الحرب السيبرانية في ضوء القانون الدولي

إعداد

الدكتور / إسلام رمضان هديب

تمهيد وتقسيم:

لا نستطيع أن ننكر في العصر الحالي مدى الأهمية القصوى لشبكة المعلومات الدولية و مدى احتياجنا إليها وحجم الاستخدامات اليومية للإنترنت؛ حيث أن مقدار تبادل المعلومات يتضخم يوماً بعد يوم ويتداخل في جميع نواحي الحياة للأشخاص على جميع المستويات سواء التعليمية أو المهنية من رواد الأعمال أو الموظفين ومختلف الثقافات بجميع أنحاء العالم بالإضافة إلى المؤسسات الحكومية بجميع دول العالم حيث اتجهت جميع الدول إلى التحول الرقمي وتقديم الخدمات العامة لمواطنيها عبر المنصات الإلكترونية؛ لتسهيل حياة المواطنين وتقديم الخدمات العامة في يسر وتوفيراً للوقت وإنجازاً للعمل، كما أن التحول الرقمي يساعد الدول على التقدم والتطور لمكافحته للفساد وتقليص الأخطاء ويساعد أجهزة الدولة على ربط المعلومات وتبادلها بسهولة ويسر ونتيجة لما سبق يتطلب الأمر تخزين تلك المعلومات والتوسع فى الشبكات الرقمية مما يدعونا للالتفات لأهمية مجال أمن المعلومات والأمن السيبراني على وجه التحديد؛ حتى يتسنى لنا الحفاظ على حجم المعلومات الضخمة المخزنة وتأمين الشبكات الخاصة بتبادل تلك المعلومات وحمايتها من أى خطر قد يهددها سواء داخلياً أو خارجياً ومنع أي محاولات للعبث بتلك المعلومات سواء بفقد أو تعديل أو إضافة أو تسريب، لاعتبار الحفاظ على تلك البيانات والحفاظ على الخدمات الرقمية الحكومية حفاظاً على الأمن القومي للدول.

ولعل مما لا يكاد يخفى أن الأمن السيبراني أصبح من أولويات الدول على الصعيد السياسي والأمني والاقتصادي، فقد أعلنت دول كثيرة عن تخصيص أقسام لمواجهة الحروب السيبرانية كما هو الحال فى الولايات الأمريكية المتحدة أنشأت قسم (us cert) الخاص بمتابعة الهجمات السيبرانية وأحدث البرمجيات الخبيثة وأنواعها وطرق مواجهتها، وأيضًا بجمهورية مصر العربية أنشأت قسم (egy cert) المركز الوطني للاستعداد لطوارئ الحاسبات والشبكات بذات الاختصاصات.

و نظراً لأهمية ذلك المجال تقوم الدول بمحاولة تضافر الجهود على الصعيدين الدولي و الوطني في توسيع سبل التعاون بين جميع القطاعات التقنية والتكنولوجية المختصة لتوفير أكبر قدر من الحماية للفضاء السيبراني والتركيز على ضمان توافر أنظمة المعلومات وتوفير السرية التامة للمعلومات وأكبر قدر ممكن من الخصوصية، واتخاذ جميع التدابير والإجراءات اللازمة لحماية المواطنين والمستخدمين عامة للفضاء السيبراني لمنع أى محاولات للاستخدام غير المشروع أو المُصرح به أو أى محاولات لاختراق تلك الشبكات الخاصة بتبادل المعلومات؛ لما تحويه من بيانات ومعلومات شخصية وهامة للمستخدمين.

وسوف نستخدم مصطلح الحرب السيبرانية للإشارة إلى أحد أحدث الأساليب المستخدمة في عمليات الفضاء السيبراني والتي قد تصل في مقدار الخطورة والتهديد إلى مستوى الحروب المسلحة ضمن المفهوم المعنى في القانون الدولي الإنساني.

ولا شك أن الحرب السيبرانية تُعدّ خطوة واسعة في مجال استخدام الأسلحة غير التقليدية في الحروب؛ إذ أدت الهجمات من هذا النوع إلى تغيير موازين القوى في تقييم القوة العسكرية للجيوش، كما أدت إلى تعديل في قواعد القتال ليتحول من قتال مباشر بين أفراد في ساحات المعارك إلى قتال يدور من خلف شاشات أجهزة الحاسب الألى، من شأنه إلحاق خسائر لا حصر لها بالقوات المعادية قد تفوق في تأثيرها المعارك التقليدية واستخدام الأسلحة الفتاكة، وهو الأمر الذي أوعز لفقه القانون الدولي أن يتداول في مناقشاته هذا النوع من الحروب نظرا للآثار التي تترتب عليه من ناحية، ونظرا لحداثته إلى درجة عدم تخصيص المشرع الدولي نصوصا لتنظيمه من ناحية أخرى.

ويتفق الفقه على أن القانون الدولي في نصوصه لم يتناول الحروب السيبرانية بصورة أو بأخرى، إلا أن هذا الفقه في الوقت ذاته يرى أن قواعد القانون الدولي المنظمة للحروب التقليدية تتسع لتستغرق كافة الأفعال التي تمثل الحرب السيبرانية، مع المطالبة بمزيد من تدخل المشرع الدولي لتنظيم هذا النوع من الحروب بما يتناسب مع التطور الحادث في النظم غير التقليدية للحرب.

إشكالية البحث:

فى ظل العصر الحالي نشهد جيلاً جديداً من الحروب على غرار الحروب التقليدية التي شهدناها في الماضى فنحن الآن في عصر الحروب اللامتماثلة ومن أبرز صورها الحروب السيبرانية والهجمات السيبرانية والتي تحدث في ميدان الفضاء السيبرانى وقد تحدث بالاتساق

مع الحروب التقليدية (العدوان المسلح) أو قد تكون منفصلة عنه ونظراً لانطباق قواعد القانون الدولى الانسانى ومبادئه على كافة النزاعات الدولية والذي يحرم العدوان المسلح بكافة أشكاله، فالإشكالية هنا هل تنطبق مبادئ وقواعد القانون الدولى على تلك الحروب السيبرانية؟

أهمية البحث:

تكمن أهمية هذا البحث في أنه يعالج موضوعاً حديثاً لا يزال في طور التبلور كما يلقي الضوء على مفهوم الهجمات السيبرانية وطبيعتها الاستثنائية، بالإضافة إلى ذلك فإنه يحلل قواعد ومبادئ القانون الدولي الإنساني لفحص قابليتها للتطبيق على الهجمات السيبرانية، ويقوم هذا التطبيق على الحالات التطبيقية للهجمات السيبرانية التي حدثت بالفعل.

منهج البحث:

اعتمدنا في هذه الدراسة على المنهج الوصفي التحليلي لأنها تتناسب مع طبيعة البحث والموضوعات التي نتناولها بالبحث؛ حيث يدور موضوع البحث حول مدى إمكانية تطبيق قواعد القانون الدولى على الحروب والهجمات السيبرانية.

وفي سبيل دراسة الحرب السيبرانية في ضوء القانون الدولي رأى الباحث تقسيم الدراسة إلى ثلاثة مباحث يتناول من خلالها توضيح مفهوم الحرب السيبرانية، والتكييف القانوني لأفعالها من خلال القانون الدولي، بالإضافة إلى توضيح دور القانون الدولي في مواجهتها، وذلك على النحو التالي:

المبحث الأول: ماهية الحرب السيبرانية وصورها فى القانون الدولي.

المبحث الثاني: التكيف القانوني للحرب السيبرانية فى ضوء القانون الدولي.

المبحث الثالث: دور القانون الدولي فى مواجهة الحرب السيبرانية.

المبحث الأول: ماهية الحرب السيبرانية وصورها فى القانون الدولي

تمهيد وتقسيم:

تُعدّ أهم الأسباب التي دعت المجتمع الدولي للاهتمام بالحرب السيبرانية وأدواتها هي دخول الفضاء السيبراني حيز الاستغلال بصورة متصاعدة، وشروع عديد من الدول في استخدامه عسكرياً، وهي الصورة التي استحدثها الواقع وفرض على المجتمع الدولي تنظيمها باعتبار أن الفضاء ملكية عامة للدول بأكملها ولا يجوز أن تستأثر إحداها باستخدامه، خاصة إذا كان هذا الاستخدام يمثل أضراراً تصيب الدول الأخرى[1].

وتعد الحرب السيبرانية إحدى الوسائل التي تستخدم في القتال العسكري؛ بحيث تمثل في حد ذاتها الحرب العسكرية، أو تكون جزءً من

---

[1] بشير حسن الحمداني، **القرصنة الإلكترونية – أسلحة الحرب الحديثة**، دار أسامة للنشر والتوزيع، عمان ٢٠١٤، ص ١١

هذه الحرب، وفي كافة الأحوال فإن تأثيرها في المعارك يماثل أو يفوق تأثير الأسلحة التقليدية؛ إذ يتجه الهجوم السيبراني للعدوان الإلكتروني على المنشآت المعادية، حيث يشمل الاختراقات والاعتداءات على النظم المعلوماتية للخصم، بحيث يؤدي هذا الاعتداء لتدمير البنية الإلكترونية للعدو من خلال إصابة منشآته بالضرر والفوضى الإلكترونية بحيث تعجز عن أداء وظائفها وربما تتحول قيادتها إلى الخصم[٢].

وتستهدف الحرب السيبرانية عادة مهاجمة تكنولوجيا المعلومات، ونظم إمدادات الطاقة، والخدمات اللوجستية، ووسائل الاتصال الإلكترونية، وكافة المنشآت الحيوية التي تعتمد على وسائل تقنية المعلومات أساًسا لعملها؛ بحيث تستهدف الهجمات تعطيل هذه المرافق عن أداء الدور المنوط بها، أو الاستيلاء على المعلومات المخزنة على مواقعها، أو تناولها بالمحو أو الإتلاف أو التعديل؛ وذلك لضمان إحداث خلل بنظم العمل بها بحيث تخرج عن السبيل الذي ترسمه الدولة للاستفادة من هذه المرافق والمنشآت[٣].

ولا يمكن النظر للحرب السيبرانية كوحدة واحدة أو صورة وحيدة للهجمات، وإنما تتعدد صور هذه الحروب بطريقة كان لا بد معها للقانون الدولي أن يراجع موقفه من هذه الهجمات؛ بحيث يتصدى لها

---

[2] عبد الكريم محمود، **تحديات السيادة السيبرانية في القانون الدولي**، المركز العربي لأبحاث الفضاء الالكتروني، القاهرة ٢٠٢١، ص ٢٤

[3] عبد القادر دندن، **العلاقات الدولية في عصر التكنولوجيا الرقمية**، مركز الكتاب الأكاديمي، عمان ٢٠٢١، ص ١٦

بالمواجهة أو على الأقل بالتنظيم الذي يتناسب مع قواعد الحروب المقررة في هذا القانون[٤].

وعلى هذا ووفقًا للتمهيد السابق فقد قسم الباحث الدراسة في هذا المبحث إلى مطلبين، حيث تناول في المطلب الأول تحديد مفهوم هذه الحرب، بينما اتجه من خلال المطلب الثاني إلى توضيح صور هذه الهجمات وتحليل كل شكل لها.

المطلب الأول: تعريف الحرب السيبرانية.

المطلب الثاني: صور الحرب السيبرانية.

المطلب الأول: تعريف الحرب السيبرانية

اشتق مصطلح السيبرانية لغوياً من المصطلح اليوناني kybernetes والذي يعني: التحكم والقيادة عن بعد ودون تعامل مباشر، كما استخدم المصطلح علمياً لأول مرة في علم الرياضيات للتعبير عن

[4] ماجد الغيطي، **دور التكنولوجيا في إدارة الصراعات الدولية المعاصرة**، دار الآن للطباعة والنشر، بيروت ٢٠١٩، ص ٢٩

التحكم والاتصالات في الحيوانات والآلات دون تلامس مباشر، أو ما سمي وقتها بآليات التنظيم الذاتي[٥].

وهو تعبير لغوي عن الهجمات الإلكترونية، والتي تستخدم فيها وسائل تقنية المعلومات لإلحاق الخسائر بالخصم وممتلكاته ومرافقه، وذلك على سبيل الإضرار بمصالح الخصم وهو هدف أي حرب[٦].

ولقد عرف البعض الحرب السيبرانية اصطلاحا بأنها: إجراءات أو تصرفات تقوم بها الدولة كنوع من مهاجمة نظم المعلومات الخاصة بالخصم، واستهداف الإضرار بها، وترك آثارًا سلبية من شأنها الإسهام في تحقيق الاستراتيجيات العامة للحروب، وتحقيق أضرار تصيب الخصم قدر الإمكان[٧].

---

[5] نور أمير الموصلي، **الهجمات السيبرانية في ضوء القانون الدولي الانساني**، بحث مقدم استكمالا لمتطلبات نيل درجة ماجستير التأهيل والتخصص في القانون الدولي الانساني، الجامعة السورية، دمشق ٢٠٢١، ص٨، البحث متوفر على الموقع الرسمي للجامعة الافتراضية السورية
https://pedia.svuonline.org/pluginfile.php/3200/mod_label/intro
تاريخ الاطلاع ٢٠٢٢/٢/١٥

[6] عمر سعد الزيات، **أسلحة الدمار الشامل في القانون الدولي**، منشورات الحلبي الحقوقية، بيروت ٢٠١٧، ص٦٢

[7] احمد حمدي علي، **الحرب في الإسلام والقانون الدولي الإنساني**، المكتبة الأزهرية للتراث، القاهرة ٢٠٢٠، ص ٤٢

والواقع أن أغلب التعريفات التي تم إقرارها بشأن الحرب السيبرانية تشترك في ذات المعنى، وهو استهداف مواقع إلكترونية أو نظم رقمية، أو أجهزة حاسب آلي، وذلك باستخدام وسائل اتصال رقمية، للاعتداء على سلامة وسرية المعلومات الخاصة بالخصم، إما بالحصول على هذه المعلومات، أو محوها أو إتلافها، أو إعادة برمجتها بحيث تعمل بصورة عكسية في صالح الجاني وضد مصلحة الدولة مالكة النظام المعلوماتي[٨].

