الحرب الإلكترونية واستراتيجية الدول لمواجهتها

م.م شيماء جمال محمد
Shaymaa.jamal@uokirkuk.edu.iq
جامعة كركوك/ كلية القانون والعلوم السياسية/ قسم القانون

ELECTRONIC WARFARE AND THE STRATEGY OF COUNTRIES TO CONFRONT IT

Assist. Lecturer. Shaima Jamal Mohammed
University of Kirkuk / College of Law and Political Science / Department of Law

الملخص

يعد النزاع الإلكتروني من اخطر التهديدات التي تواجه الدول في الوقت الحالي نتيجة تشابك المصالح وتسابق الدول الكبرى باستخدام كافة إمكانياتها وطاقاتها التكنولوجية عن طريق اختراع وتطوير أنواع مختلفة من الأسلحة الإلكترونية النووية والبيولوجية والتي شكلت بمختلف أنماطها وأنواعها تهديدا للأمن الدول نتيجة الاختراق والقرصنة وللانتقال الحرب من ساحة القتال إلى الفضاء الخارجي في الوقت الذي لا يمكن معه تصور وقوع إي نزاع دون إن يكون له جوانب وإبعاد إلكترونية، وعلى الرغم من المحاولات والمبادرات من الدول لحماية أمنها وتطبيق القانون الدولي الإنساني على النزاعات الإلكترونية إلى جانب الجهود الوطنية لمواجهته إلا إن الأمر يستدعي وجود قواعد ومبادئ قانونية دولية ملزمة لتنظيم جوانب النزاع الإلكتروني وذلك من خلال فرض الالتزامات على الدول وتقيد حريتها بخصوص الأسلحة الجديدة التي تصنعها لتحول دون إمكانية استخدامها في تهديد امن الدول أو سلامتها الاقليمية وهذا لا يتحقق إلا بتعاون وتكاتف المجتمع الدولي وبمختلف اركانه وحضاراته.

الكلمات المفتاحية: الحرب الإلكترونية، الأسلحة إلكترونية، القانون الدولي الإنساني

Abstract

Electronic conflict is one of the most dangerous threats that states face at the present time in light of the intertwining interests

and the competition of major countries using all their technological capabilities and energies by inventing and developing various types of nuclear and biological electronic weapons, which, in their various types, have posed a threat to the security of states as a result of penetration and piracy and for the transition of war from the battlefield to Outer space at a time with which it is impossible to imagine the occurrence of any conflict without its sides and electronic deportations, and despite several attempts and initiatives by states to protect their security and apply international humanitarian law to electronic conflicts as well as national efforts to confront it, the matter calls for the existence of binding international legal rules and principles to regulate aspects of electronic conflict by imposing obligations on states and restricting their freedom regarding weapons The new ones that they create to prevent them from being used to threaten the security of states or their systems are necessary, and this can only be achieved with the cooperation and intensification of the international community and its various civilizations.

Key words: electronic warfare, electronic weapons, international humanitarian law.

المقدمة

إن النزاع ظاهرة قديمة عرفته البشرية منذ الوجود بحيث نشأ العنف مع الإنسان عندما حاول قتل اخية من اجل الاستحواذ على ملكه، وتطورت إشكاله ووسائله وتنامت إلى إن أصبحت أفه تهدد استقرار وامن الدول، وقد شهدت الدول في الآونة الأخيرة صورا جديدا للنزاعات تحت مسمى الحرب المعلوماتية (الإلكترونية)القت بظلالها على مختلف مناحي حياة الإنسان الاجتماعية والاقتصادية والأمنية والسياسية نتيجة لقيام الدول الكبرى بصنع الأسلحة المختلفة(النووية والبيولوجية والكيماوية)وظهور الجماعات المتطرفة الجهادية التي ترتكب الجرائم الإرهابية الأمر الذي يحتم على الدول ضرورة اليقظة والتحرك لحماية أمنها بإتباع منهجية وخطط تحوي متطلبات الأمن على المستوى الدولي والوطني وتطبيق مبأدى القانون الدولي الإنساني فبالرغم من الاختلاف الكبير في طبيعية ووسائل وأساليب النزاعين، لاسيما بعد ما أصبح النزاع

الإلكتروني خطر حقيقي وواقعي، وتزداد خطورته يوما بعد يوم بتطور الأدوات والتنفيذ المرتبطة بالتقنيات ووسائل المعلوماتية.

هدف البحث: يسعى البحث لبيان مفهوم الحرب الإلكترونية وتاريخ ظهوره باعتباره نوع جديد من الحروب التي تهدد العلاقات الدولية والسلم والأمن الدوليين لاسيما بعد التطور التقني الذي شهدته الدول في مجال الانترنيت إلى جانب بيان مدى خضوعه لقواعد القانون الدولي الإنساني .

مشكلة البحث: تظهر مشكلة البحث في تطور وتغير إشكال الصراع البشري وانتقاله من ساحات القتال إلى ساحة الفضاء الافتراضي وغياب القوانين الدولية التي تنظم الجوانب والاتجاهات الإلكترونية ومن هنا يثور التساؤل عن:

١- ما المقصود بالحرب الإلكترونية؟ ومتى نشأت؟

٢- ماهية الأسلحة الإلكترونية الحديثة؟ وما هي المقاطعات التي تستهدفها؟

٣- هل تملك الدول إستراتيجية وقواعد خاصة لمواجهه الحرب الإلكترونية والحد من أثارها أم أنها تكتفي بتطبيق قانون الحرب الخاص بالنزاعات التقليدية عليه؟

منهجية البحث: نعتمد في بحثنا على المنهج التاريخي والتحليلي من خلال بيان تاريخ ظهور الحرب الإلكترونية والوقوف عند تحليل النصوص وبيان قواعد القانون الدولي الإنساني لمعرفة مدى فاعليته وإمكانية تطبيقه على النزاعات ذات طابع إلكتروني .

هيكلية البحث: للإجابة القانونية على التساؤلات المطروحة نقسم البحث إلى مبحثين نوضح في الأول مفهوم الحرب الإلكترونية مع بيان جذوره التاريخية إلى جانب التطرق إلى أنواع وأنماط الأسلحة الإلكترونية وذلك في مطلبين، إما المبحث الثاني سنخصصه لبيان مدى إمكانية إخضاع النزاعات الإلكترونية للقواعد القانون الدولي الإنساني إلى جانب التطرق إلى استراتيجية الدول وجهودها في مواجهته يتبعه خاتمة متضمنا أهم الاستنتاجات والمقترحات التي توصلنا إلية.

المبحث الأول

الحرب الإلكترونية ووسائلها

شهدت البشرية تطور وتقدما تقنيا كبيرا وفي مختلف المجالات وانعكس على العلاقات الدولية، وأصبح العالم أشبه بالقرية الصغيرة وأصبح الفضاء السيبراني ذات دور كبير في حركة وإقامة العلاقات الدولية التي بدأت بدورها تؤثر في أمن الدول وتصاعد التهديدات الإلكترونية مما جعل العلاقة بين التكنولوجيا وأمن الدول علاقة طردية، فكلما تطورت وسائل التكنولوجيا تزايد تعرض أمن الدول وعلاقتها إلى إخطار وقرصنة إلكترونية وتحولت الصراعات من ارض وساحات القتال الاعتيادية إلى عالم افتراضي وفضاء تقني يعتمد على كل ما هو جديد من الوسائل والأسلحة الإلكترونية والتي تعمل على تهديد الدول، فعليه وللإحاطة بموضوع البحث ينبغي تقسيم المبحث إلى مطلبين نخصص الأول لمفهوم الحرب الإلكترونية ونشأتها في حين نخصص المطلب الثاني لبيان وسائل وأسلحة الحرب الإلكتروني ووفق التفصيل الأتي :

المطلب الأول

مفهوم الحرب الإلكترونية وتاريخ نشأتها

لا يوجد للحرب الإلكترونية تعريف محدد ودقيق متفق عليه دوليا، إنما اجتهد عدد من الخبراء وكلا حسب اختصاصه ووجه نظره بإيراد تعاريف مختلفة، فقيل انه نوع من النزاع يحدث في الفضاء الإلكتروني وتكون ذات طابع سياسي يتمثل بمجموعة من الإجراءات التي تقوم بها إحدى الدول بغية اختراق أجهزة الكومبيوتر والشبكات العائدة لدول أخرى بقصد إلحاق الضرر فيه[١].وباعتباره مجموعة من الإجراءات الإلكترونية التي تستخدم فيه النظم والوسائل التقنية للاستطلاع والإشعاع الكهرومغناطيسية الصادرة من نظم العدو ومعداته الإلكترونية والاستخدام المتعمد للإشعاع للتأثير المباشر على شكل النظم الحربية[٢] ، وقال البعض أنها حرب خيالية وافتراضية ذات

(١)الحرب الإلكترونية، مقال منشور في موقع ويكيديا وعلى الموقع الإلكتروني : https://ar.wikipedia.org/wiki/%D8%AD%D8%Bتاريخ الزيارة ٢٠٢٠/٧/١
(٢)فيصل محمدالغفار،الحرب الإلكترونية،ط١،الجنادرية للنشر والتوزيع،الأردن،لبنان،٢٠١٦،ص٦.

