de/?p=43837#_ftn34، تاريخ الزيارة 1-2-2026.

(49) أمل فوزي أحمد عوض، الملكية الرقمية في عصر الذكاء الإصطناعي، تحديات الواقع والمستقبل، إصدارات المركز الديمقراطي العربي للدراسات، ألمانيا، 2021، ص4.

قائمة المصادر والمراجع

أولاً_ الكتب القانونية

1.إسماعيل محمود الرزاز، لحماية القانونية من الهجمات والجرائم السيبرانية، مركز المحمود لتوزيع الكتب القانونية، مصر، 2023.

2.أمل فوزي أحمد عوض، الملكية الرقمية في عصر الذكاء الإصطناعي، تحديات الواقع والمستقبل، إصدارات المركز الديمقراطي العربي للدراسات، ألمانيا، 2021.

3.آية طارق عبد الهادي، الأمن السيبراني والخصوصية في الفضاء الرقمي، المتحدة للنشر والتوزيع، الإمارات العربية المتحدة، 2023.

4.ايمن احمد الحديدى، الأمن السيبراني في ظل الانفجار المعرفي، ط1، دار اليازوردي للنشر والتوزيع، الأردن، 2022.

5.إيهاب خليفة، الحرب السيبرانية الاستعداد لقيادة المعارك العسكرية في الميدان الخامس، دار العربي للنشر والتوزيع، مصر، 2021.
6.حسين محمد الغول، جرائم شبكة الانترنت والمسؤولية الجزائية الناشئة عنها، منشورات زين الحقوقية، بيروت، 2017.
7.خالد وليد محمود، الهجمات عبر الانترنت ساحة الصراع الالكتروني الجديدة، المركز العربي للأبحاث ودراسة السياسات، الدوحة، 2013.
8.خضر مصباح اسماعيل، أساسيات أمن المعلومات والحاسوب، ط1، دار حامد للنشر والتوزيع، الأردن، 2019.
9.دحان حزام القريطي، الأمن السيبراني وحماية أمن المعلومات، دار الفكر الجامعي، مصر، 2021.
10.زهراء عماد كلنتر، المسؤولية الدولية الناشئة عن الهجمات السيبرانية، مكتبة القانون المقارن، العراق، 2021.
11.عبد الحسين سلمان العبوسي، مكافحة الارهاب في ضوء آليات القانون الدولي ـ دراسة مقارنة، ط1، دار السنهوري، بيروت، 2023.
12.عبد الله نوار شعت، التعاون الدولي في مكافحة الجريمة المنظمة والارهاب الدولي، ط1، مكتبة الوفاء القانونية، الاسكندرية، 2016.
13.علي العلي، تكتيكات الحروب الحديثة.. الأمن السيبراني والحروب المعززة والهجينة، دار العربي للنشر والتوزيع، مصر، 2022.
14. علي زياد العلى، على حسين حميد، تكتيكات الحروب الحديثة: الأمن السيبراني والحروب المعززة والهجينة، ط1، العربي للنشر والتوزيع، القاهرة، 2023.
15.فارس العمارات، الأمن السيبراني، المفهوم وتحديات العصر، دار الحليج للنشر والتوزيع، الأردن، 2022.
16.كاميران عزيز حسن، الجهود الدولية في مواجهة الجرائم السيبرانية، ط1، منشورات الحلبي الحقوقية للنشر والتوزيع، بيروت، لبنان، 2021.
17.ماجد الحنيطي،"تكنولوجيا الصراعات الدولية المعاصرة"، شركة الان ناشرون وموزعون، الأردن، 2021.
18.ماجد عزيز إسكندر، التوظيف السياسي للهجمات السيبرانية ومخاطرها على الأمن القومي، ط1، مركز الإمارات للدراسات والبحوث الاستراتيجية، 2023.
19.وفاء بوكابوس، تحول القوة في العلاقات الدولية: دراسة في انتقال القوة من التقليدية إلى الحديثة، ط1، المركز الديمقراطي العربي للدراسات الاستراتيجية والسياسية والاقتصادية، المانيا، 2019.

ثانياً_ المجلات

1.أحمد عبيس نعمة الفتلاوي، الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مجلة المحقق الحلي للعلوم القانونية والسياسية، العدد 4، السنة 8، كلية جامعة بابل، العراق، 2016.