وبرغم الاتفاق في المعنى إلا أن هناك اتفاق بين الفقه القانوني على غموض تعريفات الحرب السيبرانية كافة، حيث اتجه جانب من الفقه الى تعريف هذه الحرب اشتقاقا من البيئة التي تتم فيها، وهي الفضاء الإلكتروني، أو الفضاء السيبراني فاعتبر أن أي هجمات تتم من خلال هذا المحيط هي هجمات سيبرانية، كما اتجه فقه آخر إلى تعريف الحرب السيبرانية عن طريق الوسائل المستخدمة فيها، وهي الوسائل الإلكترونية، فاعتبر أن أي هجوم تستخدم أو تستهدف من خلاله هذه الوسائل هو هجوم سيبراني، تأسيسا على وسيلة القيام به وبغض النظر عن المحيط الذي تتم فيه الهجمات، وأخيراً رأى البعض أن تعريف الحرب السيبرانية يأتي من خلال تحقيق استراتيجية معينة في الحروب وهي استخدام كافة الوسائل الممكنة لتحقيق أكبر كم ممكن من الأضرار

---

[8] صبري حيدرة، **مواجهة الهجمات السيبرانية في القانون الدولي**، بحث منشور في مجلة حقوق الانسان والحريات العامة، عدد ٤، جامعة عبد الحميد بن باديس، الجزائر ٢٠١٧، ص ١٨٦

لدى الخصم، وهو ما يتطلب استخدام الوسائل الحديثة لتحقيق هذا الهدف ومنها وسائل تقنية المعلومات٩.

وفي ضوء الهدف من الحرب السيبرانية نظر إليها بعض الفقه على إنها أحد أنواع الهجمات التي ترتكب عن طريق شبكة الانترنت، وذلك بالتسلل خلال المواقع الإلكترونية للخصم، بهدف تخريب أو إتلاف المعلومات والبيانات الموجودة في هذه المواقع، وتقوم بها دولة ضد دولة أخرى، في سياق العدوان المتبادل، كما نظر إليها فقه آخر على انها عدد من الإجراءات التي تقوم بها إحدى الدول للهجوم على نظم المعلومات المملوكة لدولة أخرى، وذلك بهدف الإضرار بها، أو بهدف الدفاع عن نظم المعلومات الخاصة بالدولة المهاجمة، عن طريق تدمير نظم المعلومات الخاصة بالخصم١٠.

وقد تصدى عدد من أشخاص المجتمع الدولي لتعريف الحرب السيبرانية، منها اللجنة الدولية للصليب الأحمر، والتي عرفت الحرب السيبرانية بأنها الاستغلال المتعمد لعدد من الأنشطة بهدف إفساد أو إتلاف أو تدمير الأنظمة الخاصة بالحاسب الآلي أو الشبكات الرقمية الخاصة بالخصم، وتقع على المعلومات والبيانات والأنظمة والشبكات، وأي كيان يرتبط مع هذه الأنظمة والشبكات، وتستخدم هذه الهجمات إما

---

[9] علي عبد الله فضل الله، **الحرب الشرعية والحرب المشروعة في القانون الدولي**، منشورات الحلبي الحقوقية، بيروت ٢٠١٨، ص ١١٦

[10] احمد عبيس الفتلاوي، **الهجمات السيبرانية – دراسة قانونية تحليلية بشأن تحديات تنظيمها المعاصر**، منشورات زين الحقوقية، بيروت ٢٠١٨، ص ١٨

للإضرار بالممتلكات الإلكترونية للخصم، أو لحرمانه من استخدام هذه الممتلكات، عن طريق منعه من الولوج للمواقع الرسمية الخاصة به واستخدامها على النحو الذي يراه، كما قد تستخدم هذه الهجمات على نحو عكسي في الدفاع عن المنشآت الإلكترونية للدولة، وذلك عن طريق منع أي دخول غير مرخص له للمواقع الإلكترونية الخاصة بالدولة[١١].

ولا يمكن إطلاق مصطلح الحرب السيبرانية إلا إذا كان الاعتداء السيبراني في سياق نزاع مسلح، أو جاء ليعبر عن عدوان دولة ضد دولة؛ إذ لا يمكن اعتبار الهجمات التي يقوم بها كيان غير مشروع نوعاً من الحرب السيبرانية التي تعالج ضمن قواعد القانون الدولي العام، وهو ما يعني أن مفهوم الحرب السيبرانية هو أضيق من مفهوم الهجمات السيبرانية، حيث يشمل أي اعتداء سيبراني أي كان أطرافه، يتوقع منه إلحاق الأضرار بالأشخاص أو الأعيان، وسواء كان مصدره أحد أشخاص القانون الدولي أو غيرهم، فالهجمات السيبرانية قد تقع ضمن نطاق الحرب السيبرانية وقد تقع خارج هذا النطاق، لذلك يمكن القول أن مفهوم الهجمات السيبرانية يستغرق بداخله مفهوم الحرب السيبرانية[١٢].

---

[11] هربرت لين، **النزاع السيبراني والقانون الدولي الإنساني**، مقال منشور في مجلة اللجنة الدولية للصليب الأحمر، مجلد ٩٤ عدد ٨٨٦، جنيف ٢٠١٢، ص ٥٢٢

[12] - Philip Levitz, **The law of cyber– Attack**, 2012, Vol. 100, Issue 4, P833

وعلى هذا يمكن للباحث تعريف الحرب السيبرانية على أنها: هجمات إلكترونية تقوم بها أجهزة حكومية رسمية، ضد أجهزة حكومية رسمية في دولة معادية، وهي جزء من الحرب الشاملة، تهدف إلى إلحاق خسائر بالنظام المعلوماتي للعدو، بحيث يتم الحصول على المعلومات المخزنة عليه، أو حرمان العدو من استخدامه، أو تحويله إلى نظام يهاجم العدو بحيث يتحول إلى نظام تخريب ذاتي، وهو ما يتحقق نتيجة لتعطيل النظام وإفقاد العدو سلطة التحكم به، وذلك عن طريق الاختراق أو بث الفيروسات الإلكترونية، والتي تحول النظام الرقمي من نظام مساعد إلى نظام معادٍ.

كما تتسم الحرب السيبرانية بعدد من الخصائص يمكن تحليلها على النحو التالي:

١- تتسم الحرب السيبرانية باستخدام أدوات غاية في التطور ومهاجمة أهداف غاية في التطور، وهي الأدوات التي تعد على قمة هرم التطور

المصدر مشار اليه لدى: يحيى ياسين مسعود، **الحرب السيبرانية في ضوء القانون الدولي الانساني**، بحث منشور في المجلة القانونية، ص٨٤، العدد منشور على الموقع الإلكتروني للمجلة

https://jlaw.journals.ekb.eg/article_45192_52d735c1a23cca2bf7dbbe56c4eb6846.pdf

تاريخ الاطلاع ٢٠٢٢/٢/١٥

الإلكتروني[١٣].

٢- تتسم الحرب السيبرانية بانخفاض تكاليفها بصورة تجعلها لا تذكر أمام تكلفة الحروب التقليدية، حيث تعتمد على الأيدي الماهرة والأدوات قليلة التكاليف، بعكس الأسلحة التقليدية التي تستنفذ كثير من ميزانيات الدول١٤.

٣- لا تستغرق الحرب السيبرانية إلا وقت لا يكاد يذكر أمام الوقت الذي تحتاجه الحروب التقليدية لتسفر عن نتيجة، حيث يحدث الهجوم السيبراني في دقائق منتجا أثره على النظام المعلوماتي للعدو، والذي قد يكون أثراً مدمراً للبنية التحتية الإلكترونية الخاصة به، ودون الحاجة إلى التضحية بخسائر في الأرواح أو المعدات أو المنشآت١٥.

٤- بعكس الحرب التقليدية التي غالبا ما يكون فيها المدافع في مركز استراتيجي أفضل، فإن الحرب السيبرانية توفر للمهاجم أفضلية استراتيجية، إذ يختار وقت ومكان الهجوم دون توقع من الخصم الذي يستحيل عليه توفير الحماية الكافية لكافة الأهداف السيبرانية، على عكس

---

[13] مفيد بن علي، **الحرب السيبرانية وتداعيتها على الأمن العالمي**، مقال منشور على الموقع الرسمي للموسوعة الجزائرية للدراسات الاستراتيجية والسياسية https://www.politics-dz.com

تاريخ الاطلاع ٢٠٢٢/٢/١٥

[14] عمر سعد الزيات، **مرجع سابق**، ص١٠٨

[15] أشرف سعد منصور، **التنظيم الدولي للقوة الالكترونية**، المركز القومي للإصدارات القانونية، القاهرة ٢٠١٨، ص ٣٧

الأهداف التقليدية المتوقع الهجوم عليها والتي يسهل إحاطتها بحماية كافية مما يصعب من مهمة المهاجم١٦.

٥- تتجاوز الهجمات السيبرانية أي حدود إقليمية؛ إذ يسهل شنها عبر أي عقبات طبيعية أو جغرافية، وضد أي عدو أي كان موقعه الجغرافي من دولة الهجوم، وبغض النظر عن ميزان القوة العسكرية بين الدولتين، كما أن الأثر المترتب على الحرب السيبرانية هو أثر غير محدود، إذ قد تتسبب هذه الحرب في أضرار لأهداف عسكرية أو مدنية، وسواء كانت أهداف معلنة أو استخباراتية، كما يمكن أن تصيب المنشآت الحيوية في الدولة١٧.

٦- تتسم الحرب السيبرانية بصعوبة الوصول للجهة التي شنتها، إن لم يكن هذا مستحيلاً، نظراً لأن هذا النوع من الهجمات يستحيل رصده قبل وقوعه، كما إنه يتم في زمن يسير دون أن يترك أثراً يشير لفاعله، كما أن أغلب الهجمات السيبرانية يتم اكتشافها مصادفة، وغالباً ما يكون هذا الكشف بعد انتهاء الهجمة وبيان آثارها على هدف الهجوم١٨.

---

[16] احمد عبيس الفتلاوي، **مرجع سابق**، ص ٦٠

[17] شادي عبد الوهاب منصور، **حروب الجيل الخامس - أساليب التفجير من الداخل على الساحة الدولية**، دار العربي للنشر والتوزيع، القاهرة ٢٠٢٠، ص ٩١

[18] عادل عبد الصادق، **الإرهاب الإلكتروني كشكل جديد للصراع الدولي**، مركز الدراسات السياسية والاستراتيجية، القاهرة ٢٠١٧، ص ٦٢

مما سبق يتبين أن الحرب السيبرانية تختلف عن الحرب التقليدية، وتتسم بعدد من الخصائص التي تميزها، وهي خصائص نابعة من طبيعتها المتطورة غير التقليدية، كما تنبع من آثارها وطريقة القيام بها، والتي تختلف كليا عن الحروب التقليدية وأدواتها.

المطلب الثاني: صور الحرب السيبرانية

تتعدد أنواع الحرب السيبرانية، كما تتنوع صورها التى يمكن معها الذهاب إلى أن هذا النوع من الحروب يحتمل ارتكاب عديد من الاجراءات، والتي تقع تحت مسمى الحروب السيبرانية، لذا يتناول هذا المطلب أنواع هذه الحرب وصورها والاثار المترتبة عليها.

اولا: أنواع الحرب السيبرانية

يمكن تقسيم أنواع الحرب السيبرانية على النحو التالي:

١- الحرب السيبرانية الباردة:

غالباً ما يتخذ هذا النوع من الحروب السيبرانية صفة الاستدامة، فهي تتمثل في هجمات متبادلة دائمة منخفضة الشدة، وتستمر لآجال طويلة كنتيجة لخلافات أيدولوجية بين الدولتين، إذ يحمل هذا النوع من الحرب السيبرانية صبغة الخلاف التاريخي، كالصراع بين قوميتين معينتين، أو اتباع ديانتين بعينهما، لذلك تكون هذه الحرب غير معلنة، ويتم اللجوء إليها كبديل عن الحرب التقليدية المعلنة، وتقوم هذه الحرب على اتخاذ أنشطة سيبرانية معينة كالتجسس التجاري والعلمي، وتهديد المصالح التجارية، واختراق المواقع

الرسمية ونشر رسائل من خلالها مناهضة للدولة التي تعرضت للهجوم[١٩].

٢- الحرب السيبرانية متوسطة القوة:

تكون هذه الحرب غالباً مقدمة لحرب تقليدية، أو تسير معها على التوازي، فتعتمد على تصرفات أكثر شدة من الحرب الباردة، مثل: أنشطة التجسس العسكري، وتعطيل الاتصالات بين القوات العسكرية وقياداتها، والشوشرة على الأنظمة الرادارية، والسيطرة على أجهزة الاتصالات السلكية واللاسلكية[٢٠].

٣- الحرب السيبرانية شديدة القوة:

بعكس النوعين السابقين الذين تعرض لهما المجتمع الدولي بالفعل في أحداث سابقة كالحرب الروسية الجورجية، وحرب حلف الناتو على يوغسلافيا السابقة، فإن الحرب السيبرانية شديدة القوة لم تحدث على أرض الواقع، وهي حرب تتمثل في النشوب بصورة مستقلة عن الحرب التقليدية، وتستهدف السيطرة على كافة المواقع الإلكترونية والنظم الخاصة باستخدام الأسلحة لدى الخصم، وإخضاعها لسيطرة الدولة المهاجمة، مع استخدام الأسلحة ذاتية التشغيل ضد المنشآت المادية للدولة المعادية، مع توجيه ضربات إلكترونية شديدة للبنية التحتية للعدو بما يحقق تدمير المنشآت

---

[19] نوران شفيق، **أثر التهديدات الإلكترونية على العلاقات الدولية – دراسة في أبعاد الأمن الإلكتروني**، المكتب العربي للمعارف، القاهرة ٢٠١٦، ص ١٢٢

[20] عباس بدران، **الحرب الإلكترونية – الاشتباكات في عالم المعلومات**، مركز دراسات الحكومة الإلكترونية، بيروت ٢٠١٢، ص ٩٧

الحيوية كالسدود ومحطات توليد الطاقة، وذلك بما يحقق قدر كبير من التدمير الشامل في الدولة التي تتعرض لمثل هذا الهجوم٢١.