طبيعة ونتائج ملموسة تحدث بلا دماء وتتلخص في المواجهات والبرامج التقنية والجنود الإلكترونية للتهديد والتخريب لأجهزة العدو[١].وانه صراع إلكتروني يكون دوافعه سياسية وتستخدم فيه قدرات هجومية ودفاعية إلكترونية بهدف إفساد الشبكات والنظم المعلوماتية والبنية التحتية وذلك باستخدام الأسلحة الإلكترونية من قبل الفاعلين أو القوى المتعاونة داخل المجتمع الدولي.[٢]

وذهب البعض إلى التقريب بين الحرب الإلكترونية والفيروسات البيولوجية من ناحية إلية العمل ويعرفها على أنها الوحدات المركزية المتطورة والمتقنة التي تعمل على نشر الوباء الإلكتروني في الجسم المراد من خلال إرسال المعلومات الرقمية والمدمرة والهادفة للتخريب والتنصت والتجسس فهي أشبه بأسلحة جرثومية صنعها الإنسان. [٣]

ومن خلال استعراض التعاريف السابقة يمكن القول بان الحرب الإلكترونية لها جوانب عدة ، فهي حرب رقمية تستهدف إفراد ومؤسسات ودول وسلاحها وسائل ونظم التكنولوجية والاتصالية بأنواعها المختلفة وتحدث في البيئة الرقمية، وبذلك يمكن وضع تعريف لها على أنها النزاع الخطير الذي يحدث في الفضاء الإلكتروني وتعد جزءا من الحرب الرقمية التي تهدف إلى التأثير المباشر على إرادة الطرف الأخر وقدرته في صنع القرار فيما يتعلق بالقيادة العسكرية في مجال العمليات الإلكترونية عن طريق تشويش وإلحاق الضرر بأجهزته وأنظمته العسكرية، وان الحروب الرقمية تقوم على أساس عنصرين احدهما توفر المعلومات والأخر توفر القدرات العقلية والذهنية التي تكون مسؤولة بشكل مباشر عن تخطيط وتدبير وتوجيه الضربات الإلكترونية وزخم المعلومات في الفضاء السيبراني.[٤]

(١) مساعد كمال، الحرب الافتراضية وسيناريوهات محاكاة الواقع، بحث منشور في مجلة الجيش اللبناني، ع٢٥٣، ٢٠٠٦، ص٣.

(٢) عادل عبد الصادق، أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني، ط١، وحدة الدراسات المستقبلية، الإسكندرية ٢٠١٦، ص٣٩.

(٣) وليد غسان، دور الحرب الإلكترونية في الصراع العربي والاسرائيلي، رسالة ماجستير في جامعة النجاح الوطنية، فلسطين، ٢٠١٣، ص٨٢.

(٤) غريس فرح، التكنولوجيا وتطور قدرات العقل البشري، بحث منشور في مجلة الجيش اللبناني، ع٣٢٤، ٢٠١٢، ص٤٠.

ونرى بان توافر العنصرين السابقين مطلب أساسي في إي حرب تقوم سواء كانت تقليدية إلكترونية ام لا، وان تطور وسائل الاتصال وأدواتها هي جنود الحرب التي تحتاج إلى شبكة معلوماتية نابعة من العقل البشري وبالطريقة يمكنها من تحقيق الهدف المقصود، وتنجم عن هذه الحروب مخاطر عدة لا تقف عند استهداف المواقع والادرع العسكرية وحسب، وإنما بإمكانه استهداف المواقع الحكومية الحساسة وشبكات النقل والأنظمة المالية ومؤسسات النفط وتلوث المياه وتدميرها والوصول إلى كل المواقع الحساسة في البلد المراد وإحداث انفجارات ضخمة وتلاعب وزرع الفيروس، ومن الأدلة الواضحة عليه فيروس (ستاكس) الذي وجهته الولايات المتحدة الأمريكية وإسرائيل في سنة ٢٠١٠ إلى أجهزة الحواسيب والمنشآت الإيرانية النووية مستهدفتا أجهزة التخصيب النووي الإيراني.(١)

وعند البحث عن جذورها التاريخية نجد بان بدايتها تعود إلى الفترة التي سبقت اندلاع الحرب العالمية الأولى عندما بدأ الاتصال بين مختلف أرجاء العالم باستخدام المواصلات اللاسلكية وجهاز البرق الصوتي، غير انه أصبح محل اهتمام منذ اندلاع الحرب العالمية الثانية، فكانت أول حرب إلكتروني سنة ١٩٠٥ هي الحرب الروسية اليابانية اذ كانت السفن اليابانية تراقب الأسطول الروسي عن كثب وترسل جميع المعلومات إلى القيادة اليابانية إلى إن التقط احد قادة الزوارق الروسية الإرسال وطلب استعمال جهاز الإرسال الموجود في زورقه لإعاقة الإرسال وجوبه طلبه بالرفض وبعد فترة وجيزة تمكن من تشويش تلك إلارساليات وبدون الحصول على أذن مسبق أو الموافقة (٢). ولجأت النمسا ايضا إلى الحرب الإلكترونية بعد ادراكها أهمية التجسس والتصنت واعتبارها إحدى أهم وسائل التجسس على الأوضاع العسكرية للعدو بعد ماكان هذا الأمر موكلا سابقا إلى العملاء والجواسيس فضلا عن تعرضهم للمخاطر، وبنشوب الخلاف والازمة السياسية بينهم وبين ايطاليا في عام ١٩٠٨ بسبب مقاطعتي

(١) الحرب الإلكترونية واستخدام التقنية الحديثة في الإعمال العسكرية وعلى الموقع الإلكتروني :https// www.utradeksa-تاريخ الزيارة٢٠٢٠/٧/٧

(٢) جاسم محمد البصيلي، الحرب الإلكترونية وأسسها وأثرها في الحروب، ط٢، دار المؤسسة العربية للدراسات والنشر، بيروت، ١٩٨٩، ص٤١.

بوسينا وهيرس يجوفينا سرعان ما استخدمت النمسا أجهزة التصنت والتجسس الإلكتروني على الاتصالات اللاسلكية الايطالية وتمكنوا من فك رموزها [١].وفي حرب فيتنام استخدم الفيتناميون صواريخ سامة تجاه طائرات الفانتوم الأمريكية وقامت أمريكا بإدخال تعديلات على الطائرة التابعة لها لتكون طائرة حرب إلكترونية وتحمل أجهزة تشويش ضد رادارات وصواريخ سامة وبعد تحقيق النجاح بدأ فيتنام بإجراء تعديل وتركيب أجهزة التشويش على الطائرات العائدة له .[٢]

وخلال الحرب العالمية الأولى تمكنت إحدى السفن الانجليزية عام ١٩١٤ من إرسال معلومات عن تحرك بعض القطع الحربية الألمانية في البحر الأبيض المتوسط عن طريق الراديو وتمكن من رصد تلك الرادارات وتشويشها وبذلك قام الانكليز عام ١٩١٦ بوضع موجات إرسال في معركة جوتلايز والتي حددت موقع الأسطول الألماني وأخبرت القيادة الانكليزية به، الأمر الذي دفع الألمان إلى نصب واستخدام أجهزة الحرب الإلكترونية المسمى (bormide) للتشويش الخداعي .[٣]وتعرضت استونيا للهجمات شرسة من قبل الحكومة الروسية في سنة ٢٠٠٧ عند قيامها بمحاولة نقل النصب السوفيتي التذكاري العائد للحرب العالمية الثانية مما اثأر موجة غضب لدى روسيا فاستخدمت وسائل إلكترونية فاوقفت ٩٨% من المعاملات المصرفية الاستوانية عبر الانترنيت وشل قطاعات أخرى في الدولة [٤].وفي الحرب بين روسيا وجورجيا سنة ٢٠٠٨ استخدم الطرفين هجمات إلكترونية سميت بنمط القوة الصلبة ونجم عنها تخريب كابلات الاتصال والنظم المعلوماتية والمنشات الحيوية بشكل هدد أمن الدولة والسكان واخذت الحرب طابعا تنافسيا بلجوء كلا الطرفين إلى استخدام أمكانتها التقنية، وأكدت ألمانيا في عام ٢٠١٠ تعرضها إلى التجسس من قبل روسيا

(١) صلاح الدين الأشرم، الحرب الإلكترونية من الحرب العالمية الأولى إلى حرب النجوم، ط٢، دار طلاس للدراسات والترجمة والنشر، دمشق، ١٩٩٣، ص ٢٥.
(٢) جاسم محمد البصيلي، مصدر سابق، ص٤٢.
(٣) فيصل محمد الغفار، مصدر سابق، ص٤.
(٤) لوران جزيل، ماهية القيود التي يفرضها قانون الحرب على الهجمات السيبرانية، مقال منشور في موقع اللجنة الدولية للصليب الأحمر تاريخ الزيارة ٢٠٢٠/٧/٧ icrc.http/www..resources/documents/ara/ora

والصين واستهدفت القطاعات الصناعية والمهمة في البلد ومن بينها شبكة الكهرباء[١]. وتعرضت محطة (نطايز) النووية الإيرانية في عام ٢٠١١ إلى هجمات إلكترونية من قبل الولايات المتحدة التي استخدمت برنامج stuxnet وألحقت إضرارا كبيرا في العمليات الحساسة الخاصة بتخصيب اليورانيوم.[٢]

لذلك عند تتبع تاريخ الحرب الإلكترونية فان جذورها تعود إلى الفترة التي سبقت اندلاع الحروب العالمية عندما بدأ اتصال بين دول العالم وظهر أجهزة التواصل اللاسلكي والبرق الصوتي وتبادل المراسلات واستخدام السفن في نقل الرسائل في المؤانئ وتزايد الشوشرة والتداخل بين أجهزة الدول ونجم عنه انتقال اغلب الحروب إلى الفضاء، وارتبط تطور الحرب وأدواتها بتطور وسائل الاتصال الرقمية من خلال إرسال التقارير والاستطلاع، واستمر الصراع بين الدول لابتكار احدث النظم اللازمة للسيطرة والتشويش وإدارة إعمال القتال وأداء مهامها بكفاءة عالية في بيئة رقمية وفي الزمان والمكان المناسبين وارتبط نجاح الحروب بأسلحتها الإلكترونية المتطورة، وان النماذج التي تم ذكرها ما هي إلا دليل على تطور إشكال وأنماط النزاعات المسلحة التي تهدد الأمن والسلم وتستدعي تحركا وعلى المستوى الدولي والإقليمي لدرء مخاطرها .

المطلب الثاني

وسائل الحروب الإلكترونية

هناك عدة أنواع من الأسلحة الإلكترونية تختلف فيما بينها باختلاف تأثيراتها، وعادة تستهدف قطاعات محددة وذات أهمية ولمعرفة أنواع الأسلحة وكذلك آلياتها والمقاطعات لابد من التطرق إلى كل منها بشكل موجز من خلال النقاط الآتية:

الفرع الأول: أسلحة الحروب الإلكترونية: هناك عدة أسلحة إلكترونية يتم استخدامها وان هذه الأسلحة تختلف فيما بينها باختلاف تأثيراتها فأما يكون لها تأثير بسيط أو

(١) عادل عبد الصادق، مصدر سابق، ص٣٢.