2.أنغام عبد الرضا العكابي، توظيف الحروب السيبرانية في تطوير مفهوم القوة للدول الكبرى، مجلة قضايا سياسية، العدد3، 2024.
3.تيم مورر وارثر نيلسون، التهديد السيبراني العالمي، مجلة التمويل والتنمية، العدد (58)، صندق النقد الدولي، واشنطن، 2021.
4.جيلالي شويرب، مفهوم الحروب السيبرانية والأمن السيبراني، مجلة الحقوق والحريات، مج11، ع1، 2023.
5.حازم محمد خليل، استغلال الفضاء السيبراني في الحروب غير التقليدية: دراسة في الوكالة السيبرانية والإرهاب السيبراني، المجلة العلمية لكلية الدراسات الاقتصادية والعلوم السياسية، المجلد 8، العدد 15، 2023.
6.رحموني محمد، منظمة الشرطة الجنائية الدولية (الانتربول) آلية لمكافحة الجريمة المنظمة، مجلة آفاق علمية، المجلد 11، العدد 4، 2019.
7.سامية بوشوشة، التجسس الإلكتروني وطرق مكافحته، مجلة العلوم الاجتماعية والإنسانية، المجلد16، العدد1، الجزائر، 2023.
8.سميرة بيطام، تطور الجريمة السيبرانية والآليات القانونية للتصدي لها في ظل التحولات الجيوسياسية، مجلة كلية القانون والعلوم السياسية، العدد 22، العراق، 2023.
9.عبد الحليم مرزوقي، الدفاع الشرعي ضد فعل العدوان في اطار القانون الدولي، مجلة الاجتهاد القضائي، جامعة محمد خيضر بسكرة، المجلد 14، العدد 29، الجزائر، 2022.
10.عبد الوهاب كريم حميد، الأمن السيبراني – القيود والتحديات في ضوء القانون الدولي، مجلة العقد الاجتماعي، العدد 0، أربيل، 2021.
11.عبير علي حسين الورفلي، جرائم التجسس الالكتروني للمعلومات الشخصية في إطار اتفاقية بودابست بشأن (18) الجريمة الالكترونية، مجلة أبحاث بكلية الآداب، جامعة سرت، العدد15 ،2023.
12.محمد جبار جدوع العبدلي، الحروب الوقائية السيبرانية وفقاً لقواعد القانون الدولي، مجلة تكريت للحقوق، المجلد9، العدد4، العراق، 2025.
13.محمد محمود زيتون، القوة السيبرانية أداة للتأثير والسيطرة في الفصاء السيبراني والعلاقات الدولية، المجلة العربية للنشر العلمي، العدد77، الاردن، 2025.
14.نبراس إبراهيم مسلم، الجرائم السيبرانية وأثرها على الأمن السيبراني، مجلة القادسية للقانون والعلوم السياسية، العدد 1، العراق، 2021.
15.نسيب نجيب، الحرب السيبرانية من منظور القانون الدولي الإنساني، المجلة النقدية للقانون والعلوم السياسية، المجلد16، العدد4، الجزائر، 2021.
16.نورة شلوش، القرصنة الإلكترونية في الفضاء السيبراني "التهديد المتصاعد لأمن الدول"، مجلة بابل للدراسات الإنسانية، العدد 2، العراق، 2018.

ثالثاً_ المواثيق الدولية

1. ميثاق اللأمم المتحدة لعان 1945.

رابعاً_ المواقع الالكترونية

1. إيهاب خليفة، ما هو موقف ميثاق الأمم المتحدة من استخدام القوة السيبرانية في التفاعلات الدولية؟، منشور بتاريخ 24-10-2019 على الرابط التالي https://futureuae.com/ar-AE/Mainpage/Item/5051/.
2. بلقاسم القفصي، الفيروسات الحاسوبية وأثرها على الأمن السيبراني، منشور بتاريخ 14-3-2025 على الرابط التالي https://www.fikran.com/read-blog/69901_.
3. جيم هولدسوورث، ما المقصود بالهجوم الموزع لحجب الخدمة (DDoS)؟، منشور بتاريخ 15-10-2025 على الرابط التالي https://www.ibm.com/sa-ar/think/topics/ddos.
4. خالد الغنامي، الحروب السيبرانية وساحة الصراع الجديدة، منشور بتاريخ 1-6-2025 على الرابط التالي https://www.majalla.com/node/326267/.
5. الخنادق، الحرب الالكترونية والسيبرانية: تنوع اشكال والهدف واحد، منشور بتاريخ 9-11-2021 على الرابط التالي https://www.alkhanadeq.com/post.php?id=1682 .
6. رغدة البهي، الردع السيبراني: المفهوم والإشكاليات والمتطلبات، منشور بتاريخ 21-2-2017 على الرابط التالي https://democraticac.de/?p=43837#_ftn34.
7. ماثيو كوسينسكي، ما المقصود بهجوم موزع لحجب الخدمة (DDoS)، منشور بتاريخ 16-8-2025 على الرابط التالي https://me.kaspersky.com/resource-center/threats/ddos-attacks .
8. محمد الجنون، الحرب السيبرانية.. كل ما تود معرفته عن معارك تدار "بلا رصاص"، منشور بتاريخ 6-9-2025 على الرابط التالي https://www.alaraby.com/news/ .