وكما تتعدد أنواع الحروب السيبرانية تتعدد ايضا صور شن هذه الحروب، فالحرب السيبرانية كالحرب التقليدية تتعدد أدواتها وأسلحتها وأهدافها، مما يعني أن صور هذه الحرب لا يمكن حصرها إلا أنه يمكن ذكر عدد من هذه الصور وذلك على النحو التالي.

١- القنابل الرقمية:

هي نوع من الشفرة المعلوماتية التي يتم إدخالها خلسة ضمن النظام الرقمي المستهدف، بحيث لا يمكن التفرقة بينها وبين باقي البرامج المخزنة على النظام الرقمي، ويتم توزيع هذه الشفرة على كافة برامج النظام بحيث تتداخل أجزائها مع أجزاء الملفات الرئيسية، ولا تعيد تجميع نفسها والبدء في التأثير بفاعلية إلا بناءً على أمر رقمي يصدر لها من المهاجم، وفي هذه اللحظة تنفجر لتدمر كافة الملفات المخزنة على النظام، ويسود استخدام نوع مبسط من هذه القنابل في البرامج التجارية التي تتطلب سداد اشتراك دوري، حيث يتضمن البرنامج مثل هذه القنبلة المعدة للانفجار في نهاية فترة الاشتراك بصورة محدودة من شأنها تدمير البرنامج فقط، إلا لو أرسل البائع لها شفرة تمنعها من الانفجار في هذا الموعد، وهو ما يحرص عليه دورياً

---

[21] محمد سعادي، **أثر التكنولوجيا المستحدثة على القانون الدولي العام**، دار الجامعة الجديدة، القاهرة ٢٠١٤، ص ٩٣

طالما يتم سداد الاشتراكات بانتظام٢٢.

٢- هجوم البرمجيات الخبيثة او الفيروسات (malware attack):

هي برامج رقمية الهدف منها تخريب النظم المعلوماتية أو فتح الثغرات الإلكترونية لاختراقها والوصول للمعلومات المخزنة عليها، كما تملك هذه البرامج القدرة على استنساخ نفسها ذاتية بحيث تنتشر في النظام المعلوماتي بأكمله في مدة يحددها المهاجم، ولها القدرة على تحويل البرامج الأصلية في النظام المعلوماتي لتلبي رغبات المهاجم، سواء كانت الرغبات هي النسخ أو المحو أو التجسس على هذه البرامج، وتملك الفيروسات قدرة كبيرة على الاختفاء والاندساس وسط البرامج الأصلية للنظام، بحيث تسيطر على النظام بالصورة التي صنع الفيروس من أجلها٢٣.

حيث يقوم المهاجمون (hackers) عبر الإنترنت بإنشاء البرامج الضارة(viruses) باستخدام لغات البرمجة المختلفة وكتابة الأكواد طبقاً لها وحسب الهدف من زرع تلك البرمجيات واستخدامها وبيعها لأسباب عديدة مختلفة، ولكنها غالبًا ما تستخدم لسرقة المعلومات، سواء أكانت معلومات مالية أو اقتصادية أو عسكرية. على الرغم من دوافعهم المختلفة، يركز المهاجمون السيبرانيون دائمًا تكتيكاتهم وتقنياتهم وإجراءاتهم على الوصول إلى بيانات الاعتماد والحسابات المميزة للشخصيات القيادية والهامة بالدولة

---

[22] عمار عباس الحسيني، **جرائم الحاسوب والانترنت – الجريمة المعلوماتية**، منشورات زين الحقوقية، بيروت ٢٠١٧، ص ١٤٠

23 عمار عباس الحسيني، مرجع سابق، ص ١٤٤

أو المديرون التنفيذيون بالشركات.

والفيروسات كما عرفها المركز القومي للحاسبات في الولايات المتحدة الأمريكية، هي: "برامج مهاجمة تصيب أنظمة الحاسب بأسلوب يماثل إلى حد كبير الفايروسات الحيوية التي تصيب الإنسان"، حيث أن أول تصور ذكر لفايروس إلكتروني كان عن طريق الأستاذ الدكتور " فريد كوهن " في جامعة كاليفورنيا الأمريكية بمحاضرة تحت عنوان آمن الحاسب الآلي عام ١٩٨٣. ومن أهم السمات المميزة للبرمجيات الضارة بشكل عام تتركز في قدرتها على الاختفاء داخل جهاز الضحية، وقدرتها على الانتشار السريع بين ملفات نظام تشغيل الحاسوب، وقدرتها على إتلاف ملفات نظام التشغيل جزئياً أو كلياً.

٣- هجوم حجب الخدمة (denial of service):

تهدف هذه الصورة من الحرب السيبرانية إلى حرمان المستفيد من الخدمة الرقمية من التمتع بهذه الاستفادة، حيث يتم الهجوم بغرض قطع الشبكة المعلوماتية عن المستفيدين منها، بحيث تحرم الدولة من استخدام برامجها الرقمية الرسمية مما يوقف تدفق الاتصالات والمعلومات فيها٢٤.

ويتم هذا الهجوم عن طريق إغراق الخادم الخاص بالضحية بحركة المرور، مما يجعل موقع الويب أو المورد غير متاح، وهجوم حجب أو رفض الخدمة الموزع له نوعان(dos attack) والأخر (ddos attack)

24 عباس بدران، مرجع سابق، ص١١٣

كل منهما يعمل بطريقة مختلفة. (٢٥)

٤- برامج الدودة (worms):

هي نوع خاص من الفيروسات هدفه الانتشار عبر الشبكة المعلوماتية بأكملها ليصيب كافة الاجهزة المتعاملة بها، كما تملك هذه البرامج القدرة على الانقسام والتكاثر حتى تغطي أكبر قدر ممكن من الأجهزة والنظم المعلوماتية في أقل مدة ممكنة، وغالباً ما يتم زرع هذا النوع من البرامج من خلال إرسال الرسائل الإلكترونية (phishing mails)، حيث يُعدّ فتح الرسالة الإلكترونية إذناً للبرنامج ببدء عمله التخريبي، والبدء في التكاثر والانتشار الذي ما إن يصل لدرجة معينة حتى يبدأ في ممارسة النشاط الذي صنع من أجله أي كان٢٦.

وعلى هذا فإن الحرب السيبرانية برغم حداثتها إلا إنها استطاعت أن تفرض نفسها على ساحات النزاعات الدولية، وهو الأمر الذي نتج عن مدى تنوعها وسرعة القيام بها، وشدة تأثيرها، كما يمكن إيعاز هذه الأهمية إلى محدودية تكاليفها وعدم احتياجها لجهود أو معدات كبيرة، إذ يمكن شنها بأبسط الإمكانات وعن طريق عدد محدود من الأفراد ودون تكلفة تذكر مقارنة بالحرب التقليدية، لذا تسعى أغلب الدول اليوم لتطوير إمكانياتها السيبرانية، ودعم قوتها العسكرية بالكفاءات والأدوات التي تمكنها من شنّ هذا النوع من الحروب.

---

25 الموقع الإلكترونى التعليمي www.cisco.com

([26]) خالد وليد محمود، **الهجمات عبر الانترنت – ساحة الصراع الإلكتروني الجديد**، المركز العربي للأبحاث ودراسة السياسات، الدوحة ٢٠١٣، ص ٦٣

ثانياً: الآثار المترتبة على الهجمات السيبرانية:

قد يؤدي الافتقار في الحفاظ على الأمن السيبراني للدول وقطاعاتها ومرافقها وتحقيق مستويات الأمان المطلوبة وفقاً للمعدلات المحددة طبقاً للدراسات والأبحاث الموثقة من الخبراء والمختصين بمجال الأمن السيبرانى إلى جعل الفضاء السيبرانى عرضه إلى هجمات سيبرانية ضد شبكات المؤسسات الأمنية والعسكرية وغيرها من المؤسسات الحيوية لتلك الدول وذلك من أجل السيطرة عليها.

ومن الجدير بالذكر صعوبة تحديد نطاق الهجمات السيبرانية لأنها واسعة وتطول في ظل التطور التقني الحالي كافة المجالات مما يعطيها القدرة على التأثير في حركات الملاحة الجوية والبحرية محدثة بعض الخلل بأنظمة الملاحة والعبث في أنظمة التوجيه المعتمدة على المواقع الجغرافية الإلكترونية وأيضاً قد تحدث تشويش على أنظمة الدفاع الجوى للدول والطائرات وإدخال التعديلات الخاطئة بمسرات أجهزة التحكم، كما تسطيع الهجمات السيبرانية إصابة أنظمة المرافق العامة وتعطيلها مما يأثر على أنظمة تشغيل الطاقة ومحطات توزيع الكهرباء أو شبكات الاتصالات، بل والأكثر فقد تطول المنشآت الحيوية بالدول من محطات طاقة نووية أو محطات الوقود أو سدود مياة وسنتناول فيما يلي الآثار الناتجة عن الهجمات السيبرانية في بعض المجالات:

- **في مجال البنية التحتية:**

عندما تبدأ الدول أو التنظيمات شنّ الهجمات السيبرانية فأول ما يتبادر في أذهانهم هو تدمير البنية التحتية للدولة المستهدفة لشل أجهزتها ومؤسساتها وإرباك الأوضاع الداخلية لها وإحداث الإضرابات مستهدفه أنظمة التحكم المركزية وموارد الطاقة والتمويل والاتصالات والنقل ومرافق المياه فكلها أهداف أساسية للبنية التحتية.

- **في المجال الاقتصادي:**

إن ثورة تكنولوجيا المعلومات والطفرات الحديثة بمجال الاتصالات والتصنيع ودخول أنظمة الذكاء الاصطناعي في سوق العمل والعديد من الأنشطة والمجالات؛ مما أظهر منافسة قوية وفعالة في قطاع الصناعة والإنتاج وزيادة الناتج المحلى وظهور فرص عمل جديدة سواء من المنازل بالعمل أونلاين أو العمل الحر و التجارة الإلكترونية مما ساعد في تخفيض البطالة والحد من تأثير الأزمات كما حدث بأزمة تفشى وباء كورونا، فإصابة هذا المجال بهجوم سيبراني سيؤدى حتماً إلى صعوبات كثيرة من تدهور اقتصادي وزيادة البطالة؛ ونظراً لأن القطاع المالي والمصرفي جزءًا هام في الاقتصاد فسوف يتأثر أيضاً كما حدث في العديد من الهجمات السيبرانية التي أحدثت خللاً بأنظمة التحويلات بالبنوك وسرقة مبالغ مالية كبيرة من بعض الحسابات البنكية مما يؤدى إلى خروج المستثمرين من هذه الدولة.(٢٧)

([27]) Lyons, Marty. United States. Homeland Security. Threat Assessment of Cyber Warfare. Washington, D.C., 2005. Web

- **في المجال الصحي:**

أثمر البحث العلمي عن نتائج كثيرة في شتى المجالات وخاصة في مجال الصحة العامة مما أتاح دخول أنظمة التكنولوجيا والتقنيات المختلفة الحديثة وأنظمة الذكاء الاصطناعي في تشخيص الحالات المرضية وإجراء العمليات الدقيقة وتحديد أنواع العلاج الأكثر فاعلية وملائمه لحالات المرضى، كما ساعد الذكاء الاصطناعي في التنبؤ بالأمراض المحتمل الإصابة بها لكل شخص عن طريق دراسة تاريخه المرضى ومعرفة روتينه اليومي ونظامه الغذائي، فأصبح هناك قاعدة بيانات ضخمة تضم الملفات المرضية للأشخاص وملفات التأمين الصحي كما تطورت المستشفيات بتعديل أنظمتها وإدخال الأنظمة الذكية فإذا تعرضت هذه المنظومة الصحية لهجمات سيبرانية ستدمر منظومة الرعايا الصحية وقد ينتج عن هذا الخلل عدم المقدرة على السيطرة على تفشى الأوبئة و الأمراض المزمنة ومن ثم حدوث العديد من الوفيات.

- **في مجال الحفاظ على البيئة:**

نتيجة لتطور الصناعات وتعددها وبعض الممارسات الخاطئة من البشر تزايد التلوث البيئي في العالم أجمع وتتبع ذلك تغيرات مناخية أثرت على مجالات عديدة في حياتنا مثل: الصحة والغذاء وازدياد درجات الحرارة وزيادة الحرائق بالغابات وغيرها من الأثار مما دعي جميع دول العالم والمنظمات الدولية المختصة إلى سرعة التحرك لمجابهة هذا الخطر ومعالجة ومن أهم الخطوات الهامة والمؤثرة في مجابهة هذا الخطر قيام منظمة الأمم المتحدة بمشاركة من جميع الدول في عقد قمم المناخ للتوصل لأفضل السبل للمجابهة.

وفي إطار هذا التعاون ظهر دور جمهورية مصر العربية الهام في استضافة مؤتمر الأمم المتحدة للتغير المناخي السابع والعشرين (cop27) بمدينة شرم الشيخ بالفترة من ٢٠٢٢/١١/٦ حتى ٢٠٢٢/١١/١٨، حيث قامت الدولة بجهود عظيمة لتنظيم تلك القمة المناخية والحرص على أن يؤتى ذلك المؤتمر ثماره من حيث التنسيق بين الدول الحاضرة وتذليل كافة الصعاب وعرض الأفكار البناءة والمقترحات في سبيل حماية دول العالم أجمع من تلك المخاطر حيث ظهر أثر مجهودات الدولة الواضح في نجاح القمة المناخية والوصل لنتائج هامة ومؤثرة.