(٢) احمد عبيس نعمة الفتلاوي، الهجمات السيبرانية، مفهومها، والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، بحث منشور في مجلة المحقق الحلي للعلوم القانونية والسياسية، ع٤، س، ٢٠١٦، ص٦١٩.

كبير، ولذلك يمكننا بيان أهم الأسلحة الإلكترونية والتي يتم استخدامها كوسائل الحرب الإلكترونية ومنها:

١- التجسس ألمعلوماتي: يقصد به وسائل التجسس التقني والتي تعتبر احد أشهر وأقدم الأسلحة التي استخدمت منذ بداية الاستعمال الإنساني لوسائل الاتصال والتواصل[١] وتتخذ وسائل التجسس المعلوماتي عدة إشكال إما إن تكون عن طريق التجسس على المعلومات الصادرة من أجهزة الحواسيب والصادرة عن المحطات الطرفية أو يكون عن طريق اعتراض المراسلات الإلكترونية عن الأقمار الصناعية والهواتف .

٢-الاختراق الإلكتروني: هي نوع من أنواع الجرائم التي ترتكب ضد الإفراد وتلحق ضررا تصيب الضحية بأذى نفسي أو جسدي بشكل مباشر أو غير مباشر.[٢]

٣- القرصنة الإلكترونية: تعتبر القرصنة من أضخم واشمل الأسلحة الإلكترونية المستخدمة عبر الفضاء الرقمي، وان هذا السلاح الرقمي يشمل على غالبية وسائل الصراع الإلكتروني وذلك لشمولية مفهومه ومضمونه.[٣]

٤- شبكات التواصل الاجتماعي: هي منظومة من الشبكات الإلكترونية التي تسمح للمشترك فيها بإنشاء موقع خاص به، ومن ثم ربطه عن طريق نظام اجتماعي إلكتروني مع أعضاء أخرى لديهم نفس الاهتمامات والهوايات.[٤]

٥- الأقمار الصناعية: وهي من الأسلحة ذات دلالات استحواذية هدفها السيطرة على اكبر قدر ممكن من المعلومات، وذلك عن طريق التقاط الصور وإرسالها لقاعدة

(١) جاسم جعفر ، حرب ألمعلوماتي بين ارث الماضي وديناميكية المستقبل، ط١، دار البداية للنشر والتوزيع، عمان، ٢٠١٠ ، ص ١٧١.

(٢) غفران علي ، شهد عبد الصمد ، الاختراق الإلكتروني، المنشور على الموقع الإلكتروني sites<colawuobaghdad.edu.ip. تاريخ الزيارة ٢٠٢٠/٧/٩.

(٣) علوه رأفت، قرصنة الانترنيت ، ط١، مكتبة التجمع المصري للنشر والتوزيع ، ٢٠٠٦ القاهرة، ص٢٣-٢٤.

(٤) رضا إبراهيم عبدا لله، مواجهة نشر الشائعات من شبكات التواصل الاجتماعي في الفقه الإسلامي والقانون الوضعي ، أطروحة دكتوراه، كلية الحقوق /جامعة طنطا، ٢٠١٩، ص١٢.

المعلوماتية الموجودة على الأرض، وتعتبر هذا نوع من الأسلحة الإلكترونية من أكفأ وسائل التقنية.([١])

٦- أسلحة الناتو تكنولوجية: تعتبر هذا نوع من الأسلحة من أكثر أنواع إثارة فهو يهتم بتعميم الأجهزة التقنية في غاية الدقة، وذلك من خلال وضع الذرة بجوار الذرة للحصول على الشكل أو التكنولوجيا المطلوبة.([٢])

٧- قنابل التعليم الميكروفية: يعتبر هذا نوع من الأسلحة من مولدات الطاقة، كالمزودات الكهربائية، الرادارات ومحطات تزويد بالخدمات الانترنيت ومراكز الاتصالات وكذلك شبكات السلكية واللاسلكية وغيرها من وسائل تزويد الطاقة والمعلومات [٣]

٨- الإرهاب الإلكتروني: يقع هذا النوع في المستوى الرابع في الفضاء الإلكتروني وانه مصطلح يستخدم لوصف الهجمات الغير الشرعية التي تقوم بها الفاعلون غير الدوليين وتكون ضد أجهزة كومبيوتر والشبكات وعلى هذه الأساس لا يمكن اعتبار أي هجوم إلكتروني إرهاب إلكتروني إلا إذا نجم عنه أذى مادي للأشخاص والممتلكات. [٤]

الفرع الثاني: إلية عمل الحروب الإلكترونية :تقوم إلية الحروب الإلكترونية بدرجة الأولى على توافر عنصرين مهمين في أي صراع إلكتروني في الفضاء الرقمي، وان أول هذه العناصر وهي توافر المعلومات والتي ترتكز عليها الحروب التكنولوجية بشكل كبير وهذا العنصر يعتبر أول باب عمل الحروب الإلكترونية، إما العنصر الثاني فهو القدرات الفعلية والذهنية والتي تكون مسؤولة عن تخطيط وتوجيه الضربات الإلكترونية

(١) حرب الفضاء والأقمار الصناعية – صراع استراتيجي جديد ، المنشور على موقع شبكة النبأ المعلوماتيةwww.annabaa.org تاريخ زيارة الموقع٢٠٢٠/٧/١٢.

(٢) سلامة صفات، أسلحة الحروب المستقبل بين الخيال والواقع، ط١، مركز الإمارات للدراسات والبحوث الإستراتيجية ، أبو ظبي، ٢٠٠٥، ص٢٨-٢٩.

(٣) جاسم جعفر ، حرب ألمعلوماتي في الماضي وديناميكية المستقبل ، مصدر سابق، ص١٣٦.

(٤) المنشور على الموقع الإلكتروني stuies.aljazeera.net تاريخ زيارة٢٠٢٠/٧/٧.

في العالم [١]وان عنصري المعلوماتية والقدرات الفعلية البشرية تتبعها الإجراءات الفنية والقائمة على أساس تنفيذ الخطوات واليات الحروب الإلكترونية عبر الفضاء الرقمي [٢] وتنقسم إلاليات إلى نوعين :

١- عمليات الهجوم الإلكتروني: وهي عملية اعتداء مبرمج من حاسوب موجه نحو حاسوب أخر لاختراق جدار حمايته وفتح ثغرة للبث فيه، وتكون على نوعين: الأول يكون مخصص في التركيز على حاسوب واحد ويكون ذلك سبب في توقفه عن العمل، إما الثاني يكون اخطر من الأول وذلك لان هدفه الأساسي ليس فقط إيقاف عمل نظام الجهاز بل اقتحامه والنيل من أدوات الحماية فيه لتمكن من سرقة ما موجود فيه من بيانات كما ان هناك حالات تستطيع فيه هذه الهجمات إن تسيطر على جهاز الضحية بشكل كام.[٣]

٢- عمليات الدفاع الإلكتروني: وتشمل الإجراءات والوسائل الوقائية وذلك للحد من ردة فعل الخصم الهاجم وتتخلص تلك العمليات بالمنع والوقاية والتي تهدف إلى حماية النظم المعلوماتية للطرف الهاجم وذلك لكشف الاختراقات الرقمية في حالة حدوثها، أو وضع خطط استبيانيه لمنع وقوع أي اختراقات معلوماتية .[٤]

الفرع الثالث: القطاعات التي تستهدفها الحروب الإلكترونية: وتعني الأهداف والمقاطعات التي تستهدفها الحروب الإلكترونية ومن أهمها:

١- قطاع الاتصالات والمعلومات: وتعني به محطات الاتصال السلكي واللاسلكي وشبكات إرسال المعلومات وتعتمد تكنولوجيا الاتصالات بشكل رئيسي على البصريات الإعلامية والسمعية ومن هذه التكنولوجيات (الهاتف –الأقمار الصناعية –الأنسجة البصرية[٥]، وتعد هذه القطاعات مواءمة للحروب الإلكترونية لاعتمادها

(١) خالد محمد ، الحروب الإلكترونية ، موسوعة علوم، سلسلة الكتاب العلمي العسكري، ط١، المكتبة العالمية، بغداد، ١٩٨٦، ص٨٨.
(٢) سلامة صفات ، مصدر سابق، ص٣٨-٣٩.
(٣) المنشور على الموقع الإلكتروني www.arageek.com//hittp: تاريخ زيارة ٢٠٢٠/٧/١٢.
(٤) سلامة صفات، مصدر سابق، ص٣٨-٣٩.
(٥) عبد الرزاق تومي، تكنولوجيا المعلومات ودورها في التنمية الوطنية – دراسة ميدانية بولاية أم بواق، رسالة ماجستير، جامعة قسطينية ، ٢٠٠٥-٢٠٠٦، ص٥٦.

بشكل كامل على وسائل الاتصال الحديثة ويتضمن هذه القطاع عدة جوانب حساسة ويكون لها دور كبير في بناء البنية التحتية والاتصالية للدولة[١].

٢- قطاع الإعمال العسكرية والحربية: شهدت القطاعات العسكرية والحربية تطورات عديدة في مجالات ذات اعتمادية كبيرة على عنصر المعلوماتية والرقمية وحولتها إلى بناءات تتسلح بأجيال جديدة من الأسلحة التكنولوجية والاتصالية وازدادت قدراتها وفعاليتها على الدعم اللوجستي والتواصل ألمعلوماتي والاستخباراتي القائم على توافر عنصر التقنية الحديثة، وارتبطت تلك المرافق ارتباطا وثيقا بالتطورات الرقمية والاتصالية ورافقها تهديدات أمنية يكشف نقاط الضعف في هذه المرافق لتحولها إلى أهداف واضحة[٢].