List of Sources and References

First: Legal Books

1. Ismail Mahmoud Al-Razzaz, Legal Protection from Cyber Attacks and Crimes, Al-Mahmoud Center for Legal Book Distribution, Egypt, 2023.
2. Amal Fawzi Ahmed Awad, Digital Property in the Age of Artificial Intelligence: Challenges of Reality and the Future, Arab Democratic Center for Studies Publications, Germany, 2021.
3. Aya Tariq Abdel-Hadi, Cybersecurity and Privacy in the Digital Space, United Publishing and Distribution, United Arab Emirates, 2023.
4. Ayman Ahmed Al-Hadidi, Cybersecurity in Light of the Knowledge Explosion, 1st Edition, Al-Yazourdi Publishing and Distribution House, Jordan, 2022.
5. Ehab Khalifa, Cyber Warfare: Preparing to Lead Military Battles in the Fifth Field, Arab Publishing and Distribution House, Egypt, 2021.

6. Hussein Muhammad Al-Ghul, Internet Crimes and the Arising Criminal Liability, Zain Legal Publications, Beirut, 2017.

7. Khaled Walid Mahmoud, Cyber Attacks: The Arena of Electronic Conflict Al-Jadeeda, Arab Center for Research and Policy Studies, Doha, 2013.

8. Khader Misbah Ismail, Fundamentals of Information and Computer Security, 1st ed., Hamed Publishing and Distribution House, Jordan, 2019.

9. Dahan Hazam Al-Quraiti, Cybersecurity and Information Security Protection, University Thought House, Egypt, 2021.

10. Zahraa Emad Kalantar, International Responsibility Arising from Cyber Attacks, Comparative Law Library, Iraq, 2021.

11. Abdul Hussein Salman Al-Abousi, Combating Terrorism in Light of International Law Mechanisms – A Comparative Study, 1st ed., Al-Sanhouri Publishing House, Beirut, 2023.

12. Abdullah Nawar Shaat, International Cooperation in Combating Organized Crime and International Terrorism, 1st ed., Al-Wafaa Legal Library, Alexandria, 2016.

13. Ali Al-Ali, Modern Warfare Tactics: Cybersecurity and Enhanced and Hybrid Warfare, Arab Publishing and Distribution House, Egypt, 2022.

14. Ali Ziad Al-Ali, Ali Hussein Hamid, Modern Warfare Tactics: Cybersecurity and Enhanced and Hybrid Warfare, 1st ed., Al-Arabi Publishing and Distribution, Cairo, 2023.

15. Fares Al-Amarat, Cybersecurity: The Concept and Challenges of the Era, Dar Al-Khaleej Publishing and Distribution, Jordan, 2022.

16. Kamiran Aziz Hassan, International Efforts to Combat Cybercrime, 1st ed., Al-Halabi Legal Publications for Publishing and Distribution, Beirut, Lebanon, 2021.

17. Majed Al-Hunaity, "The Technology of Contemporary International Conflicts," Al-An Publishers and Distributors, Jordan, 2021.

18. Majed Aziz Iskandar, The Political Exploitation of Cyberattacks and Their Risks to National Security, 1st ed., Emirates Center for Strategic Studies and Research, 2023.

19. Wafaa Boukabous, Power Transformation in International Relations: A Study in the Transition of Power from Traditional to Modern, 1st ed., Arab Democratic Center for Strategic, Political and Economic Studies, Germany. 2019.

Secondly - Journals

1. Ahmed Abis Naama Al-Fatlawi, Cyber Attacks: Their Concept and the International Responsibility Arising Therefrom in Light of Contemporary International Organization, Al-Muhaqqiq Al-Hilli Journal of Legal and Political Sciences, Issue 4, Year 8, College of Babylon University, Iraq, 2016.

2. Angham Abdul-Ridha Al-Akabi, Employing Cyber Warfare in Developing the Concept of Power for Major Powers, Political Issues Journal, Issue 3, 2024.

3. Tim Moorer and Arthur Nelson, The Global Cyber Threat, Finance & Development Journal, Issue (58), International Monetary Fund, Washington, 2021.

4. Jalali Shweireb, The Concept of Cyber Warfare and Cybersecurity, Rights and Freedoms Journal, Vol. 11, No. 1, 2023.

5. Hazem Muhammad Khalil, Exploiting Cyberspace in Unconventional Warfare: A Study in Cyber Agencies and Cyber Terrorism, Scientific Journal of the College of Economic and Political Studies, Vol. 8, No. 15. 2023.