كما نلاحظ أن التطور التقني و التكنولوجيا لها أثر بالغ في الحفاظ على البيئة وحمايتها من التلوث وباستغلال تلك التكنولوجيا وأنظمة الذكاء الاصطناعي أصبح من الممكن معرفة الأماكن المعرضة للتلوث البيئي وكذا قياس درجاته ومصدره بل والأكثر حيث ساعد الذكاء الأصطناعى في التنبؤ بأماكن حدوث التلوث وإتجاه كما تساعد تلك الأنظمة في دقة استشعار التلوث الأشعاعى أو وجود تسرب نووي وعلية يمكن مواجهته بسرعة والسيطرة عليه، ومما سبق يتضح إذا تعرضت هذه المنظومة البيئية والبالغة الأهمية لهجوم سيبراني، سيأثر ذلك تأثير على الدولة المعرضة للهجوم وإلحاق أضرار بالغة الخطورة بها.

- **في المجال العسكري:**

وهو من أكثر المجالات خطورة وحساسية لكونه هو خط الدفاع عن

الدول ونظراً لاعتماد التطورات بمجال التسليح والدفاع على التقنيات الحديثة والتكنولوجيا المتطورة فتأثير الهجمات السيبرانية على المجال العسكري قد يتمثل في قطع الإشارات وموجات التواصل بين السكنات العسكرية وقادة الجيش ويؤثر على إعطاء الأوامر الخاطئة للأسلحة ذاتية التوجيه أو الطائرات ذاتية القيادة بتعديل إحداثيات الأهداف وتوجيهها لضرب أهداف داخل الدولة نفسها؛ مما يؤدى إلى نفس العواقب الوخيمة الناجمة عن الحرب المادية التقليدية كمقتل مواطنين من العسكريين أو المدنيين وسقوط العديد من الضحايا.

ونتيجة لما سبق عرضه يظهر لنا نتائج الهجمات السيبرانية على الدول وما قد يلحق بها من هلاك وتدمير وسقوط الضحايا والتي لا تقل أهمية أو تأثيراً عن الحروب التقليدية وجرائم العدوان وهو ما تأباه مبادئ الإنسانية ومبادئ القانون الدولي وكافة المواثيق والمعاهدات والاتفاقيات الدولية وعمل منظمة الأمم المتحدة وغيرها من المنظمات الدولية وأجهزتها وكما جاء بنظام روما الأساسي لإنشاء المحكمة الجنائية الدولية للحفاظ على الإنسان وحمايته من الجرائم المختلفة الداخلة باختصاصها.

المبحث الثاني: التكيف القانوني للحرب السيبرانية فى ضوء القانون الدولي

تمهيد وتقسيم:

إذا كان الفقه يعتبر أن القانون الدولي قد نشأ كنتيجة طبيعية للحروب، فإن هذا القانون هو دائمًا عرضة للتطور بتطور أنواع وأساليب هذه الحروب، لأن استفادة الحروب من هذا التطور دون قواعد القانون الدولي من شأنه أن يعجز قواعد هذا القانون عن إيجاد التنظيم الملائم لهذه التكنولوجيا المستحدثة، كما يصنع فجوة بين النظرية والتطبيق تجعل من المواجهة القانونية لهذه الظاهرة مواجهة مستحيلة، الأمر الذي يصنع أمام القانون تحدي من نوع جديد يستلزم معه أن يبدأ المشرع الدولي في إعادة هيكلة المواد التي تنظم الحروب[٢٨].

وتتمثل أهم التحديات التي تواجه القانون الدولي في شقين هما: تحديد الطبيعة القانونية للحرب السيبرانية من جهة، ومدى إمكانية تطبيق مبادئ وقواعد القانون الدولي والمتمثلة في الحرب والعدوان من ناحية أخرى على هذا الشكل المستحدث من الحرب، حيث يواجه القانون الدولي اليوم فراغ تشريعي ترتب عليه الافتقار لقواعد قانونية من شأنها تنظيم الحرب

---

[28] علي الرفاعي، **الحروب السيبرانية وتداعيتها على الأمن والسلم الدوليين**، بحث منشور في المجلة العلمية الأكاديمية، عدد ٥٧، كلية العلوم السياسية جامعة بغداد، ٢٠١٩، ص ٩٩

السيبرانية[٢٩].

وعلى هذا تنقسم الدراسة في هذا المبحث إلى مطلبين:

المطلب الأول: الطبيعة القانونية للهجمات السيبرانية

المطلب الثاني: مدى انطباق مفاهيم الحرب والعدوان على الهجمات السيبرانية

المطلب الأول: الطبيعة القانونية للهجمات السيبراني

كان انتشار استخدام الدول للفضاء الإلكتروني في شن الحروب السيبرانية واللجوء لها في دعم عملياتها العسكرية أثناء النزاعات المسلحة، سبباً في وضع قواعد القانون الدولي والمشرع الدولي نفسه أمام اختبار يتمثل في تحديد الطبيعة القانونية لهذا النوع من الحروب، خاصة مع اعتماد المشرع الدولي في مواجهة الحروب على اتفاقيتي لاهاي ١٨٩٩-١٩٠٧، واتفاقيات جنيف الأربعة ١٩٤٩، والبروتوكولان الإضافيان ١٩٧٧، وهي المواثيق الدولية التي لم يكن للحرب السيبرانية وقت عقدها أي وجود، وهو ما يعني أن هذا النوع من الحروب لم ينظم عن طريق أحكام خاصة ولا

---

[29] حسن فياض، **الهجمات السيبرانية من منظور القانون الدولي الإنساني**، مقال منشور على الموقع الرسمي للجيش اللبناني
https://www.lebarmy.gov.lb/ar/content
تاريخ الاطلاع ٢٠٢٢/٢/١٦

سبيل لمواجهته عن طريق قواعد القانون الدولي من الناحية النظرية[٣٠].

وجدير بالذكر أنّه وبرغم هذا الفراغ التشريعي وعلى ضوء قانون الحرب، فإنه يمكن الاستناد الى المادة ٣٦ من البروتوكول الإضافي الأول لاتفاقيات جنيف والتي نصّت على أن تلتزم الأطراف المتعاقدة عند دراستها أو تطويرها أو اقتنائها لسلاح جديد أو أحد أدوات أو أساليب الحرب، بأن يتحقق مما إذا كان تصرفه حيال السلاح المعني محظورًا في بعض أو كافة الأحوال بمقتضى هذا البروتوكول أو بمقتضى أي من قواعد القانون الدولي التي يلتزم بها أطراف البروتوكول، وهي المادة الاحتياطية التي تضع إطار عام لتنظيم استخدام الوسائل والأساليب المستحدثة في النزاعات المسلحة[٣١].

ويوضح حكم المادة ٣٦ أنه في ضوء قانون الحرب، تلتزم الدول التي تملك أسلحة مستحدثة أو تعمل على تطوير أسلحة تقليدية لاستخدامها في أسلوب قتال مستحدث، أن تحدد أولاً مشروعية استعمال هذه الأسلحة، كما يستنتج من استقراء هذا النص أن كل قواعد قانون الحرب هي قواعد قابلة للتطبيق على مستحدثات القتال وأساليبها، ففي حال خلو النظام التشريعي من النص الخاص يتم تطبيق النص العام، وهو المبدأ القانوني المعروف في القانون الدولي والقوانين الوطنية كما يستفاد من المادة ٣٦ أن القانون الدولي لا يحظر اقتناء أو تطوير أو حيازة الأسلحة الحديثة، واعتماد أساليب مستحدثة للحرب لم يسبق تنظيمها بموجب قواعد القانون الدولي، إلا إنها

---

[30] نوران شفيق، **مرجع سابق**، ص٦٧

[31] ريماس صعب، **المواجهة القانونية للأسلحة غير التقليدية في القانون الدولي**، منشورات زين الحقوقية، بيروت ٢٠٢١، ص ٣٤

تلزم الدول بالمراجعة القانونية عند استخدام سلاح من نوع جديد وهو الوضع الذي يعرف بالمطابقة القانونية مع القانون الدولي٣٢.

فحق أطراف النزاع في اختيار الوسائل والأساليب المستخدمة في الحرب هو: حق مقيد باحترام قواعد القانون الدولي المنظمة للنزاعات المسلحة، وأهم هذه القواعد هو حظر استخدام الأسلحة التي تسبب تدميراً هائلاً وآلاماً زائدة، دون داعي واقعي لذلك، أو دون ضرورة لهذا الاستخدام، وخاصة في مواجهة المدنيين٣٣.

وبالنظر للحروب السيبرانية نجد أنها يمكن أن تستهدف القطاعات العسكرية والأمنية والصناعية والطبية والتعليمية، وغيرها من القطاعات، وذلك في إطار النزاعات المسلحة، إذ تطال الحرب السيبرانية قطاعات خدمية مدنية فرض القانون الدولي لها قدر من الحماية تناسب مهامها الوظيفية، وذلك فضلاً عن الأعيان المدنية مثل: السدود ومحطات الطاقة وتحلية المياه والمحمية أيضًا بموجب قواعد قانون الحرب٣٤.

---

[32] عمار حميد عبد الأمير الحسني، **حماية الممتلكات ومبدأ المسئولية عند الحماية وعلاقته بجرائم الحرب**، دار الكتب والدراسات العربية، القاهرة ٢٠١٩، ص ٣٦

[33] أحمد مبخوتة، **إعمال المسئولية الجنائية الدولية عن جرائم الحرب**، دار الفكر الجامعي، القاهرة ٢٠٢٠، ص ١٨

[34] صلاح عبد الرحمن الحديثي، **التفصيل الشامل لتطور القواعد القانونية الخاصة بالحرب السيبرانية**، المجموعة العلمية للنشر والتوزيع، القاهرة ٢٠٢١، ص ٤٤

كما توفر المواد ٤٨، ٥١ فقرة ٢، ٥٢، ٥٥، ٥٦، الحماية للمدنيين سواء أشخاص أو أعيان، وللبيئة، وللأشغال الهندسية، وللمنشآت التي تضم قوى خطرة، وهي الحماية التي تعني أن حق الأطراف المتحاربة في اختيار السلاح المستخدم في المعارك ليس حقاً مطلقاً، لكنه حق مرهون باحترام قواعد القانون الدولي، حيث يقر هذا القانون بضرورة قبول حد من الخسائر في الأرواح والأعيان من جانب القوات المتحاربة وذلك كنتيجة طبيعية للحرب، إلا أن هذا الحد لا يجب أن يتعدى الأفراد والمنشآت والمعدات العسكرية[٣٥].

وإسقاطا على الحرب السيبرانية نجد أن هناك فضاءً سيبرانياً واحداً فقط يضم القوات العسكرية مع السكان المدنيين دون أن يمكن الفصل بينهم في الاستهداف السيبراني، حيث يبرز التحدي من خلال اقتصار توجيه هذا النوع من الحروب ضد الأفراد والأهداف العسكرية فحسب، وتحييد الأهداف المدنية المتمثلة في الأشخاص والأعيان والتي تعد أهدافاً محمية بموجب القانون الدولي، كما يجب على الدول المتنازعة أن تحرص عند اللجوء للحرب السيبرانية على استهداف المواقع العسكرية دون غيرها، مع الوضع في الاعتبار أن خصائص الحروب السيبرانية من الناحية التقنية تمنحها قدرة كبيرة على أن يتم توجيهها بدقة لتستهدف منشآت عسكرية فقط[٣٦].

فالقاعدة التي تحكم الحرب السيبرانية أنه لا يجوز لها استهداف

---

[35] ريماس صعب، **مرجع سابق**، ص ٤٨

[36] نسرين عبد الحميد نبيه، **تطور أساليب الحروب وظهور أنواع جديدة تتناسب والتكنولوجيا الحديثة**، مكتبة الوفاء القانونية، القاهرة ٢٠٢١، ص ٥٢

المدنيين إلا في الحالة التي تتأكد فيها مشاركتهم بصورة مباشرة في الأعمال القتالية، مع الالتزام بزمن هذه المشاركة بحيث تنسحب عنهم صفة الهدف المشروع في حالة انتهائهم من المشاركة في العمل العسكري المباشر؛ بحيث يخسر المدنيين الحماية التي كفلها لهم القانون الدولي ضد الهجمات السيبرانية إذا ما شاركوا في حروب سيبرانية لصالح دولهم، كما تخسر المنشآت المدنية الحماية المكفولة لها إذا ما استخدمتها القوات العسكرية كمنصات الكترونية لشن الحروب السيبرانية[٣٧].

وبناءً على ما سبق توضيحه، فإن محاولات التمييز بين العسكريين والمدنيين خلال شن الحرب السيبرانية هي محاولات غاية في التعقيد، إذ أن المهاجم غالباً ما يبعد عن مكان الهجوم المستهدف بمئات وربما آلاف الأميال، مما يفقده القدرة على تمييز طبيعة الخصم والمنشأة المستهدفة[٣٨].

وعلى هذا فإن القواعد العامة في القانون الدولي تحظر أي هجمات من أي نوع لا تميز في آثارها أو استهدافها ما بين الهدف العسكري والمدني، أما الخسائر العرضية فيسمح بها القانون الدولي في حدود، على اعتبار أن العمل القتالي هو عمل خطر بطبيعته، ومن شأنه أن يرفع احتمالات تعرض المدنيين للمخاطر، ففي حال كانت الحرب السيبرانية موجهة إلى هدف عسكري بحت، فإنها في هذه الحالة تعد حرباً مشروعة

---

[37] عمار حميد عبد الأمير الحسني، **مرجع سابق**، ص٤٢

[38] احمد عبد المعطي حسين، **الحرب وقيودها الأخلاقية – مقارنات بين الفقه الإسلامي والقانون الدولي الإنساني**، مركز الحضارة لتنمية الفكر الإسلامي، برلين ٢٠١٨، ص ١٤٦

حتى وان كان هناك احتمال لتعرض المدنيين لمخاطر عرضية، إلا أن صفة المشروعية تنزع عنها في حالة كانت حرب عشوائية لا يمكن أن تفرق في هدفها بين الأهداف العسكرية والمدنية، وخاصة في ظل طبيعة الفضاء السيبراني الذي يتسم بالارتباط بين الشبكات ونظم المعلومات وأجهزة الحاسب الآلي، مما يجعل هناك صلة الكترونية بين النظم العسكرية والنظم المدنية سواء أكانت نظم طبية أو تعليمية أو مصرفية[٣٩].