٣- قطاع الطاقة والتوزيع الفيزيقي: يشكل هذا النوع من القطاعات البناء الأساسي للبنى التحتية الكاملة لأي دولة في العالم اذ أنها تتضمن العديد من القطاعات الهامة ومنها الأمن القومي –الأمن السياسي والاقتصادي، وارتباط الطرق عبر الخرائط الإلكترونية ومراكز مراقبة الكوارث الطبيعية وغيرها من الإدارات المسؤولة عن قطاعات توليد الطاقة داخل أي بلد وبما إن هذه القطاعات ترتبط ارتباطا كثيفا بوسائل الانترنيت وشبكات الداخلية والخارجية لذا فإنها تكون أكثر عرضه من غيرها للاستهداف [٣]

٤- قطاع المعلومات الإعلامية والمجتمعية: تشترك وسائل الإعلام والصحافة مع وسائل والاتصال الجماهيري في العديد من الوظائف والأهداف اذ أصبحت الصحافة جزءا أساسيا من نسيج الحياة اليومية للناس العاديين وإنها متنوعة بالرغم

(١) ذياب البداينة، الأمن وحرب المعلومات ، ط١، دار الشروق للنشر والتوزيع، عمان، ٢٠٠٦، ص٣٦-٣٧.

(٢) بو رجيلي ريمون، التكنولوجيا الحديثة في المجالات العسكرية ، المنشور على الموقع الإلكتروني www.leb army.gov تاريخ الزيارة ٢٠٢٠/٧/١١.

(٣) ذياب البداينة، مصدر سابق، ص٣٩.

من التحدي الذي فرضته وسائل الإعلام الأخرى مثل المذياع والتلفاز[١]، وان هذه القطاعات خطت خطوات جبارة تجاه اشتراكها العملي مع وسائل الإعلام الإلكتروني، وتعمل كمؤثر نفسي في الصراعات الإلكترونية التي قد تنشا بين الإطراف المتخاصمة والتي تعرف بالحرب الإعلامية[٢]

٥- القطاعات الإنسانية: تتضمن هذه القطاعات الطابع المعنوي والتي تقوم بتعزيز القيم الإنسانية والاعتبارات الوطنية والاجتماعية وغيرها من القيم التي يحتاجها الإنسان لتعزيز وضعه في ظل التأثيرات الذي قد يتعرض له إثناء تجواله عبر الفضاء الإلكتروني[٣].

المبحث الثاني

استراتيجية الدول في مواجهة الحرب الإلكترونية

باستمرار تسابق الدول الكبرى والمتقدمة تكنولوجيا فيما بينها للهيمنة وفرض السلطة على الفضاء الإلكتروني عن طريق الهجمات الإلكترونية والتجسس والقرصنة المعلومات والبيانات الضرورية للدولة المعادية ولانتقال النزاع إلى الفضاء ولتطور إشكالها التي أصبحت مرهونا ومرتبطا بتقدم التقني للدول وتخلف اثأر مختلفة وبدرجات متفاوتة من حيث الضرر والشدة والتي تصيب المنشأت الحيوية وتلحق إضرارا بسكان المدنيين، فكان لزاما على الدول إن تتسارع لوضع خطط واستراتيجية معينه لحد من الآثار الناجمة عن هذه النوع من الحروب وبيان القواعد القانونية الدولية الواجبة أو بالامكان تطبيقة عليه، وبذلك يثور التساؤل عن مدى خضوع الحرب الإلكترونية لقانون الدولي الإنساني ؟ وما هو موقف الدول أو الجهود الدولية والإقليمية في هذا المجال؟

(١) خالد أمين عبد الفتاح ، اثر الصحافة الإلكترونية على التنمية السياسية الفلسطينية في فلسطين(الضفة الغربية-قطاع الغزة في عام ١٩٩٦-٢٠٠٧)، رسالة ماجستير ، جامعة النجاح الوطنية، كلية الدراسات العليا، ٢٠٠٨، ص١١-١٢.

(٢) بدران عباس، الحرب الإلكترونية – الاشتباك في عالم المعلومات ، المنشور على الموقع الإلكتروني www.stideshare.net تاريخ زيارة ٢٠٢٠/٨/١.

(٣) جاسم جعفر ، مصدر سابق، ص٦٥-٦٦.

هل تملك الدول استتراتيجية مناسب لمواجهته؟ وللإجابة عليه قسمنا المبحث إلى مطلبين وكالاتي :

المطلب الأول

تطبيق القانون الدولي الإنساني على الحرب الإلكتروني

يهدف القانون الدولي الإنساني ومنذ نشوئه إلى الحد من اثأر النزاعات المسلحة الدولية وغير الدولية وحماية السكان المدنين والأهداف المدنية من خلال وضع القواعد والضوابط التي تنظم وتحكم سير العمليات العسكرية، وعلى الرغم من عدم قدرته على منع الحرب باعتبارها أمر واقع لا محال له الا انها وضعت مبادئ في ضوء الحرب التقليدية وفرضت التزامات على عاتق الإطراف المتنازعة ومع تطور إشكال الحرب من مفترض وجود ضوابط لحماية الفئات المدنية في سياق النزاعات الجديدة وبذلك يثور التساؤل عن مدى إمكانية تطبيقه على النزاعات الجديدة أو بالأحرى النزاعات الإلكترونية؟ لا تملك إي دولة القدرة في فرض سيادتها وسيطرتها على الفضاء بشكل كامل مما أدى ذلك إلى استخدامها بشكل يضر الإنسانية، ولأجل التخفيف والحد من الخسائر الناجمة عنها سعت بعض الدول إلى اعتبارها نزاعات مسلحة وتطبق علية قانون الحرب المطبق على النزاعات التقليدية غير إن الجدل فقهي لا يزال قائما بين الإطراف والجماعات في مسالة تطبيق القانوني الدولي الإنساني من عدمه ولكل جهة وطرف حجج وبراهين.

واعتبر الفقه الأمريكي والأوربي الفضاء الخارجي مكان غير خاضع لأي قانون معين وان إي تصرف وعمل مباح فيه وبالتالي لا يمكن تطبيق قوانين الحرب على النزاعات التي تحدث فيه، كما ورفض أصحاب هذا الاتجاه التعامل القانوني مع الانترنيت لكونه لا يتفق مع الواقع التقليدي، ونصوص القانون الدولي الإنساني تخلو من الإشارة إلى الهجمات الإلكترونية على شبكات الحاسوب أو الحرب المعلوماتية، وان التكنولوجيا والانترنيت حديثه نسبيا ولم تكون موجودة عند وضع قانون النزاعات

وان الأخير لا يتلائم مع وسائل الحرب الإلكترونية .[١]ومن الحجج التي استند إليها أصحاب هذا الرأي هي عدم وجود إي مفهوم أو مصطلح يشير إلى الحرب الإلكترونية في ميثاق الأمم المتحدة واتفاقية لاهاي أذ انها أوردت مفهوم الهجوم المسلح واستخدام القوة في النزاعات وغيرها من المفاهيم وخير امثال على ذلك النزاع بين استونيا وجورجيا والتي استمرت الهجمات الإلكترونية فيها لفترة معينة وألحقت إضرارا جسيمة بالطرفين غير انه لم تعد نزاعا مسلحا بالمعنى الحقيقي ولم تخضع لقواعد الحروب [٢].وباعتبار ان إي نشاط إلكتروني استخدم لإغراض عسكرية لا يعد هجوما ولا تنطبق عليه مفهوم الهجوم المسلح وفقا للمادة ٤٩ من البروتوكول الإضافي الأول والذي نص على(إن الهجوم المسلح هي الهجمات وإعمال العنف الدفاعية والهجومية ضد الخصم)وان هذا الأمر لا يتحقق لكون الهجوم الإلكتروني لا يصاحبه أو لا ينتج عنه عنف مسلح وتأثير مباشر .[٣]

في ضوء ما تقدم لا يمكن الاعتماد على الفقرة ١من المادة ٤٩ أعلاه وبمعزل عن باقي إحكام البروتوكول لتحديد وتحقيق العنف والهجوم المسلح في إي نشاط إلكتروني، ودليل على ذلك إن إعمال العنف تنجم عنه اثأر مباشرة تلحق بالمدنيين أو تكون ذات ثاثير وضرر لاحق أو غير مباشرة بعد وقوع الهجوم كتعطيل مفاعل الطاقة الكهربائية وبذلك يكون التركيز على الضرر وجسامته التي تلحق بالمدنيين لوصف النشاط الإلكتروني بالهجوم المسلح ولاسيما إن الفقرة ٢ من المادة ٤٩ للبروتوكول حظر الهجوم وبث الذعر والتهديد ضد السكان المدنيين، وتأكيدا على ما ذكرناه فان ديباجة قرار الجمعية العامة (مكافحة إساءة استعمال التكنولوجيا والاتصالات)ذكرت خطورة اثأر الهجمات الإلكترونية وإنها غير محددة يمكن إن

(١) عمر محمود عمر، الحرب الإلكترونية في ضوء القانون الدولي الإنساني، بحث منشور في مجلة دراسات علوم الشريعة والقانون، مج ٤٦، ع٣، ٢٠١٩ ص١٣٦.
(٢) وليام، بارليتا، النزاع السيبراني والاستقرار الجيوسيبراني، ط١، الاتحاد الدولي للاتصالات والاتحاد العالمي للعلماء، ٢٠١١، ص٥١-٥٢.
(٣) احمد عبيس نعمة، مصدر سابق، ص٦١٨.