6. Rahmouni Mohamed, The International Criminal Police Organization (Interpol): A Mechanism for Combating Organized Crime, Afaq Ilmiya Journal, Vol. 11, No. 4, 2019.

7. Samia Bouchoucha, Electronic Espionage and Methods of Combating It, Journal of Social and Human Sciences, Vol. 16, No. 1, Algeria, 2023.

8. Samira Bitam, The Evolution of Cybercrime and Legal Mechanisms for Addressing It in Light of Geopolitical Transformations, Journal of the College of Law and Political Science, No. 22, Iraq, 2023.

9. Abdelhalim Marzouki, Legitimate Defense Against Acts of Aggression within the Framework of International Law, Journal of Judicial Reasoning, Mohamed Khider University of Biskra, Vol. 14, No. 29, Algeria, 2022.

10. Abdelwahab Karim Hamid, Cybersecurity – Restrictions and Challenges in Light of International Law, Social Contract Journal, No. 0, Erbil, 2021.

11. Abeer Ali Hussein Al-Warfali, Crimes Electronic Espionage of Personal Information within the Framework of the Budapest Convention on Cybercrime (18), Journal of Research, Faculty of Arts, University of Sirte, Issue 15, 2023.

12. Muhammad Jabbar Jadou' Al-Abdali, Cyber Preemptive Warfare According to the Rules of International Law, Tikrit Journal of Law, Volume 9, Issue 4, Iraq, 2025.

13. Muhammad Mahmoud Zaitoun, Cyber Power: A Tool for Influence and Control in Cyberspace and International Relations, Arab Journal of Scientific Publishing, Issue 77, Jordan, 2025.

14. Nibras Ibrahim Muslim, Cyber Crimes and Their Impact on Cybersecurity, Al-Qadisiyah Journal of Law and Political Science, Issue 1, Iraq, 2021.

15. Naseeb Najib, Cyber Warfare from the Perspective of International Humanitarian Law, Critical Journal of Law and Political Science, Volume 16, Issue 4, Algeria, 2021.

16. Noura Shaloush, Cyber Piracy in Cyberspace: The Escalating Threat to State Security, Babel Journal of Human Studies, Issue 2, Iraq, 2018.

Third: International Conventions

1. United Nations Charter of 1945.

Fourth – Websites

1. Ehab Khalifa, What is the UN Charter's stance on the use of cyber power in international interactions?, published on October 24, 2019, at the following link: https://futureuae.com/ar-AE/Mainpage/Item/5051/ .

2. Belkacem Al-Qafsi, Computer viruses and their impact on cybersecurity, published on March 14, 2025, at the following link: https://www.fikran.com/read-blog/69901_ .

3. Jim Holdsworth, What is a Distributed Denial-of-Service (DDoS) attack?, published on October 15, 2025, at the following link: https://www.ibm.com/sa-ar/think/topics/ddos 4. Khaled Al-Ghannami, Cyber Wars and the New Arena of Conflict, published on June 1, 2025, at the following link: https://www.majalla.com/node/326267/.

5. Al-Khanadeq, Electronic and Cyber Warfare: Diverse Forms, One Goal, published on November 9, 2021, at the following link: https://www.alkhanadeq.com/post.php?id=1682 .

6. Raghad Al-Bahi, Cyber Deterrence: Concept, Problems, and Requirements, published on February 21, 2017, at the following link: https://democraticac.de/?p=43837#_ftn34 7. Matthew Kosinski, What is a Distributed Denial-of-Service (DDoS) Attack?, published on August 16, 2025, at the following link: https://me.kaspersky.com/resource-center/threats/ddos-attacks .

8. Muhammad Al-Janoun, Cyber Warfare: Everything You Need to Know About Battles Waged "Without Bullets", published on September 6, 2025, at the following link: https://www.alaraby.com/news/.

The impact of cyber warfare on international relations and mechanisms for responding to it according to the rules of international law

Dr. Essam Ali Hussein Al-Obaidi

Faculty of Law- Al-Amin University

Keywords: Cyberwarfare, International Responsibility, Digital Espionage, Viruses

Summary:

This study examines the impact of cyber warfare on international relations within the framework of international law, by defining its concept and characteristics and distinguishing it from cybercrime, and analyzing its most prominent forms such as sabotage attacks and digital espionage. It also addresses its repercussions on the balance of power and the stability of the international system in light of the increasing reliance on digital technology. Cyber warfare also raises complex legal issues related to attributing the wrongful act and determining the scope of international responsibility, and the extent to which the provisions of the Charter of the United Nations and the rules of public international law apply to it. In light of this, the need arises to develop modern legal and institutional mechanisms capable of enhancing international cyber security and regulating the behavior of states in this field.