وحلاً لهذه الاشكالية اعتبر الفقه الدولي أن الأعيان والمنشآت كافة ذات الطبيعة المزدوجة والتي تخدم القطاعات العسكرية والمدنية هي أهداف عسكرية، ولذلك لا تتمتع هذه المنشآت بالحماية المقررة للأعيان المدنية، وهو الاتجاه الذي حرص على ألا تستخدم القوات العسكرية أعيانا مدنية في العمليات العسكرية، وقد أسس هذا الفقه رأيه على أن اتفاقية جنيف قد أقرت وجود بعض الضرورات الحربية والتي قد تمليها ظروف الحرب، وعلى القوات المتحاربة قبول هذه الضرورات، لذا فقد بررت اتفاقيات جنيف المتعددة هذه المخاطر إذ كان لها ضرورات حربية تبررها[٤٠].

إلا أن فكرة الضرورة الحربية لا تعني تجاوز الأهداف المشروعة للحرب، وهي إضعاف القدرة العسكرية للخصم بالطرق التي لا تتنافى مع قواعد الحرب، سواء كانت هذه القواعد تعاهدية أو عرفية، وفي الإطار

---

[39] اسامة عرفات، **القواعد الحامية للمدنيين زمن الحرب في القانون الدولي العام وشريعة الاسلام**، دار الإجادة، القاهرة ٢٠١٧، ص ٩٨

[40] نسرين عبد الحميد نبيه، **مرجع سابق**، ص ٦٦

الضروري لرد العدوان والحفاظ على كيان الدولة[٤١].

بناءً على ما تقدم، يرى الباحث أن مبدأ الضرورة العسكرية يتيح شن الحرب السيبرانية ضد الأهداف العسكرية كهدف رئيسي، إلا أن هذا لا يمنع مهاجمة المدنيين أشخاص وأعيان إذا كان هؤلاء المدنيين مساهمين بصورة مباشرة في الأعمال القتالية وتحقيق مميزات للقطاع العسكري، وفي هذه الحالة يجب على المهاجم أن يتخير كهدف للحرب السيبرانية المنشآة التي يمثل الهجوم عليها تحقيق أقل قدر من الأضرار للمدنيين.

وإذا كان الفقه قد اتفق على مشروعية الحرب السيبرانية مع التزام القوات المتحاربة بعدم استهداف منشآت مدنية إلا في حالات الضرورة العسكرية وذلك كطبيعة قانونية، فإن هذا الفقه قد اختلف في تحديد الطبيعة الواقعية للحرب السيبرانية؛ إذ رأى البعض أنها سلاح قتالي مستحدث، ويعد أحد الوسائل الحديثة التي تلجأ لها القوات المتحاربة لتعزيز احتمالات تحقيق النصر، بينما رأى فقه آخر أنها نوع من الحروب المستقل بذاته، ولا يدور مع الحرب التقليدية، إذ يمكن شن هذا النوع من الحروب على سبيل الاستقلال، ومهاجمة الأهداف المعادية هجوماً سيبرانياً دون غيره من أنواع الهجوم والقتال، فالحرب السيبرانية عند هذا الفقه ليست مجرد استخدام لسلاح معين، وإنما هي حرب كاملة ينطبق عليها قواعد قانون الحرب؛ بحيث يؤدي تجاوز هذه القواعد خلالها إلى مسئولية الدولة المتجاوزة بموجب القانون

---

[41] احمد عبد المعطي حسين، **مرجع سابق**، ص ١٥٢

الدولي٤٢.

ويرى الباحث أن شن حرب سيبرانية رسمية معلنة على سبيل الاستقلال هو افتراض لم يتحقق الآن ويستبعد تحققه، لذا فالأكثر واقعية اعتبار الحرب السيبرانية نوع من الأسلحة المستحدثة ذات التأثير الشامل، وهو الاختيار الذي يسمح للقانون الدولي أن يواجه هذا النوع من الحروب على اعتبار أنها استخدام لأسلحة غير تقليدية، أما اعتبارها حرب مستقلة فيؤدي لوجود فراغ تشريعي في القانون الدولي يمنع قواعد هذا القانون من تنظيم هذه الحرب.

المطلب الثاني: مدى انطباق مفاهيم الحرب والعدوان على الهجمات السيبرانية

لا يعد إغفال القانون الدولي عن النص على الحرب السيبرانية بصورة محددة، إغفالاً منه عن تنظيم هذا النوع من الحروب؛ إذ يتسع القانون الدولي بقواعده التعاهدية والعرفية ليتمكن من سحب هذه القواعد على الحروب السيبرانية، وهو ما يعني شمول قواعد القانون الدولي لهذا النوع من الحروب، وخاصةً تلك القواعد الخاصة بتنظيم استخدام الأسلحة لا سيما غير

---

[42] زهراء عماد، **المسئولية الدولية عن شن الهجمات السيبرانية**، دار السنهوري للطباعة والنشر، بغداد ٢٠١٦، ص ٣١

التقليدية منها٤٣.

حيث نظم القانون الدولي استخدام الأسلحة بأنواعها، وذلك من خلال اتفاقية حظر أو تقييد استعمال أسلحة تقليدية معينة يمكن اعتبارها مفرطة الضرر أو عشوائية الأثر، وهي الاتفاقية التي تنظم استخدام أي سلاح مستحدث، أو أي نوع من الحروب الحديثة التي طرأت دون أن تجد لها تنظيماً مباشراً في القانون الدولي، وهي الاتفاقية التي أشارت إلى أن حق الأطراف في النزاعات المسلحة في اختيار أساليب ووسائل الحرب لا يمكن عده حقاً غير محدود؛ إذ يحظر استخدام أسلحة تسبب أضراراً مفرطة أو آلاماً لا داعي لها٤٤.

وفي سياق إسقاط مفهومي الحرب والعدوان على الحرب السيبرانية، نجد أن الحرب في القانون الدولي العام التقليدي هي: نزاع مسلح بين قوتين عسكريتين من دولتين مختلفتين، إذ تدافع الدول المتحاربة من خلال عن حقوقها ومصالحها، ولا يمكن اطلاق مصطلح الحرب إلا على النزاع المسلح

---

[43] مصطفى نعوس، **حقوق والتزامات الدول في الحرب المعلوماتية**، بحث منشور في مجلة دراسات علوم الشريعة والقانون، مجلد ٤٠ ملحق ٤، الجامعة الأردنية، عمان ٢٠١٣، ص ٧٨٤

[44] للاطلاع على النص الكامل للاتفاقية راجع الموقع الرسمي للجنة الدولية للصليب الاحمر

https://www.icrc.org/ar/doc/resources/documents/misc/62sd4j.htm

تاريخ الاطلاع ٢٠٢٢/٢/١٦

بين الدول[٤٥].

أما الفقه الحديث فقد تغاضى عن بعض القواعد في تحديده لمفهوم الحرب، حيث قام هذا الفقه بالتوسع في مفهوم الحرب ليتضمن أي نزاع جماعي مسلح، حتى لو لم تتوفر له عناصر التعريف الكلاسيكي من تمتع الجماعة المسلحة بصفة الدولة، كما أصبحت الحرب الأهلية التي تنشب داخل نفس الدولة تندرج تحت مسمى الحرب لدى هذا الفقه[٤٦].

وبغض النظر عن اتباع أي من الرأيين نجد أن الحرب السيبرانية تتماشى مع مضمون الرأيين، فسواء التزمنا التعريف التقليدي واعتبرنا أن الحرب لا تقوم إلا بين الدول، فإنه يتصور أن تهاجم الدول بعضها سيبرانياً، فتستهدف بهجومها الإلكتروني المنشآت والأهداف الحيوية التي يمتلكها العدو، أما إذا تماشينا مع الفقه الحديث نجد إنه يتصور أن تلجأ الجماعات المسلحة غير الرسمية لهذا النوع من الحروب، كما يتصور أن تتم خلال الحرب الأهلية إذا قامت جماعة بالهجوم السيبراني على منشآت ومعدات الجماعة المعادية، لذا فيمكن منطقياً وتماشياً مع قواعد القانون الدولي اعتبار الحرب السيبرانية نوعاً من التصرفات التي تخضع لتعريف الحرب.

---

[45] تمارا برو، **استخدام الأسلحة غير التقليدية في القانون الدولي العام**، دار المنهل اللبناني للطباعة والنشر، بيروت ٢٠١٥، ص ٣٠

[46] لفقير بولنوار بن الصديق، **جرائم الحرب في ضوء أحكام القانون الدولي**، دار الأيام للنشر والتوزيع، عمان ٢٠١٧، ص ٢٢

أما عن مدى تماشي مفهوم العدوان مع الحرب السيبرانية فيستلزم أولاً الوقوف على ماهية العدوان، وهو المفهوم الذي شكّل إحدي المسائل الشائكة التى أثارت جدلاً واسعاً لسنوات طويلة في مختلف المحافل الدولية والإقليمية، الأمر الذى تمخض عنه ظهور العديد من المحاولات الفقهية والدولية لوضع تعريف لتلك الجريمة٤٧.

وبالرغم من رفض لجنة حقوق الإنسان تحديد تعريف دقيق لجريمة العدوان إلا أن قرار الجمعية العامة للأمم المتحدة رقم ٣٣١٤ المؤرخ في ١٩٧٤/١٢/١٤، توصل إلى تحديد تعريف لها فكان بذلك من أهم الخطوات الإيجابية في طريق تحديد أركانها والحد من وقوعها وتجنب الإنسانية ويلاتها، وبناءً عليه ذهب بعض الفقه إلى تعريف العدوان على أنه استخدام القوة المسلحة سواء بشكل مباشر أو غير مباشر، ويستند هذا الفريق في حجته إلى خلو ميثاق الأمم المتحدة من تعريف للعدوان واستخدام الميثاق مصطلحات أخرى متداخلة مع بعضها البعض إلا أنها قد تكون بصورة أو بأخرى ركناً من أركان العدوان مثل استخدام القوة المسلحة، تهديد السلم، الإخلال بالسلم، أعمال العدوان٤٨.

---

[47] أمجد هيكل، **المسئولية الجنائية أمام القضاء الجنائي الدولي عن جريمة العدوان – دراسة في إطار القانون الدولي الإنساني**، دار النهضة العربية، القاهرة ٢٠١٠، ص ٢٨

[48] وليد السعدني، **اختصاص المحكمة الجنائية الدولية بنظر جريمة العدوان**، بحث مقدم إلى ندوة علمية بعنوان المحكمة الجنائية الدولية – تحدي الحصانة، نظمتها كلية الحقوق بجامعة دمشق بالاشتراك مع اللجنة الدولية للصليب الأحمر

أما الاتجاه الآخر فقد توسع في تحديد مفهوم العدوان، حيث يرى أنصاره أن العدوان لم يعد يقتصر على العدوان المسلح فحسب، بل هناك صور أخرى للعدوان مثل: العدوان الاقتصادي والأيدولوجي، ويستند أنصار هذا الاتجاه في حجتهم إلى نص المادة ٢ مثل فقرة ٤ من ميثاق الأمم المتحدة بأن واضعي الميثاق أرادوا وضع مفهوم موسع للفظ القوة بحيث يشمل قوة مسلحة وغير مسلحة بدليل استخدام لفظ (force)[٤٩].

وبالنظر إلى أضيق التعريفات التي قدمت للعدوان وهو التعريف الذي قدمه الاتحاد السوفيتي محاولاً حصر العدوان في أفعال محددة على سبيل الحصر، نجد أنه قد عرف العدوان على أنه تصرف ينحصر في أحد التصرفات التالية[٥٠]:

١. إعلان دولة الحرب على دولة أخرى.
٢. غزو دولة لإقليم دولة أخرى بقواتها المسلحة، ولو لم يكن هناك إعلان عن الحرب.

في الفترة من ٣-٤ /٢٠١٠/١١، إصدارات اللجنة الدولية للصليب الأحمر، جنيف ٢٠١٢، ص ٣١ .

[49] محمد عبد المنعم عبد الغني، **الجرائم الدولية – دراسة في القانون الجنائي الدولي**، دار الجامعة الجديدة، القاهرة ٢٠١٧، ص ٦٦٨

[50] تقدم بهذا التعريف الحصري الفقيه السوفيتي بولوتيس في تقرير مقدم لمؤتمر نزع السلاح عام ١٩٢٣، حيث وافقت عليه لجنة الأمن التابعة لعصبة الأمم، لمزيد من التفاصيل راجع: أشرف محمد لاشين، **النظرية العامة للجريمة الدولية**، دار النهضة العربية، القاهرة ٢٠١٦، ص ٢٢٨

٣. مهاجمة دولة بقواتها المسلحة، برية أو بحرية أو جوية، إقليم دولة أخرى أو قواتها ولو لم تعلن الحرب عليها.
٤. حصار دولة لموانئ أو شواطئ دولة أخرى.
٥. قيام دولة بمساعدة جماعات مسلحة موجودة على إقليمها بقصد غزو إقليم دولة أخرى، أو عدم استجابتها لطلب الدولة الأخرى بالكف عن مساعدة أو حماية هذه الجماعات.

ومع الالتزام بالتعريف الضيق للعدوان كنوع من الاحتياط نجد أن هناك من التصرفات ما ينطبق على الحرب السيبرانية مما ورد في هذا التعريف، فيتصور إعلان الحرب السيبرانية، كما ورد في البند الأول، كما أن غزو القوات المسلحة لدولة إقليم دولة أخرى يمكن أن يكون غزواً سيبرانياً، إذ أن الهجمات السيبرانية قد تؤدي إلى نتائج تماثل وتفوق الهجمات بالأسلحة التقليدية، كما أن الدولة قد تساعد سيبرانياً جماعات مسلحة على إقليمها بقصد غزو إقليم دولة أخرى، وهو ما يتطابق مع حصر بولوتيس، للأفعال التي تشكل جريمة العدوان٥١.