تصيب كل نواحي الحياة وتسبب دمارا شاملا للأعيان والأهداف المدنية وان البحث عن مدى خطورتها تقع في أولويات الدول.[١]

ونرى بان أصحاب هذا الراى استبعدوا إمكانية تطبيق القانون الدولي الإنساني على النزاعات الإلكترونية لأنهم يرون بان الحرب تتطلب جيوشا نظاميا وميدان القتال والمواجهة وتسبقها مرحلة إعلان على عكس الحرب الإلكترونية التي تتم عبر شبكات المعلومات وتوجه نحو المنشات الحيويه فهي اقرب إلى الإرهاب بتوصيفها وبعيدا عن مفهوم الحرب إلى جانب خلو ميثاق الأمم المتحدة وقانون الحرب من الإشارة إلى الحرب الإلكترونية، وان كنا نتفق معهم بخلو القانون الدولي الإنساني من الاشارة إليه وعدم إيرادها إي عبارات تشير إليه بوجه الخصوص غير اننا لا نتفق معهم ونرى إمكانية تطبيق قواعده ومبادئها بشكل يطبق على النزاعات التقليدية ولاسيما إن تلك المبادئ تشمل كل التطورات ذات العلاقة بالنزاع والتي اكدها البروتوكول الإضافي الأول الملحق باتفاقيات جنيف لعام ١٩٤٩من حيث التزام الدول عند اقتناء الأسلحة التحقق إن كان محظورا أم لا .[٢]ووفقا لنص البروتوكول أعلاه إذا ماعدا تكنولوجيا سلاح أو أسلوب من أساليب الحرب فيتوجب على الإطراف التأكد من مشروعيته قبل استخدامه ووفقا لقواعد القانون الدولي العام، كما ويمكن الاستدلال بالمبادئ الأساسية لقانون الدولي الإنساني وفي مقدمته شرط مارتينز باعتباره الحجر الأساس له وتم وضعه في ديباجة اتفاقية لاهاي الرابعة لعام ١٨٩٩ و١٩٠٧ بحيث نص على انه في حاله عدم وجود قاعدة محددة في القانون ألتعاهدي فان للمحاربين حق الحماية بموجب القانون العرفي ومبادئ الإنسانية التي يمليه الضمير العام [٣] وان كانت العبارة مبادئ

(١) ينظر قرار الجمعية العامة للأمم المتحدة رقم ٥٥/٣٦ لعام ٢٠٠٠

(٢) يلتزم أي طرف سام متعاقد عند دراسة أو تطوير أو اقتناء سلاح جديد أو أداة للحرب إن يتحقق مما إذا كان محظورا في جميع الأحوال أو بعضها بمقتضى البروتوكول أو أية قاعدة أخرى من قواعد القانون الدولي التي يلتزم بها الطرف السامي المتعاقد، المادة ٣٦ من البروتوكول الاضافي الأول الملحق باتفاقية جنيف لعام ١٩٤٩ .

(٣)ينظر الموقع الإلكتروني: https://www.ahewar.org/debat/show.art.asp?aid=59179 تاريخ الزيارة ٢٠٢٠/٨/١٠

الإنسانية وما يمليه الضمير العام ينتابها الغموض من ناحية كونها قاعدة قانونية تتعلق بالأسلحة المستخدمة أم أنها مجرد مبادئ إنسانية غير ملزمة فإننا نجد بأنه لا يمكن الاستمرار بالشك في مدى تطبيقه لكون شرط مارتينز وسيلة لمواجهة التغيير التكنولوجي في نطاق العمليات العدائية وهذا ما اشارت إليه محكمة الولايات المتحدة الأمريكية عام ١٩٤٨ في قضية كروب لان شرط جزء من المعايير القانونية التي يمكن القياس واللجوء إلية بتطبيقه على المسائل التي لا تنظمها الاتفاقيات المحددة .([1]وان كان قانون الحرب لا توفر الحماية المطلوبة والمراد تحقيقه ولا تنظم بعض الجوانب مع ذلك يمكن تطبيقه على الحرب الإلكترونية بتطبيق مبدأ القياس مع المطالبة بضرورة عقد وإبرام اتفاقية دوليه ملزمة تنظم القضايا المتعلقة بالأمن والفضاء السيبراني وتفرض التزامات على عاتق الدول وتمنع بموجبة الاعتداءات الإلكترونية ، في حين اقر الفريق الثاني بإمكانية تطبيق القانون الدولي الإنساني على الحرب الإلكترونية وضرورة احترامه من قبل الإطراف ولا حاجة إلى وضع قواعد ومبادئ جديدة واستند بذلك إلى ما جاءت به ميثاق الأمم المتحدة المادة٢و٤ والتي حظرت على الدول الأطرف اللجوء إلى الحرب باستخدام القوة أو التهديد ضد الدول واستقلالها السياسي وسلامة أراضيها وبشكل لا ينجسم مع مقاصدها [٢].وان حفظ السلم والأمن الدوليين يقع على عاتق مجلس الأمن فله وبموجب اختصاصه سلطة وصلاحية تقديرية لتحديد المعنى الحقيقي للاستخدام القوة وحسب الظروف المحيطة وبغض النظر عن نوع النزاع إن كان تقليديا أم إلكترونيا [٣].ودليل الآخران ميثاق أعطت للدول الحق الكامل في الرد على الهجمات الإلكترونية التي تتعرض لها أو إي هجوم وتهديد مسلح من خلال حق الدفاع عن نفسه وبغض النظر عن نوع السلاح المستخدم .[٤]وعلى مجلس الأمن إن يحدد فيما إذ كان

(١) يحي ياسين سعود، الحرب السريانية في ضوء قواعد القانون الدولي الإنساني، بحث منشور في المجلة القانونية، مجلة متخصصة في الدراسات والبحوث القانونية isnn ٢٥٣٧-٠٧٥٨، ص٩١.
(٢) احمد عبيس نعمة، الهجمات السيبرانية، ط١، منشورات زين الحقوقية، بيروت، ٢٠١٨، ص٤٩.
(٣) يقرر مجلس الأمن ماذا كان وقع تهديد للسلم أو الإخلال به أو كان ماوقع عملا من إعمال العدوان، ينظر المادة ٣٩ من ميثاق الأمم المتحدة
(٤) ينظر المادة (٥١) من ميثاق الأمم المتحدة .

الهجوم قد شكل تهديدا أو خرقا للسلم أو انه من قبيل إعمال العدوان وان تصدر قرارا باتخاذ التدابير القسرية بحيث تجيز لأي دول تعرضت للهجوم إلكتروني الرد علية وباستخدامه وسائله إلكترونية كما فعلت أمريكا في سنة ٢٠١١ والهجمات ضد استوانيا ٢٠٠٧ اذ عدت من قبيل إعمال العدوان وتجيز حق اللجوء إلى الحرب خاصة إن ميثاق الأمم المتحدة في المادة ٥١ لم تشير إلى نوع الأسلحة المستخدمة والتي تجيز حق الدفاع واستخدام القوة للرد عليه.(١)

يضاف إلى ذلك إن الفقه الدولي اجمع على اعتبار الحرب الإلكترونية حربا حقيقية وبالمعنى الدقيق وذلك لما لها من اثأر مدمرة على العالم المادي وتسمح الرد من خلال الإلية الحديثة للدفاع ، في الوقت التي بينت فيه محكمة العدل الدولية إن المادة ٥١ من ميثاق لا تشير إلى نوع محدد من الأسلحة وطبقته على قضية نيكاراغوا ضد الولايات المتحدة الأمريكية في عام ١٩٨٦بشأن الأنشطة العسكرية المستخدمة (٢). وقد منح دليل تالين* للدولة الحق في الرد على الهجمات الإلكترونية التي تتعرض لها من الدولة المعادية والتي تتسبب بخسائر كبيرة في الأرواح البشرية أو التي تسبب تعطل في أنظمة الكومبيوتر والحوادث الهندسية المتعمدة والتي تستهدف شبكة المعلومات وانهيار المحطات الطاقة النووية .(٣)

كما أكدت اللجنة الدولية للصليب الأحمر شرعية وضرورة تطبيق القانون الدولي الإنساني على الهجمات الإلكترونية، لكون العمليات والهجمات التي ترتكب إثناء النزاعات شانها شان إي أسلحة حرب أخرى بغض النظر عن نوع النزاع وتخضع في تنظيمها للقانون ذاته، لاسيما إن لجوء الدول إلى القوة محكوم بميثاق الأمم المتحدة

(1) see ،eg ،Schmitt ،m 1999 ،computer network atatck and the use of forse in international law .thoughts on a normative framework ،37 ،colum j trananat l.885.l

(٢) عمر محمود عمر، مصدر سابق، ص١٣٨ .

(٣) دليل تالين .*يذكر في المطلب الثاني ويتكون دليل تالين من ٢٨٢صفحة وبواقع ٩٥ مادة متضمنا القوانين الدولية الواجبة تطبيقة على الحرب الإلكترونية، وقسم الدليل إلى قسمين الأول اختص بالامن الإلكتروني والثاني خاص بالنزاعات الإلكترونية .ينظر شريف نسيم قلته، دليل تالين والهجمات الإلكترونية وحظر استخدام القوة في القانون الدولي، بحث منشور في مركز الفضاء العربي للابحاث الفضاء الإلكتروني، ع ١٦٤، ٢٠١٧، ص٢.

والمواثيق الدولية الاخرى المعنية بتنظيم السلاح والنزاعات المسلحة وعلى المتحاربين احترام وحماية المرافق المدنية الضرورية والمواد التي لاغني عنها لبقاء السكان المدنيين وان الاعتداء عليه من خلال الهجمات الإلكترونية تشكل انتهاكا للقانون الدولي الإنساني.[١]

وبالنسبة لنوع الأسلحة المستخدمة فإذا أمعنا النظر في التعريف التي أوردها لجنة الأسلحة التقليدية عام ١٩٨٦ بأنه أسلحة الانفجارات الذرية والمصنوعة .... وأسلحة الفتك الكيميائية والبيولوجية وأي نوع أخر من الأسلحة التي يتم تصنعيها في المستقبل وتتشابه خصائصها في الأثر التدمري مع القنبلة .وبالتالي إن إيراد عبارة إي نوع من الأسلحة يتم صنعها في المستقبل تتسع وتدل شموليته للهجمات الإلكترونية التي تحدث في الفضاء من اختراق شبكة المعلومات والحواسيب وينجم عنه إضرار تلحق بالمدنيين من جراء تعطل السدود والاحتياجات الأساسية والتي يصعب فيه الحد من أثره التدمري وبالتالي تشمل العبارة ألاسلحة الإلكترونية المستخدمة في نطاق النزاعات الحديثة .[٢]

نجد إن للدول الحق الكامل في الرد على الهجمات التي تتعرض لها أو إي تهديد مسلح وبغض النظر عن نوع الأسلحة المستخدمة في الهجمات وسواء كان الهجوم واقعا في العالم الحقيقي أم في الفضاء الافتراضي واتخاذ التدابير اللازمة للتأمين وحماية أنظمتها وذلك للدفاع عن النفس المقرر لها بموجب ميثاق، إلى جانب الصلاحية الواسعة وحق التدخل لمجلس الأمن في اعتبار الفعل الواقع تهديد للسلم والأمن الدوليين وبذلك يعد النزاع الإلكتروني حربا حقيقة، وان مفهوم استخدام القوة ورد مطلقا ولم يحدد نوع الأسلحة المستخدمة فيه وبذلك إن كل ما يقع إثناء النزاعات الإلكترونية تخضع في تنظيمها للقانون الدولي الإنساني ما دام ينتج عنه نفس الآثار التي تنتج عن استخدام الأسلحة التقليدية، غير إن الاكتفاء بتطبيق القانون الدولي

(١) فرونيك كريستوري، القانون الدولي الإنساني توفر طبقة إضافية من الحماية، تقرير عن الحد من التسلح في اللجنة الدولية للفريق العامل المفتوح العضوية المعني بالتطورات في ميدان المعلومات والاتصالات في سياق الأمن الدولي، ١٠ أيلول، ٢٠١٩.

(٢) يحي ياسين سعود، مصدر سابق، isnn ٢٥٣٧-٠٧٥٨ص٨٤-٨٥

الإنساني وان كانت ذات أهمية كبيرة الا انها لا تحقق الحماية الكافية لوجود فراغ قانوني وجوانب كثيرة لم يتطرق إلية بالتنظيم، كما انه عند تطبيقه على الحرب الإلكترونية لا نضفي الشرعية على الأخيرة ولا نشجع عسكرة وتسلح الفضاء وانما ندعو الدول إلى حل خلافاتها وبالطرق السلمية وإبرام اتفاقية ووضع قواعد مبنية على أساس مبادئ وقواعد القانون الدولي الإنساني.

المطلب الثاني

الجهود الدولية والإقليمية لمواجهة الحرب الإلكترونية

نظرا لأعتماد الدول على الأنظمة الإلكترونية بشكل كبير فقد اصبحت هدفا للهجوم ومصدرا لتهديد اقتصاد الدول التي تتعرض للهجمات الخطيرة من قبل عصابات الجريمة المنظمة والارهابين وازدادت الجرائم الإلكترونية بحيث بلغ عدد هجمات القرصنة حوالي ٢٦مليون عملية مابين السطو على البيانات والحسابات والاعتداء على أنظمة المعلومات بفترة قصيرة جدا، الأمر الذي اقتضى ضرورة تضافر الجهود لردع الهجمات السيبرانية.[١] وبذلك ابرمت أول معاهدة دولية (معاهدة الفضاء الخارجي)لحظر استخدام أسلحة الدمار الشامل على الإجرام السماوية وإقامة المنشات والقواعد العسكرية في عام ١٩٦٧وبمصادقة الدول التي كانت ترتاد الفضاء، غير انه مع التقدم والتغيير أصبح الالتزام ببنود المعاهدة بعيدة المنال في الوقت الحالي .[٢]

اذ بدا اهتمام المجتمع الدولي بالنزاع الإلكتروني منذ عام ١٩٩٠، إذ عقد أول مؤتمر قانوني للتشاور حول التهديدات الإلكترونية في الكلية البحرية عام ١٩٩٩التي عدت الهجوم الإلكتروني من اخطر أنواع التهديد للأمن الوطني للدول وبعد تعرض استونيا للهجمات شرسة في ٢٧ نيسان ٢٠٠٧زاد اهتمام الدول وتغيرت رؤيتها نحو النزاعات المسلحة التي تحدث في الفضاء وكرست جهودها لوضع استتراتيجية للامن

(١) عادل عبد الصادق، الانترنيت والاتصالات، ساحة جديدة للتجسس الدولي، ط١، المركز العربي للأبحاث، القاهرة، ٢٠٠١، ص١٠.

(٢) محمد محمود السيد، حرب الفضاء، مستقبل الصراعات والقوى الكبرى حول الأقمار الصناعية، تقرير صادرعن مركزالمستقبل للأبحاث والدراسات المتقدمة العدد٣١،١٨أغسطس ٢٠١٩، ص٤

الإلكتروني.[١] وقد تضمنت وثيقة وزارة الدفاع الأمريكي الموضوعة عام ١٩٩٩مجموعة من المقترحات لدراسة المعاهدات تنظم أمور والقضايا المتعلقة بالحرب الإلكترونية من خلال تحليل وبيان إي مخطط ونشاط يرتكب وإمكانية احتواءه وخضوعه لقانون الحرب لكن يبدو ان المجتمع الدولي غير قادر على إنتاج قانون ينظم سلوك الحرب الإلكترونية وعدم وجود سبل قانونية للتصدي. [٢]

ففي هذا سياق بادرت بعض الدول الكبرى لوضع سياسات دفاعية ووقائية كالولايات المتحدة الأمريكية واستراليا، فخصصت مبالغ وميزانية كبيرة لتأمين الفضاء الإلكتروني ومعالجة مسائل الأمن السيبراني لاسيما إن اقتصادها متصل اتصالا وثيقا بالفضاء الافتراضي ولكون العلاقات الدولية أصبحت معرضة للتهديد بصورة مستمرة بسبب الاختراقات والاعتداءات على الشبكة العالمية وقواعد البيانات [٣].والأمن السيبراني بحسب التقرير الذي صدر عن الاتحاد الدولي للاتصالات في ٢٠١٠ هي مجموعة من الأنشطة ووسائل وإجراءات أمنية ومبادئ توجهيه لأجل حماية البيئة السيبرانية والمؤسسات من الاعتداء وباعتباره نشاط يوفر حماية للموارد الحيوية والمالية المتعلقة بالتقنيات .[٤] اذ ادركت الدول خطورة القرصنة والهجمات التي تأتي من الفضاء فسارعت لحماية مصالحها من خلال توفير الأمن السيبراني ، فتبنت الدول مبادرات مختلفة ومن امثلته تبني الاتحاد الأوربي استتراتيجية الأمن الإلكتروني عام ٢٠١٣وركزت على جرائم الانترنيت وضرورة التزام الدول الإطراف بمواجهة الحرب الإلكترونية وصد هجماتها [٥]. وفي عام ٢٠٠٣ قدم داي كوجيمن رئيس قسم الحرب الإلكترونية في الصين اقتراحا إلى القادة للقيام بإعداد واستخدام كل جهودها وإمكانياتها لصد إي هجمات إلكترونية المحتمل تعرض لها، وقد صرح اوباما الرئيس الأمريكي

(١) يونس عرب،قانون الكومبيوتر،ط١منشورات اتحاد المصارف العربية ' القاهرة،٢٠٠١، ص٢٤.
(٢) عمر محمود عمر، مصدر سابق، ص١٤٠.
(3) http://www.techno.branchezvou.com>/actualite.تاريخ الزيارة١٠/٨/٢٠٢٠.
(٤) منى الأشقر ، الأمن السيبراني، التحديات ومستلزمات المواجهة، بحث مشارك في اللقاء السنوي للمختصين في امن وسلامة الفضاء السيبراني، بيروت، ٢٧-٢٨اب ٢٠١٢، ص١٠.
(٥) عمر محمود عمر، مصدر سابق، ص١٣٥.

السابق في عام ٢٠٠٩ بخطورة الفضاء السيبراني والمخاطر المحيطة بأمنها وعدم قدرتها على تامين البنية الرقمية التابعة لهم وتوفير الحماية اللازمة تأكيدا منه على الإخطار المحدقة بأمنهم الفضائي .[١] وقبل ذلك أكد بيل كلينتون الرئيس الأمريكي الاسبق على ضرورة التصدي للإرهاب ألمعلوماتي التي تقودها جماعات جهادية والتي تشكل تهديدا إلكترونيا لدول العالم والتي تعود بصفه عامة إلى انحراف أخلاقي وفكري لدى مرتكبة وتزداد خطورته في حال ما إن ارتبط بالإرهاب النووي والكيماوي.[٢]

فقامت منظمة حلف شمال الأطلسي (الناتو) في عام ٢٠١٤ بوضع استتراتيجية خاصة تسمح لاعضاءها بالدفاع واستخدام القوة في حال تعرضهم للاختراقات والهجمات الإلكترونية بحيث أصبح الدفاع الإلكتروني جزءا من خطط الدفاع الجماعي والتي تفرض على الدول تسخير قدراته وامكانيتة لحماية الشبكات المعلوماتية .[٣]

وبجهود من اللجنة الدولية للخبراء القانونيين وبناءا على دعوة من حلف شمال الأطلسي تم وضع دليل تالين في عام ٢٠١٢ لتنظيم الحرب الإلكترونية وتطبيق القانون الدولي الإنساني عليهم، إذ تم كتابته من قبل العلماء السياسين وعلى رأسهم مايكل سميث وبعد إجراء التعديل علية تم نشره في فبراير ٢٠١٧وباسم (Tallinn) وعلى الرغم من انه غير ملزم للدول الاانه له ثاثير واسع النطاق على المفاوضات بين الدول وبشكل تعكس رؤية أمريكية للحرب التي كانت محل انتقاد من قبل الدول الكبرى [٤].كما عقدت اللجنة المؤتمر الدولي ٢٨ في عام ٢٠٠٣ وفرضت على جميع الإطراف بإخضاع الأسلحة الجديدة لاستعراض دقيق ولضمان عدم استخدامها في الهجمات الإلكترونية وتأكيدها على الالتزام بالمادة ٣٦ من البروتوكول الإضافي الأول

(1) larrywortzel china s cyber offensive wall street journal 1now 2009. نقلا عن احمد عبيس نعمة

(٢) إدريس عطية الطيب، الظاهرة الإرهابية في زمن مابعد الحداثة، دراسة تحليلة في الأساليب والإشكال،بحث منشورفي مجلة عربية للدراسات الأمنية،مج ٣١، ع٦٣،الرياض، ٢٠١٥،ص٢٥

(٣) نايلة صليبي، الحرب الإلكترونية بين الافتراضي والواقع وعلى الموقع الإلكتروني :تاريخ الزيارة ٢٠٢٠/٨/١٠-https://www.mc-doualiya.com/chronicles/email: mcd/20160624

(٤) شريف نسيم قلته، مصدر سابق، ص٥.