مما سبق يرى الباحث أن مفهومي الحرب والعدوان حتى وإن كانا مفهومين تقليديين فهما ينطبقا على الحرب السيبرانية، إذ أن هذه الحرب تشكل هجوما من دولة على دولة أخرى، أو هجوماً من جماعة تفتقر لصفة الدولة على جماعة أو دولة، كما أن إعلان الحرب السيبرانية يتطابق مع أضيق التعريفات لجريمة العدوان، والنتائج التي تترتب على هذا النوع من الحروب هي ذات النتائج المترتبة على الحرب التقليدية أو ربما تفوقها

[51] تمارا برو، **مرجع سابق**، ص ٨٧

خطورة، لذلك فإن الباحث يتوصل من خلال هذا الجزء من الدراسة إلى انطباق مفهومي الحرب والعدوان على الحرب السيبرانية.

المبحث الثالث: دور القانون الدولي فى مواجهة الحرب السيبرانية

تمهيد وتقسيم:

لا يمكن إنكار عمومية وشمول قواعد القانون الدولي، ذلك الشمول الذي يمكّن القانون الدولي من تنظيم الحرب السيبرانية عن طريق تلك القواعد، وبالرغم من ذلك فإن تصاعد استخدام هذا النوع من الحروب، وتطور الأدوات والتكنولوجيا التي تقف خلف هذه الحرب قد جعلا من الأهمية بمكان تصدي المشرع الدولي بالتنظيم عن طريق نصوص تعاهدية صريحة، خاصة مع التوصل حالياً لكيفية شن هذه الحرب وأسلوب هجماتها والنتائج المترتبة عليها[٥٢].

وتثير الحرب السيبرانية عدداً من الإشكاليات القانونية، أهمها تحديد الأهداف المشروعة للحرب السيبرانية، والتي يجيز القانون الدولي استهدافها دون غيرها من الأهداف في الدولة المعادية، والتعرف على معايير تحديد تلك الأهداف، كما تثير إشكالية نظرة القانون الدولي لهذه الحرب، باعتبارها واقع قد فرض نفسه على

---

[52] محمد رفعت مندور، **المواجهة القانونية لأسلحة حروب الجيل الرابع والخامس**، دار النهضة العربية للنشر والتوزيع، القاهرة ٢٠١٧، ص ٧٣

خارطة النزاعات المسلحة الدولية وغير الدولية[٥٣].

وإذا كانت الحرب السيبرانية تثير عدد من الاشكاليات فإن الواجب هو تصدي القانون الدولي لهذه الإشكاليات، وهو ما حاول المشرع الدولي أن يقوم به عن طريق عدد من المواثيق الدولية، أهمها اتفاقية بودابست ٢٠٠١ بشأن الجريمة السيبرانية، وأحكام دليل تالين ٢٠١٣ الخاص بالحرب السيبرانية، وهو ما فرض التقسيم التالي:

المطلب الأول: الإشكاليات القانونية التي تثيرها الهجمات السيبرانية.

المطلب الثاني: سبل مواجهة الهجمات السيبرانية في القانون الدولي.

المطلب الأول: الإشكاليات القانونية التي تثيرها الهجمات السيبرانية

لم يختلف القانون الدولي فقهاً وتشريعاً على اعتبار المقاتل المسلح هدف مشروع خلال النزاع، إلا أن وضع الحرب السيبرانية قد فرض واقعا لا يفرق في الهدف بين المسلح وغير المسلح، وهو ما استلزم من القانون الدولي النظر لهذا النوع من الحروب نظرة خاصة تتوافق مع ذاتيتها.

[53] زهراء عماد، **مرجع سابق**، ص ٤٣

أولا: تحديد الأهداف المشروعة للحرب السيبرانية

إذا كان الفقه والتشريع الدوليين قد اتفقا على قاعدة أن الحروب هي علاقات بين الدول لا الأفراد، فإن مشروعية أهداف الحرب لا بد أن تتفق مع تحقيق مصلحة الدولة من الحرب والمتمثلة في إضعاف الدولة المعادية، وحرمانها من وسائل التفوق العسكري، وهو ما يعني استبعاد الأهداف البشرية والعينية التي لا تسهم بفاعلية في الجهود الحربية، ولا توفر ميزة للقوات المتحاربة٥٤.

ويوفر القانون الدولي حماية تشمل البنية التحتية الضرورية لحياة السكان، بحيث لا يجوز استهداف هذه البنية بأي صورة من الصور، إذ تحظر الحروب التقليدية والسيبرانية التي تستهدف القطاعات الطبية والغذائية وقطاعات توليد الطاقة وقطاع التعليم، كما تشمل توفير غطاء من الحماية للأفراد غير المشاركين مباشرة في العمليات العسكرية، وهو ما يستدعي وضع ضوابط معينة يتحدد من خلالها الهدف المشروع والهدف غير المشروع للحرب السيبرانية٥٥.

وقد اتجه بعض الفقه إلى أن الحماية التي يوفرها القانون الدولي للأشخاص والأعيان غير المشاركة في العمليات العسكرية إنما تنصب على حمايتهم من الأضرار الجسدية والمادية التي يمكن أن تتسبب فيها الحرب

---

[54] احمد طلعت حامد، **ضوابط الإتلاف في الحرب – دراسة فقهية مقارنة بالقانون الدولي**، المكتب الجامعي الحديث، القاهرة ٢٠١٦، ص ١٥٤

[55] تمارا برو، **مرجع سابق**، ص ١٠١

السيبرانية، وهو ما قد يتمثل في حالات الوفيات الناتجة عن الفقر المائي والغذائي نتيجة اصابة الحرب السيبرانية لمصادر الماء والطاقة بالأضرار، أو وفاة المرضى نتيجة استهداف البنية الإلكترونية للمستشفى بما يتسبب في اتلاف أجهزة الإعاشة الطبية، أي أن الهجمات السيبرانية المحظورة بموجب القانون الدولي من وجهة نظر هذا الفقه هي الهجمات التي تتسبب في ضرر مباشر كالوفيات والاصابات الجسدية وتلف الأجهزة والمعدات اللازمة للحياة المعتادة، بحيث يجيز القانون الدولي القيام بالهجمات السيبرانية التي يكون في الإمكان إصلاح الاضرار المترتبة عليها٥٦.

بينما يتجه فقه آخر إلى أن مناط الحظر هو صفة الهدف الذي يتعرض للهجوم السيبراني، لا الأثر المترتب على الهجوم، وعلى هذا يحظر أي عمل سيراني عسكري يستهدف الأفراد أو المنشآت المدنية، بغض النظر عما قد يسفر عنه هذا الهجوم، فالقانون الدولي يحظر القيام بعمليات عسكرية من أي نوع تقع على المدنيين، وهو ما يعني أن الهجوم السيبراني الذي يتم بمناسبة العمليات العسكرية يجب أن يقتصر في استهدافه على الأهداف العسكرية دون غيرها٥٧.

وإذا كان القانون الدولي قد وفر هذا الغطاء من الحماية للمدنيين فإن التساؤل يثور حول قيام مدنيين بهذه الهجمات بتكليف رسمي من الجهات المختصة، حيث يعد المدني في هذه الحالة يمارس عملاً عسكرياً مرتبط بالحرب، والواقع أن قيام القوات المسلحة في الدولة بتخصيص وحدات

---

[56] محمد سعادي، **مرجع سابق**، ص ٩٠

[57] نسرين عبد الحميد نبيه، **مرجع سابق**، ص ١٢٢

عسكرية تضم افراد ذوي مهارة فنية معينة للقيام بشن هذا النوع من الهجمات لا يثير أزمة، إذ يعد هؤلاء الأفراد في هذه الحالة أفراد عسكريون لا شبهة في صفتهم، بينما تثور الإشكالية الحقيقية في حالة الإيعاز لهيئات مدنية تضم موظفين مدنيين بالقيام بهذه المهمة؛ إذ لا يمكن إسباغ الصفة العسكرية على هؤلاء الأشخاص أو على المنشآت أو الجهات الإدارية المخولة بالقيام بهذه الوظيفة٥٨.

ويرى الباحث أن الحظر الذي يفرضه القانون الدولي على العمليات العسكرية التي تستهدف المدنيين لا بد أن يكون مناطه هو هدف الهجوم السيبراني، ومدى تمتع هذا الهدف بالصفة المدنية، إذ أن اشتراط وقوع اصابات جسدية أو مادية هو تكلف لا ضرورة قانونية له، والا في هذه الحالة فإن المجتمع الدولي يجد نفسه أمام مفارقة غير مقبولة، وهي وقوع هجومين سيبرانيين على هدفين مدنيين، فيعد أحد الهجومين هجوما محظورا نظرا لوقوع ضحايا من المدنيين بينما الاخر يعد هجوما مصرحا به لمجرد عدم وقوع ضحايا من المدنيين، فلا يمكن اعتبار منفذ الهجوم كان قاصداً إيقاع ضحايا أو غير قاصد، لأن الهدف من أي هجوم عسكري لا يختلف؛ إذ يستهدف دائما ايقاع أــكبر قدر من الضرر بالعدو، كما يرى أن مشاركة أي فرد في العمليات العسكرية يسبغ عليه هذه صفة المقاتل طالما كان يقوم به بتكليف رسمي من الدولة المحاربة، وبالتالي يعد المدني الذي يقوم بهجوم سيبراني لحساب دولته هو شخص يحمل أحد أنواع الأسلحة ويستخدمها ضد العدو، مما ينتفي معه منطقية شموله بالحماية المقررة للمدنيين، سواء حمايته

---

[58] وائل أنور بندق، **موسوعة القانون الدولى للحرب- جرائم الحرب والإبادة الجماعية وقواعد الحرب**، مكتبة الوفاء القانونية، القاهرة ٢٠١٤، ص ٢٣٦

على المستوى الشخصي أو على مستوى المنشأة التي يمارس منها هجومه، وبمفهوم المخالفة يتمتع بالحماية الدولية للمقاتل ويتمتع في حالة وقوعه في الأسر بكافة حقوق الأسير.

ثانيا: نظرة القانون الدولي للحرب السيبرانية

إذا كان القانون الدولي الانساني هو القانون المنوط به تنظيم النزاعات المسلحة والحروب التي تقع بين الدول، فإن هذا الاختصاص يفرض منطقاً تغطيته للحروب السيبرانية التي تأتي في سياق النزاعات المسلحة، إذ تخضع الحروب السيبرانية لذات القانون الذي يحكم النزاع المسلح الذي تمت في ظله[٥٩].

أما التساؤل الحقيقي فيثور بشأن الحروب السيبرانية التي يتم شنها دون أن ترتبط بنزاع مسلح، وهو ما قد يشير لعدم اختصاص القانون الدولي الانساني بشأنها، وخاصة في ظل عدم اعتمادها على الأسلحة التقليدية، حيث يجعل هذا الوضع من الحرب السيبرانية تصرف يفتقر إلى التنظيم القانوني، الأمر الذي ينقل عبء التنظيم كاملاً إلى المبادئ القانونية، حيث تحمي هذه المبادئ عدد من قطاعات البنية التحتية بصورة عامة من أي ضرر أي كان مصدره طالما كان مصدر الضرر هو عدوان خارجي، إذ تضمن مبادئ القانون الدولي الانساني حد أدنى من سير هذه المرافق والمنشآت، بحيث

---

[59] موسى بن تغري، **الحرب السيبرانية والقانون الدولي الانساني**، بحث منشور في مجلة الاجتهاد القضائي، مجلد ١٢ عدد خاص، جامعة محمد خيضر بسكرة، الجزائر ٢٠٢٠، ص ٢٠٧

يحظر تناولها بأي عمل عدائي من شأنه توقفها عن العمل، وإصابة المدنيين بأضرار جراء هذا العمل العدائي٦٠.

وعلى هذا تلزم مبادئ القانون الدولي الطرف الذي يشن الحرب السيبرانية بأن يتخذ أكبر قدر من الاحتياطات والتدابير في سبيل تجنب الأضرار التي قد تلحق بالأهداف المدنية في سياق الهجوم على الأهداف العسكرية، ومن باب أولى الامتناع عن مهاجمة اي هدف مدني، لذا تستوجب هذه المبادئ إلغاء التخطيط لأي هجوم سيبراني طالما كان من شأن هذا الهجوم أن يعرض الأعيان المدنية للخطر، كما تلزم هذه المبادئ الأطراف المتحاربة بتحييد الأهداف المدنية، حيث يمتنع عليها استخدامها في الهجمات السيبرانية، بما يعرضها لخطر الرد من العدو، واستهدافها نظرا لبدء الهجوم منها٦١.

كما تلتزم الأطراف المتحاربة باحترام حياد الدول، حيث تلتزم بعدم استخدام الشبكات المحلية للدول غير الأطراف في النزاعات في شن الحروب السيبرانية، وسواء كان من شأن هذا الاستخدام إلحاق أضرار بهذه الشبكات أو كان استخدامها على سبيل الاستضافة والنقل فحسب، دون أن تتعرض لأي مظاهر سلبية أو خسائر، حيث يعد استخدام الشبكات الأجنبية نوعا من اقحام الدول المحايدة في النزاع، وهو ما يترتب عليه ضرورة إعلام الدولة

---

[60] احمد طلعت حامد، **مرجع سابق**، ص ١٦٦

[61] ستار عبد عودة الفهداوي، **حماية المدنيين وقت الحرب في الشريعة الاسلامية والقانون الدولي العام**، مركز البحوث والدراسات الإسلامية، عمان ٢٠١٧، ص ١٣١

مالكة الشبكة باستخدام شبكتها في الهجوم السيبراني[٦٢].