للعام ١٩٧٧التي فرضت على الدول تقييم مشروعية الأسلحة الجديدة .[١] وقد أوكلت الأمم المتحدة إلى المجلس الاقتصادي والاجتماعي واللجنة الخاصة بالعدالة الجنائية مهمة ومسؤولية متابعة المسائل والقضايا المتعلقة بالأنترنيت والجرائم الوطنية العابرة للحدود، في الوقت نفسه تعاون المكتب الخاص ب (undoc) والتابع لها مع الاتحاد الدولي للاتصالات بمساعدة الدول الإطراف على عقد مذكرة تفاهم في منتدى القمة العالمية للحد من مخاطر الجرائم السيبرانية[٢]. ولمنع تسليح الفضاء عقد الأمم المتحدة اجتماعا في اذار ٢٠١٩ بجنيف وبمشاركة ٢٥ دولة وسمي بالاجتماع المغلق لأجل إبرام معاهدة جديدة غير أنها لم تصل إلى مبتغاها على خلفية انعدام الثقة والتعاون بين الدول الكبرى والتي تملك زمام الأمور.[٣]

وصفوة القول نجد انه على مر التاريخ شهد المجتمع الدولي تغييرا وصعودا في قضايا الأمن والعلاقات الدولية وضعف بعض الدول وصاحب التغير موجة من التطورات في مجال استخدام الانترنيت بشكل يضر الإنسانية ، وتحول الفضاء إلى ساحة جدية للصراعات تخوضها الجماعات الإرهابية وتعددت أنماط الصراع بين ما هو اقتصادي وعسكري وسياسي، ولخطورته سعت الدول للاستجابة للتطور الحاصل في إشكال الحروب والوسائل الجديدة وأبدت مبادرات ومحاولات لإبرام اتفاقية وبدعم من الأمم المتحدة التي طالما تسعى بكل أعضائها لحماية الأمن والسلم الدوليين غير أنها باتت بالفشل ولحد ألان لم تتمكن الدول من تامين وحماية أمنها الإلكتروني ، لذلك الحل الوحيد للحماية من الهجمات هو ابرام اتفاقية تتضمن شروط وقواعد التنافس في الفضاء بين الدول وهذا لايتم إلا بتوافر الإرادة السياسية لديهم كما كان الحال ابان

(١) ماهي القيود التي تفرضها قانون الحرب، على الموقع إلكتروني :تاريخ الزيارة ٢٠٢٠/٨/١٢: https://www.icrc.org/ara/resources/documents/faq/130628-cyber-warfare-q-and-a-eng

(2) economic and social council resolution 1992/22 implemention of general assembly resolution46/152concerning operational activities and coordinathonin the field of crime prevention and criminaljustic 30 july 1992 p7.

(٣) محمد محمود السيد، حرب الفضاء، مستقبل الصراعات والقوى الكبرى حول الأقمار الصناعية، مصدر سابق، ص٥.

الحرب الباردة إلى جانب إصرار وتأكيد الدول على الآثار الناجمة عن الحرب الإلكترونية والتي لا يمكن التغاضي عنها أو السكوت عنه كما حصل خلال انتشار الأسلحة البيولوجية والكيميائية إلى إن تم حظرها .

وعلى المستوى المحلي أكدت العديد من الدول خطورة تكنولوجيا الإرهاب التي باتت تشكل خطرا على الدول العربية ، وتستدعي المواجهة الإلكترونية الحاسمة لحماية أنظمة والمعلومات المهمة ، وهذا الأمر أكده الخبير امن المعلومات وأستاذ التكنولوجيا في مصر محمد الجندي عندما أشار إلى عدم وجود إي قوانين مصرية تواجه الإرهاب الإلكتروني وطالب بتشريع قانون يجرمه بعدما أصبح الإرهاب والتجسس الإلكتروني لا يقتصر على تنظيمات إرهابية فقط وإنما ظهر متطوعون وجماعات مسلحة في مجال الانترنيت يعملون لحساب جماعات الجهاد الإلكتروني والتي استخدمت الانترنيت لارتكاب الجرائم الإرهابية.[١]وقد اتبعت العديد من الدول العربية كالعراق وسوريا والإمارات سياسية جديدة لحماية المواقع الإلكترونية وتجريم الدخول غير القانوني وغير المشروع للأنظمة المعلوماتية باعتباره جريمة وفرض عقوبات من خلال سن التشريعات تنظميه وجزائية .[٢] وان كنا نثمن الجهود التي قامت بها الدول في مجال مواجهة الحرب الإلكترونية من خلال اتخاذ جملة من التدابيروعلى المستويات الأمنية والتشريعية وتفعيل استراتيجيات وخطط العمل لتأمين الأمن الإلكتروني إلا إن القضية تستدعي تعزيز الجهود وتقويتها وسن تشريعات مقترنة بجزاءات تفرض على مرتكبيها.

الخاتمة

بات معروفا إن التطور والتغير المستمر في جوانب الحياة المختلفة انعكس على طبيعة النزاعات المسلحة، إذ انتقلت من ساحات المواجهة القتالية إلى ساحة الفضاء الخارجي ولاسيما بعد تطور وتنوع الأسلحة الإلكترونية التي تمتلكها الدولة

(١) محمد صفوت، جيل جديد من الحروب في مواجهة الإرهاب، تقرير يصدر عن مركز تكنولوجيا في مصر، ٢٤، أغسطس، ٢٠١٧، ص٣.

(٢) على سبيل المثال قانون المعاملات الإلكترونية العراقي رقم ٧٨ لسنة ٢٠١٢ والقانون الإماراتي رقم ٢ لسنة ٢٠٠٦ الخاص بمكافحة جرائم تقنية المعلومات والقانون رقم ٤ لسنة ٢٠٠٩ الخاص بالتوقيع الإلكتروني والشبكات في سوريا .

الكبرى، وفي ظل غياب القواعد والمبادئ القانونية والدولية ملزمة ومنظمة لها فعلية توصلنا إلى جملة من النتائج والتوصيات :-

أولا / النتائج

١-ظهر في السنوات الأخيرة نوعا جديدا من الحروب الدولية أطلقت عليها الحرب الإلكترونية وتختلف بكل مظاهرها وأسلحتها عن الحرب التقليدية المعروفة وشكلت تهديدا للمبادئ الأساسية للقانون الدولي ولسيادة الدول التي طالما نصت وأكدت علية المواثيق الدولية ولاسيما ميثاق الامم المتحدة.

٢- لا يزال مفهوم الحرب الإلكترونية غير واضح لدى الكثيرين وغير متفق عليه دوليا، الأمر الذي يكون حائلا دون إبرام اتفاقية خاصة ما لم يحدد مفهومه وطبيعته والتي تعد الأساس لأي اتفاقية دولية كما تعددت المسميات التي أطلقت علية مابين الحرب السيبرانية، حرب المعلوماتية ، حروب الأنترنيت والتي شكلت معضلة أخرى.

٣- لاشك إن التكنولوجيا ووسائل الاتصال الحديثة تمثل تطورا كبيرا في حياة الإنسان غير انه لا تخلو من المضار إذ تحمل بين طياتها مخاطر لا غنى عنها ولاسيما بعد لجوء الدول إلى استخدام طاقتها وتقدمها التكنولوجي لإغراض القرصنة والتجسس والإرهاب الإلكتروني وظهور جماعات إلكترونية مسلحة تحت مسمى الجهاد الإلكتروني

٤- إن القانون الدولي الإنساني له أهمية قصوى وإبعاد حقيقة لحماية ضحايا النزاعات المسلحة التقليدية غير انه عند تطبيقه وبكل مضمونه وقواعده وفحواه وإحكامه على الحرب الإلكترونية وان كان ذا دور لا يستهان به إلا انه لا تفي بالغرض ولا تحقق الحماية المطلوبة لاختلاف الكبير بين وسائل وأساليب القتال، وبالتالي تبرز حاجة ماسة لإبرام ميثاق أو معاهدة تنظم الحرب الإلكترونية.

ثانيا / التوصيات

١-تعد الحرب إحدى الحقائق الثابتة في حياة الإنسان وعلى مختلف المستويات سواء كانت التقليدية أم الإلكترونية ولا يمكن تجنبها غير انه يمكن التخفيف عن الآثار والمعاناة الإنسانية التي تخلفها من خلال فرض التزامات على الدول المتنازعة وفرض القانون بالقوة لحفظ الأمن والسلم الدوليين .

٢-ضرورة عقد اتفاقية أو معاهدة دولية ملزمة يكون عنوانه حظر أو تقييد استخدام الوسائل الإلكترونية للإغراض العسكرية لمنع التسلح داخل الفضاء الإلكتروني وتلزم الإطراف بالابتعاد عن الاستخدام غير السلمي للفضاء لكون الاتفاقية صمام الأمان للمعالجة القضايا الدولية ومن ضمنها الحرب الإلكترونية ، إلى جانب إنشاء جهاز دولي لمراقبة وتحقق من مدى امتثال والتزام الدول ببنود الاتفاقية الجديدة.

٣- تقع على عاتق الدول مسؤولية حماية أمنها وشبكاتها وتطوير قدراتها ووسائل الدفاع الإلكتروني لها لمواجهة الهجمات في الوقت التي أصبح فيه من الصعب توقع أو تخيل صراع عسكري دون إن يكون له إبعاد إلكترونية وذلك من خلال إنشاء مركز وطني يتضمن الأكفاء والمختصين في وسائل الدفاع الإلكتروني لصد هجمات التي تتعرض له المنشات العسكرية والمدنية.