ويرى الباحث أن مبادئ القانون الدولي الانساني برغم امكان تطبيقها على الحرب السيبرانية إلا أن الواقع قد يفرض تهرب الدول المتحاربة من تطبيق هذه المبادئ، حيث لا يتصور عملاً أن تعمد الدولة المهاجمة لإعلام الدولة المحايدة باستخدام شبكتها الرقمية في شن الهجوم؛ لما في ذلك من تعارض مع مبادئ السرية التي تتميز بها العمليات الحربية، كما أن تأسيس خطط الهجوم السيبراني على اساس تجنب اصابة المنشآت المدنية هو مسلك مثال قلما يتبع في الحروب بصفة عامة.

المطلب الثاني: سبل مواجهة الهجمات السيبرانية في القانون الدولي

برغم غياب التنظيم التشريعي الدولي للحرب السيبرانية الا أن المشرع الدولي حاول أن يضمن بعض خطواته مواجهة هذا النوع من الحروب، وذلك بصورة واقعية تنفي عنه السلبية وتثبت مواكبته للتطورات التكنولوجية التي تمتعت بها العمليات العسكرية في الفترة الأخيرة، وعلى ذلك فقد تم عقد اتفاقية بودابست لمواجهة الجريمة السيبرانية عام ٢٠٠١، كما تم إصدار دليل عن طريق تكليف حلف الناتو لعدد من فقهاء القانون الدولي سمي حينها بدليل تالين وصدر عام ٢٠١٣.

---

[62] ياسر خلف، **الحرب الإلكترونية**، دار يافا للنشر والتوزيع، عمان ٢٠١٧، ص ٩٠

أولا: اتفاقية بودابست ٢٠٠١[٦٣]

كانت اتفاقية بودابست محاولة من المشرع الدولي لتحديد القانون واجب التطبيق على الحرب السيبرانية، ووضع قواعد قانونية حاكمة لهذا النوع من الهجمات، حيث جاء في ديباجة الاتفاقية أن إبرامها قد جاء كنتيجة للتغيرات الناجمة عن التكنولوجيا السيبرانية، وعولمة الشبكات الرقمية، حيث أدرك المشرع الدولي وأشخاص المجتمع الدولي ما قد ينجم من مخاطر عن استخدام هذه التكنولوجيا في ارتكاب أفعال تعد من قبيل الجريمة، حيث حاولت إيجاد نظام فعال للتعاون الدولي في مجال مكافحة الهجمات السيبرانية، إذ حاولت الدول الأطراف في الاتفاقية الوصول لصيغة تشريعية عامة لمكافحة الهجمات السيبرانية، والحد من آثارها٦٤.

ويعيب الباحث على هذه الاتفاقية عدم التفاتها إلى الهجمات السيبرانية التي تقوم بها الدول في إطار رسمي، حيث تناولت فقط في نصوصها الهجوم السيبراني الذي يشنه الأشخاص ضد بعضهم، بمعنى أن اهتمامها قد انصب

---

[63] الاتفاقية المتعلقة بالجريمة الإلكترونية، اعتمدت في ٨ نوفمبر ٢٠٠١، وفتح باب التوقيع عليها في ٢٣ نوفمبر ٢٠٠١، ودخلت حيز النفاذ في ١ يوليو ٢٠٠٤ للاطلاع على النص الكامل للاتفاقية راجع الموقع الرسمي لمجلس اوروبا، مجموعة المعاهدات الاوروبية

https://rm.coe.int/budapest-convention-in-arabic/1680739173

إتاريخ الاطلاع ٢٠٢٢/٢/١٧

[64] هلالي عبد اللاه احمد، **اتفاقية بودابست لمكافحة جرائم المعلوماتية**، دار النهضة العربية، القاهرة ٢٠١١، ص ٢٩

على الطابع التجريمي للهجمات السيبرانية، وهو ما يتبين من عنوانها، وذلك برغم واقعية وجود الحرب السيبرانية، وسبق وقوع مثل هذه الحرب قبل توقيع الاتفاقية في حرب البلقان التي دارت على أرض يوغسلافيا السابقة؛ إذ استخدمت قوات حلف شمال الأطلسي الحرب السيبرانية ضد الأهداف الإلكترونية الصربية، أي أن الحرب السيبرانية كانت واقعا موجودا قبل دخول الاتفاقية حيز النفاذ، مما كان يوجب على المشرع الدولي أن يلتفت الى هذا النوع من الحروب من خلال هذه الاتفاقية.

ثانيا: أحكام دليل تالين بشأن الحرب السيبرانية[٦٥]

وبناءً على إغفال اتفاقية بودابست والاتفاقيات القارية التي سارت على نهجها تناول الحرب السيبرانية في صورتها الرسمية بين الدول وبعضها، قام حلف شمال الأطلسي بتشكيل لجنة ضمت أساطين الفقه الدولي لوضع عدد من القواعد التي تنظم هذا النوع من الحروب، وتحديد أساس قانوني يمكن الاستناد إليه في تحديد الطبيعة القانونية لهذه الحروب، حيث أعد هؤلاء الفقهاء دليلاً يضم قواعد القانون الدولي التي يمكن تطبيقها على الحرب السيبرانية سمي بدليل تالين٦٦.

---

[65] للاطلاع على دليل تالين راجع الموقع الرسمي للجنة الدولية للصليب الأحمر https://www.icrc.org/ar/doc/resources/documents/faq/130628-cyber-warfare-q-and-a-eng.htm

تاريخ الاطلاع ٢٠٢٢/٢/١٨

[66] ازهر عبد الأمير الفتلاوي، **العمليات العدائية طبقا لقواعد القانون الدولي الإنساني**، المركز القومي للاصدارات القانونية، القاهرة ٢٠١٩، ص ١٧٧

ويعد دليل تالين هو الوثيقة الدولية الوحيدة حتى كتابة هذه السطور والتي تناولت الحرب السيبرانية بين الدول، وذلك من خلال خمس وتسعين قاعدة تأسست جميعها على قواعد القانون الدولي، والقانون الدولي الإنساني، وقد أسسّ هذا الدليل عدد من المبادئ أهمها امكانية النظر للحرب السيبرانية على أنها نزاع مسلح، حتى لو لم تتوازي مع نزاع مسلح فعلي، بحيث يمكن الاعتداد بالحرب السيبرانية إذا كانت قد تم شنها على سبيل الاستقلال، كما يتصور أن تكون الحرب السيبرانية دولية أو غير دولية٦٧.

ويعرف الدليل الحرب السيبرانية على أنها إجراء إلكتروني هجومي أو دفاعي يتوقع أن يسفر عن قتل أشخاص أو إصابتهم أو الإضرار بمنشآت مدنية، وقد اعتدّ المجتمع الدولي بهذا الدليل كمصدر لتنظيم الحرب السيبرانية، نظراً لعدم توفر أي مصدر تنظيمي بخلافه، كما تم الاتفاق على أن تطبيق هذا الدليل لا يتأتى إلا في حالات النزاع المسلح، بغض النظر عن كونه نزاع دولي أو غير دولي٦٨.

ويرى الباحث أن دليل تالين برغم الجهد المبذول في إعداده، وكونه التنظيم الدولي الوحيد للحرب السيبرانية، إلا أنه في طبيعته القانونية لا يتعدى كونه نوع من التوصيات غير الملزمة، فهو لا يعد اتفاقية أو قرار ملزم صادر من منظمة دولية، كما أن هناك من عارض الأحكام الواردة به

---

[67] منذر رابح، **الطبيعة القانونية للهجمات السيبرانية التي تقع بين الدول**، بحث منشور في مجلة صوت القانون، مجلد ٨ عدد ١، معهد الحقوق والعلوم السياسية، جامعة الجزائر ٢٠٢١، ص ٥٤٨

[68] ازهر عبد الأمير الفتلاوي، **مرجع سابق**، ص١٨٥

مثل: روسيا والصين وهما من الدول الدائمة العضوية في مجلس الأمن، مما يشكك في جدوى إعداد هذا الدليل ومدى التزام المجتمع الدولي بما ورد في مضمونه، كما أن الفقه الذي قام على إعداده لم يراعِ في تشكيله التمثيل العادل للدول الأعضاء في الأمم المتحدة.

من العرض السابق يتبين أن الحرب السيبرانية وإن كانت أحد الظواهر العسكرية المستحدثة إلا أنها لا تعدو كونها أحد أنواع الحروب التي تستهدف الدولة المتحاربة من خلالها أن تضعف من قدرات الدولة المعادية وتلحق بها أكبر قدر من الخسائر، وهو الأمر الذي يوجب على المجتمع الدولي تنظيمها باعتبارها حرب تستخدم أسلحة غير تقليدية.

خاتمة

تعد الحرب السيبرانية أو الهجمات السيبرانية من بين أهم الموضوعات التي يتداولها المجتمع الدولي في العصر الراهن، غير أنه ولاعتبارات قانونية، وأخرى سياسية لم يتفق المجتمع الدولي على تعريف موحد لها برغم جدية الفقه في وضع مثل هذا التعريف، حيث لم تتطرق الاتفاقيات والقرارات الدولية لوضع معايير للحرب السيبرانية.

وعلى هذا الأساس كان الاتجاه للاهتمام بالحرب السيبرانية أمراً ملحاً بالنسبة للفقه والتشريع الدوليين، حيث فرض الواقع استخدام التكنولوجيا في العمليات العسكرية، والإغارة الإلكترونية على الأهداف المعادية، وهو الوضع المستحدث الذي جذب أنظار المجتمع الدولي خاصة مع تفاوت الدول في القدرات السيبرانية، وهو ما يصنع نوعا من الحرب غير العادلة بين الدول المختلفة.

وإذا كانت نصوص القانون الدولي قد اعتراها القصور بالنسبة لتنظيم الحرب السيبرانية ومواجهتها، فإن القواعد العامة لهذا القانون قد نجحت في وضع عدد من المعايير والاعتبارات التي يمكن للفقه الاستناد اليها في تأسيس قواعد لاستخدام الحرب السيبرانية، وخاصة مع الاعتداد بها كحرب تماثل الحرب التقليدية، وكفعل يحمل الكثير من سمات جريمة العدوان.

والواقع إنه لا يصعب على القانون الدولي أن يتناول الحرب السيبرانية بالتنظيم، وذلك بالتدخل لضبط مفهوم هذا النوع من الحروب، ووضع الضوابط والمعايير التي تنظمه، وفرض حدود استخدام هذه الحرب

على الدول التي تمتلك التقنيات اللازمة لها، وذلك في ضوء ترسيخ مبدأ الشرعية وتأكيده، فضلاً عن الحاجة إلى وجود معيار قانوني واضح ومحدد يمكن من خلاله حسم الاتهامات المتبادلة التي قد تثور بين الدول بشأن الهجمات السيبرانية، حيث أن الواقع قد كشف عن مدى الحاجة إلى وجود مثل هذا التعريف والتحديد، لأن عدم وضع تعريف رسمي يعرقل من جهود المنظمات الدولية في تنظيم هذه الحرب والحد من آثارها.

النتائج

١- الحرب السيبرانية هي هجمات إلكترونية تقوم بها أجهزة حكومية رسمية، ضد أجهزة حكومية رسمية في دولة معادية، وهي جزء من الحرب الشاملة، تهدف إلى إلحاق خسائر بالنظام المعلوماتي للعدو؛ بحيث يتم الحصول على المعلومات المخزنة عليه، أو حرمان العدو من استخدامه، أو تحويله إلى نظام يهاجم العدو بحيث يتحول إلى نظام تخريب ذاتي.

٢- الحرب السيبرانية تختلف عن الحرب التقليدية، وتتسم بعدد من الخصائص التي تميزها، وهي خصائص نابعة من طبيعتها المتطورة غير التقليدية، كما تنبع من آثارها وطريقة القيام بها، والتي تختلف كليا عن الحروب التقليدية وأدواتها.

٣- برغم حداثة الحرب السيبرانية إلا أنها استطاعت أن تفرض نفسها على ساحات النزاعات الدولية، وهو الأمر الذي نتج عن مدى تنوعها وسرعة القيام بها، وشدة تأثيرها، كما يمكن إيعاز هذه الأهمية إلى محدودية تكاليفها وعدم احتياجها لجهود أو معدات كبيرة، إذ يمكن شنها بأبسط الامكانات وعن طريق عدد محدود من الأفراد ودون تكلفة تذكر مقارنة بالحرب التقليدية، لذا تسعى أغلب الدول اليوم لتطوير امكانياتها السيبرانية، ودعم قوتها العسكرية بالكفاءات والأدوات التي تمكنها من شن هذا النوع من الحروب.

٤- مبدأ الضرورة العسكرية يتيح شن الحرب السيبرانية ضد الأهداف العسكرية كهدف رئيسي، إلا أن هذا لا يمنع مهاجمة المدنيين أشخاص وأعيان إذا كان هؤلاء المدنيين مساهمين بصورة مباشرة في الأعمال القتالية

وتحقيق مميزات للقطاع العسكري، وفي هذه الحالة يجب على المهاجم أن يتخير كهدف للحرب السيبرانية المنشآة التي يمثل الهجوم عليها تحقيق أقل قدر من الأضرار للمدنيين.

٥- شن حرب سيبرانية رسمية معلنة على سبيل الاستقلال هو افتراض لم يتحقق الآن ويستبعد تحققه، لذا فالأكثر واقعية اعتبار الحرب السيبرانية نوع من الأسلحة المستحدثة ذات التأثير الشامل.

٦- مفهومي الحرب والعدوان حتى وإن كانا مفهومين تقليديين فهما ينطبقا على الحرب السيبرانية، إذ أن هذه الحرب تشكل هجوماً من دولة على دولة أخرى، أو هجوماً من جماعة تفتقر لصفة الدولة على جماعة أو دولة، كما أن إعلان الحرب السيبرانية يتطابق مع أضيق التعريفات لجريمة العدوان.

٧- الحظر الذي يفرضه القانون الدولي على العمليات العسكرية التي تستهدف المدنيين لا بد أن يكون مناطه هدف الهجوم السيبراني، ومدى تمتعه بالصفة المدنية.

٨- مشاركة أي فرد في العمليات العسكرية يسبغ عليه هذه الصفة طالما كان يقوم به بتكليف رسمي من الدولة المحاربة، وبالتالي يعدّ المدني الذي يقوم بهجوم سيبراني لحساب دولته هو شخص يحمل أحد أنواع الأسلحة ويستخدمها ضد العدو، مما ينتفي معه منطقية شموله بالحماية المقررة للمدنيين.

٩- الالتزام بمبادئ القانون الدولي الانساني في تنفيذ الحرب السيبرانية يتنافى مع الواقع والمنطق ويصعب تصور حدوثه عملاً.

١٠- لم تتناول اتفاقية بودابست الحرب السيبرانية بمفهومها الفعلي، وإنما اقتصر دور المشرع الدولي من خلالها على تنظيم الهجمات التي يرتكبها الأفراد ضد الأفراد، دون التي ترتكبها الدول ضد الدول.

١١- حاول المجتمع الدولي تنظيم الحرب السيبرانية من خلال إصدار وثيقة تتسم بالصفة الدولية، إلا أن نتيجة هذه المحاولة كانت إصدار دليل غير ملزم تضمن عدد من التفسيرات والأحكام التي تعد وثيقة ارشادية أكثر منها وثيقة ملزمة.

التوصيات

١- آن للمشرع الدولي أن يتدخل بموجب نصوص تعاهدية صريحة لتنظيم الحرب السيبرانية على اعتبار أنها أصبحت أمر واقع في مجتمع الحروب، من شأنه أن يلحق بالقوات المعادية خسائر فادحة على الصعيدين العسكري والمدني، وقد تتماثل هذه الخسائر مع ما تسببه الأسلحة التقليدية بل قد تفوقها في الآثار التدميرية.

٢- إذا كانت الدول كافة تسعى لتعزيز قدراتها العسكرية واستحداث أسلحة من شأنها أن تلحق بالعدو أكبر خسارة ممكنة، فإن هذا السعي لا بد أن يسير بالتوازي مع السعي لتحييد المدنيين أشخاص وأعيان، بحيث لا يكون من شأن هذا الاستحداث إلحاق أضرار بالبنية التحتية المدنية.

٣- يجب أن يراعي استخدام الحرب السيبرانية الدقة البالغة في تخير

الأهداف محل الهجوم، إذ وجب على الدول الالتزام بقصر الهجمات السيبرانية على الأهداف العسكرية المشتركة في المعركة دون غيرها من الأهداف.

٤- وجب على القانون الدولي أن يضمن الالتزام باحترام وضع الحياد من قبل الأطراف المتحاربة سيبرانيا، إذ لا بد من النص الصريح على حظر استخدام الفضاء السيبراني لأي دولة محايدة دون علمها في شن هجمات سيبرانية.

٥- يجب على المشرع الدولي التدخل بالنص على حظر استخدام الأعيان المدنية في شن هجمات سيبرانية، وحظر استغلال المدنيين في هذه الهجمات مهما بلغت مهارتهم، إذ من شأن هذا الاستغلال تعريض الأشخاص والأعيان المدنيين لشن الهجمات الانتقامية من قبل القوات المعادية.

٦- يجب على الدول الالتزام باستخدام الحرب السيبرانية على سبيل الدفاع فقط، بحيث تكون الدولة غير بادئة بالعدوان، وذلك نظرا لاتساع مدى هذه الهجمات، وفداحة الآثار المترتبة عليها للعسكريين والمدنيين.

٧- لا بد من التزام الدول كافة بالتعاون في مجال أمن الفضاء السيبراني، بحيث يكون هذا التعاون ضامنا لعدم استخدام هذا الفضاء في العدوان المتبادل بين الدول، كما يضمن عدم استخدام الفضاء في شن الهجمات السيبرانية.

قائمة المراجع

أولا: المراجع العامة

١- أحمد حمدي علي، الحرب في الإسلام والقانون الدولي الإنساني، المكتبة الأزهرية للتراث، القاهرة ٢٠٢٠

٢- أحمد عبد المعطي حسين، الحرب وقيودها الأخلاقية – مقارنات بين الفقه الإسلامي والقانون الدولي الإنساني، مركز الحضارة لتنمية الفكر الإسلامي، برلين ٢٠١٨

٣- أزهر عبد الأمير الفتلاوي، العمليات العدائية طبقا لقواعد القانون الدولي الإنساني، المركز القومي للاصدارات القانونية، القاهرة ٢٠١٩

٤- علي عبد الله فضل الله، الحرب الشرعية والحرب المشروعة في القانون الدولي، منشورات الحلبي الحقوقية، بيروت ٢٠١٨

٥- عمار عباس الحسيني، جرائم الحاسوب والانترنت – الجريمة المعلوماتية، منشورات زين الحقوقية، بيروت ٢٠١٧

ثانيا: المراجع المتخصصة

١- أحمد عبيس الفتلاوي، الهجمات السيبرانية – دراسة قانونية تحليلية بشأن تحديات تنظيمها المعاصر، منشورات زين الحقوقية، بيروت ٢٠١٨

٢- أحمد طلعت حامد، ضوابط الإتلاف في الحرب – دراسة فقهية مقارنة بالقانون الدولي، المكتب الجامعي الحديث، القاهرة ٢٠١٦

٣- أحمد مبخوتة، إعمال المسئولية الجنائية الدولية عن جرائم الحرب، دار الفكر الجامعي، القاهرة ٢٠٢٠

٤- أسامة عرفات، القواعد الحامية للمدنيين زمن الحرب في القانون الدولي العام وشريعة الاسلام، دار الإجادة، القاهرة ٢٠١٧

٥- أشرف سعد منصور، التنظيم الدولي للقوة الالكترونية، المركز القومي

للإصدارات القانونية، القاهرة ٢٠١٨
٦- أشرف محمد لاشين، النظرية العامة للجريمة الدولية، دار النهضة العربية، القاهرة ٢٠١٦
٧- أمجد هيكل، المسئولية الجنائية أمام القضاء الجنائي الدولي عن جريمة العدوان – دراسة في إطار القانون الدولي الإنساني، دار النهضة العربية، القاهرة ٢٠١٠
٨- بشير حسن الحمداني، القرصنة الإلكترونية – أسلحة الحرب الحديثة، دار أسامة للنشر والتوزيع، عمان ٢٠١٤
٩- تمارا برو، استخدام الأسلحة غير التقليدية في القانون الدولي العام، دار المنهل اللبناني للطباعة والنشر، بيروت ٢٠١٥
١٠- خالد وليد محمود، الهجمات عبر الانترنت – ساحة الصراع الإلكتروني الجديد، المركز العربي للأبحاث ودراسة السياسات، الدوحة ٢٠١٣
١١- ريماس صعب، المواجهة القانونية للأسلحة غير التقليدية في القانون الدولي، منشورات زين الحقوقية، بيروت ٢٠٢١
١٢- زهراء عماد، المسئولية الدولية عن شن الهجمات السيبرانية، دار السنهوري للطباعة والنشر، بغداد ٢٠١٦
١٣- ستار عبد عودة الفهداوي، حماية المدنيين وقت الحرب في الشريعة الاسلامية والقانون الدولي العام، مركز البحوث والدراسات الإسلامية، عمان ٢٠١٧
١٤- شادي عبد الوهاب منصور، حروب الجيل الخامس – أساليب التفجير من الداخل على الساحة الدولية، دار العربي للنشر والتوزيع، القاهرة ٢٠٢٠
١٥- صلاح عبد الرحمن الحديثي، التفصيل الشامل لتطور القواعد القانونية

الخاصة بالحرب السيبرانية، المجموعة العلمية للنشر والتوزيع، القاهرة ٢٠٢١

١٦- عادل عبد الصادق، الإرهاب الإلكتروني كشكل جديد للصراع الدولي، مركز الدراسات السياسية والاستراتيجية، القاهرة ٢٠١٧

١٧- عباس بدران، الحرب الإلكترونية – الاشتباكات في عالم المعلومات، مركز دراسات الحكومة الإلكترونية، بيروت ٢٠١٢

١٨- عبد القادر دندن، العلاقات الدولية في عصر التكنولوجيا الرقمية، مركز الكتاب الاكاديمي، عمان ٢٠٢١

١٩- عبد الكريم محمود، تحديات السيادة السيبرانية في القانون الدولي، المركز العربي لأبحاث الفضاء الإلكتروني، القاهرة ٢٠٢١

٢٠- عمار حميد عبد الأمير الحسني، حماية الممتلكات ومبدأ المسئولية عند الحماية وعلاقته بجرائم الحرب، دار الكتب والدراسات العربية، القاهرة ٢٠١٩

٢١- عمر سعد الزيات، أسلحة الدمار الشامل في القانون الدولي، منشورات الحلبي الحقوقية، بيروت ٢٠١٧

٢٢- لفقير بولنوار بن الصديق، جرائم الحرب في ضوء أحكام القانون الدولي، دار الأيام للنشر والتوزيع، عمان ٢٠١٧

٢٣- ماجد الغيطي، دور التكنولوجيا في إدارة الصراعات الدولية المعاصرة، دار الآن للطباعة والنشر، بيروت ٢٠١٩

٢٤- محمد رفعت مندور، المواجهة القانونية لأسلحة حروب الجيل الرابع والخامس، دار النهضة العربية للنشر والتوزيع، القاهرة ٢٠١٧

٢٥- محمد سعادي، أثر التكنولوجيا المستحدثة على القانون الدولي العام، دار الجامعة الجديدة، القاهرة ٢٠١٤

٢٦- محمد عبد المنعم عبد الغني، الجرائم الدولية - دراسة في القانون الجنائي الدولي، دار الجامعة الجديدة، القاهرة ٢٠١٧
٢٧- نسرين عبد الحميد نبيه، تطور أساليب الحروب وظهور أنواع جديدة تتناسب والتكنولوجيا الحديثة، مكتبة الوفاء القانونية، القاهرة ٢٠٢١
٢٨- نوران شفيق، أثر التهديدات الإلكترونية على العلاقات الدولية – دراسة في أبعاد الأمن الإلكتروني، المكتب العربي للمعارف، القاهرة ٢٠١٦
٢٩- هلالي عبد اللاه احمد، اتفاقية بودابست لمكافحة جرائم المعلوماتية، دار النهضة العربية، القاهرة ٢٠١١
٣٠- وائل أنور بندق، موسوعة القانون الدولى للحرب- جرائم الحرب والإبادة الجماعية وقواعد الحرب، مكتبة الوفاء القانونية، القاهرة ٢٠١٤
٣١- ياسر خلف، الحرب الإلكترونية، دار يافا للنشر والتوزيع، عمان ٢٠١٧

ثالثا: الأبحاث والدوريات

١- صبري حيدرة، مواجهة الهجمات السيبرانية في القانون الدولي، بحث منشور في مجلة حقوق الانسان والحريات العامة، عدد ٤، جامعة عبد الحميد بن باديس، الجزائر ٢٠١٧
٢- علي الرفاعي، الحروب السيبرانية وتداعيتها على الأمن والسلم الدوليين، بحث منشور في المجلة العلمية الأكاديمية، عدد ٥٧، كلية العلوم السياسية جامعة بغداد، ٢٠١٩
٣- مصطفى نعوس، حقوق والتزامات الدول في الحرب المعلوماتية، بحث منشور في مجلة دراسات علوم الشريعة والقانون، مجلد ٤٠ ملحق ٤، الجامعة الأردنية، عمان ٢٠١٣
٤- منذر رابح، الطبيعة القانونية للهجمات السيبرانية التي تقع بين الدول،

بحث منشور في مجلة صوت القانون، مجلد ٨ عدد ١، معهد الحقوق والعلوم السياسية، جامعة الجزائر ٢٠٢١

٥- موسى بن تغري، الحرب السيبرانية والقانون الدولي الانساني، بحث منشور في مجلة الاجتهاد القضائي، مجلد ١٢ عدد خاص، جامعة محمد خيضر بسكرة، الجزائر ٢٠٢٠

٦- نور أمير الموصلي، الهجمات السيبرانية في ضوء القانون الدولي الانساني، بحث مقدم استكمالا لمتطلبات نيل درجة ماجستير التأهيل والتخصص في القانون الدولي الانساني، الجامعة السورية، دمشق ٢٠٢١

٧- هربرت لين، النزاع السيبراني والقانون الدولي الإنساني، مقال منشور في مجلة اللجنة الدولية للصليب الأحمر، مجلد ٩٤ عدد ٨٨٦، جنيف ٢٠١٢

٨- وليد السعدني، اختصاص المحكمة الجنائية الدولية بنظر جريمة العدوان، بحث مقدم إلى ندوة علمية بعنوان المحكمة الجنائية الدولية - تحدي الحصانة، نظمتها كلية الحقوق بجامعة دمشق بالاشتراك مع اللجنة الدولية للصليب الأحمر في الفترة من ٣-٤ /١١/٢٠١٠، إصدارات اللجنة الدولية للصليب الأحمر، جنيف ٢٠١٢.

٩- يحيى ياسين مسعود، الحرب السيبرانية في ضوء القانون الدولي الإنساني، بحث منشور في المجلة القانونية.

رابعا: المواقع الالكترونية

١- الموقع الرسمي للجامعة الافتراضية السورية
https://pedia.svuonline.org/pluginfile.php/3200/mod_label/intro

٢- الموقع الرسمي للمجلة الالكترونية
https://jlaw.journals.ekb.eg/article_45192_52d735c1a23cca2bf7dbbe56c4eb6846.pdf

٣- الموقع الرسمي للموسوعة الجزائرية للدراسات الاستراتيجية والسياسية
https://www.politics-dz.com

٤- الموقع الرسمي للجيش اللبناني
https://www.lebarmy.gov.lb/ar/content

٥- الموقع الرسمي للجنة الدولية للصليب الاحمر
https://www.icrc.org/ar/doc/resources/documents/misc/62sd4j.htm

٦- الموقع الرسمي لمجلس اوروبا، مجموعة المعاهدات الاوروبية
https://rm.coe.int/budapest-convention-in-arabic/1680739173

٧- الموقع الإلكترونى التعليمي
https://www.cisco.com