٤- ضرورة تعزيز التعاون وتنسيق الجهود بين دول العالم لمواجهة الهجمات الإلكترونية بالمتابعة والكشف عن المواقع المشبوهة إلى جانب حماية المواقع والبيانات المهمة عن طريق تشفيرها ووضع رموز وأرقام حماية صعبة الاختراق من قبل الجماعات الإرهابية.

٦- على الدول إن تسن تشريعات جزائية وتنظميه للتعويض عن الإضرار التي تلحق بمصالحها نتيجة الهجمات الإلكترونية وفي حال وقوع ضحايا والقتلى يقتضي توجيه مسؤولية الجنائية الفردية للقادة ووفق القواعد القانونية الدولية ووفق الإحكام التي تقرها المحكمة الجنائية الدولية.

المصادر

الكتب

١-احمد عبيس نعمة ، الهجمات السيبرانية ، ط١، منشورات زين الحقوقية ، بيروت ، ٢٠١٨.

٢-جاسم جعفر ، حرب المعلوماتي بين ارث الماضي وديناميكية المستقبل، ط١، دار البداية للنشر والتوزيع، عمان، ٢٠١٠.

٣-جاسم محمد البصلي ، الحرب الإلكترونية وأسسها وأثرها في الحروب ، ط٢ ، دار المؤسسة العربية للدراسات والنشر، بيروت ، ١٩٨٩.

٤-خالد محمد ، الحروب الإلكترونية ، موسوعة علوم ، سلسلة الكتاب العلمي العسكري ، ط١، المكتبة العالمية ، بغداد، ١٩٨٦.

٥-ذباب البداينة، الأمن وحرب المعلومات ، ط١، دار الشروق للنشر والتوزيع ، عمان ، ٢٠٠٦.

٦-سلامة صفات، أسلحة الحروب المستقبل بين الخيال والواقع، ط١، مركز الإمارات للدراسات والبحوث الإستراتيجية ، أبو ظبي، ٢٠٠٥.

٧-صلاح الدين الاشرم ، الحرب الإلكترونية من الحرب العالمية الأولى إلى حرب النجوم ، ط٢، دار طلاس للدراسات والترجمة والنشر ، دمشق ، ١٩٩٣.

٨-علوة رأفت، قرصنة الانترنيت ، ط١، مكتبة التجمع المصري للنشر والتوزيع ، ٢٠٠٦.

٩-عادل عبد الصادق ، اسلحة الفضاء الإلكتروني في ضوء القانون الدولي الانساني ، ط١، وحدة الدراسات المستقبلية ، الاسكندرية ٢٠١٦.

١٠- عادل عبد الصادق ، الأنترنيت والاتصالات ، ساحة جديدة للتجسس الدولي ، ط١، المركز العربي للأبحاث ، القاهرة ، ٢٠٠١.

١١- فيصل محمدالغفار،الحرب الإلكترونية، ط١،الجنادرية للنشر والتوزيع ،الاردن،لبنان،٢٠١٦.

١٢-وليام ، بارليتا ، النزاع السيبراني والاستقرار الجيوسيبراني،ط١،الاتحاد الدولي للاتصالات والاتحاد العالمي للعلماء ، ٢٠١١.

١٣-يونس عرب ، قانون الكومبيوتر ، ط١ منشورات اتحاد المصارف العربية ' القاهرة ، ٢٠٠١.

رسائل واطاريح الدكتوراه

١- خالد امين عبد الفتاح ، اثر الصحافة الإلكترونية على التنمية السياسية الفلسطينية في فلسطين(الضفة الغربية-قطاع الغزة في عام ١٩٩٦-٢٠٠٧)، رسالة ماجستير ، جامعة النجاح الوطنية ، كلية الدراسات العليا، ٢٠٠٨.

٢- رضا ابراهيم عبدالله، مواجهة نشر الشائعات من شبكات التواصل الاجتماعي في الفقه الاسلامي والقانون الوضعي ، اطروحة دكتوراه، كلية الحقوق /جامعة طنطا، ٢٠١٩.

٣- عبد الرزاق تومي، تكنلوجيا المعلومات ودورها في التنمية الوطنية – دراسة ميدانية بولاية ام بواق، رسالة ماجستير، جامعة قسطينية ، ٢٠٠٥-٢٠٠٦.

المجلات

١- احمد عبيس نعمة الفتلاوي، الهجمات السيبرانية، مفهومها، والمسؤلية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر،بحث منشور في مجلة المحقق الحلي للعلوم القانونية والسياسية،ع٤،س، ٢٠١٦.

٢- ادريس عطية الطيب ، الظاهرة الارهابية في زمن مابعد الحداثة ، دراسة تحليلة في الاساليب والاشكال ، بحث منشور في مجلة عربية للدراسات الامنية ، مج ٣١، ع٦٣، الرياض ، ٢٠١٥.

٣- شريف نسيم قلته، دليل تالين والهجمات الإلكترونية وحظر استخدام القوة في القانون الدولي ، بحث منشور في مركز الفضاء العربي للابحاث الفضاء الإلكتروني ، ع ١٦٤، ٢٠١٧.
٤- عمر محمود عمر ، الحرب الإلكترونية في ضوء القانون الدولي الانساني ، بحث منشور في مجلة دراسات علوم الشريعة والقانون ، مج ٤٦، ع٣، ٢٠١٩
٥- غريس فرح ، التكنلوجيا وتطور قدرات العقل البشري ، بحث منشور في مجلة الجيش اللبناني ، ع٣٢٤، ٢٠١٢
٦- مساعد كمال ، الحرب الافتراضية وسيناريوهات محاكاة الواقع ، بحث منشور في مجلة الجيش اللبناني ، ع٢٥٣، ٢٠٠٦.
٧- يحي ياسين سعود ، الحرب السيرانية في ضوء قواعد القانون الدولي الانساني ، بحث منشور في المجلة القانونية ، مجلة متخصصة في الدراسات والبحوث القانونية .

التقارير

١-فرونيك كريستوري ، القانون الدولي الانساني توفر طبقة اضافية من الحماية ، تقرير عن الحد من التسلح في اللجنة الدولية للفريق العامل المفتوح العضوية المعني بالتطورات في ميدان المعلومات والاتصالات في سياق الامن الدولي.
٢-منى الاشقر، الامن السيبراني ، التحديات ومستلزمات المواجهة ، بحث مشارك في اللقاء السنوي للمختصين في امن وسلامة الفضاء السيبراني ، بيروت ، ٢٧-٢٨اب ٢٠١٢
٣-محمد صفوت ، جيل جديد من الحروب في مواجهة الارهاب ، تقرير صادرعن مركز تكنلوجيا في مصر ، ٢٤، اغسطس ، ٢٠١٧ .
٤-محمد محمود السيد ، حرب الفضاء ، مستقبل الصراعات والقوى الكبرى حول الاقمار الصناعية ، تقرير صادر عن مركز المستقبل للابحاث والدراسات المتقدمة العدد ٣١ ، ١٨ اغسطس ٢٠١٩.

القرارات الدولية

١- قرار الجمعية العامة للامم المتحدة رقم ٥٥/٣٦ لعام ٢٠٠٠.
٢- قرار مجلس الامن ماذا كان وقع تهديد للسلم أو الاخلال به أو كان ماوقع عملا من اعمال العدوان ، ينظر المادة ٣٩ من ميثاق الامم المتحدة.

المصادر الانكليزية

1- economic and social council resolution 1992/22 implemention of general assembly resolution 46/152 concerning operational activities and coordinathonin the field of crime prevention and criminaljustic 30 july 1992
2- larrywortzel china s cyber offensive wall street journal 1now

3- see ،eg ،Schmitt ،m 1999 ،computer network atatck and the use of forse in international law .thoughts on a normative framework ،37 ،colum j trananat l.885.l.

المواقع الإلكترونية

١- الحرب الإلكترونية ، مقال منشور في موقع ويكيديا وعلى الموقع الإلكتروني : https://ar.wikipedia.org/wiki تاريخ الزيارة ٢٠٢٠/٧/١.

٢- الحرب الإلكترونية واستخدام التقنية الحديثة في الاعمال العسكرية وعلى الموقع الإلكتروني : https// www.utradeksa-تاريخ الزيارة٢٠٢٠/٧/٧.

٣- بدران عباس، الحرب الإلكترونية – الاشتباك في عالم المعلومات ، المنشور على الموقع الإلكتروني www.stideshare.netتاريخ زيارة ٢٠٢٠/٨/١.

٤- بو رجيلي ريمون، التكنلوجيا الحديثة في المجالات العسكرية ، المنشور على الموقع الإلكتروني www.leb army.gov تاريخ الزيارة ٢٠٢٠/٧/١١.

٥- حرب الفضاء والاقمار الصناعية – صراع استراتيجي جديد ، المنشور على موقع شبكة النبأ المعلوماتيةwww.annabaa.orgتاريخ زيارة الموقع ٢٠٢٠/٧/١٢.

٦- غفران علي ، شهد عبد الصمد ، الاختراق الإلكتروني، المنشور على الموقع الإلكتروني sites<colawuobaghdad.edu.ip. تاريخ الزيارة ٢٠٢٠/٧/٩.

٧- لوران جزيل ، ماهي القيود التي يفرضها قانون الحرب على الهجمات السيبرانية ، مقال منشور في موقع اللجنة الدولية للصليب الاحمر . تاريخ الزيارة icrc٢٠٢٠/٧/٧ .ora/ara/resources/documents..http/www.

٨- نايلة صليبي ، الحرب الإلكترونية بين الافتراضي والواقع وعلى الموقع الإلكتروني : / ttps://www.mc-doualiya.com

٩- المنشور على الموقع الإلكتروني stuies.aljazeera.netتاريخ زيارة ٢٠٢٠/٨/١٠.

١٠- المنشور على الموقع الإلكتروني www.arageek.com: تاريخ زيارة ٢٠٢٠/٧/١٢.

١١- http://www.techno.branchezvou.com.تاريخ الزيارة١٠/٨/٢٠٢٠

١٢- الموقع الإلكتروني:https://www.ahewar.org تاريخ الزيارة ٢٠٢٠/٨/١٠