ISSN-2032-2075 مجلة رسالة الحقوق
الإصدار (17) العدد الثالث
يوليو – أغسطس – سبتمبر 2025

# الحرب السيبرانية وأثرها في القانون الدولي الانساني

# *Cyber warfare and its impact on international humanitarian law*

**بحث مقدم من قبل**
**أ.م.د. مسلم طاهر حسون**
**م.د. كريم لفتة مشاري**
**كلية القانون / جامعة أهل البيت (ع)**
**Dr. Muslim Tahet Hassoon**
**musllim al husainy @ gmail . com**
**Dr.karim Lafta Meshari**
**drkareemaljarahi@gmail.com**
**Ahl Bayyt university . College of law**

**الخلاصة:**
مما لا شك فيه ان العالم يشهد العديد من التحولات العميقة نتيجة النمو المتسارع في الشبكات الإلكترونية والتي ادت الى ظهور اشكال جديدة من العلاقات والنشاطات المختلفة وقد احدثت التكنولوجيا الحديثة للمعلومات والاتصالات ثورة شاملة في جميع نواحي الحياة الاقتصادية والاجتماعية والسياسية والثقافية والعسكرية والامنية ، وفي مقابل ذلك تزايدت المخاطر السيبرانية كلما تزايدت هيمنة تكنولوجيا الاتصالات والمعلومات على الحياه العامة فاصبحنا امام تحديات حقيقية عن طريق شبكة الانترنت بمختلف اشكاله ، وعلى هذا الاساس فأن تطور مفهوم الحرب السيبرانية في ظل تطور تكنولوجيا المعلومات حيث يمكن اعتبار تحدي الامن السيبراني اعلى التحديات للامن الوطني والدولي باعتبار التهديدات السيبرانية عابرة للحدود الوطنية فضلا عن أن هذه الهجمات السيبرانية تمثل تحدياً خطيراً على قواعد القانون الدولي الانساني وشغلت حيزا واسعاً من الاهتمام الوطني والدولي خصوصاً في ظل التطورات التكنولوجية المتسارعة في عالم الاتصالات الإلكترونية مما يستوجب التعاون الدولي لمكافحة الهجمات السيبرانية وهذا يتأتى من خلال ابرام المعاهدات الدولية الإقليمية والعالمية فضلا عن تشريع القوانين الوطنية التي تواكب التشريعات الدولية للتصدي للاعتداءات السيبرانية وتؤمن الامن السيبراني الوطني والدولي في وقت السلم والنزاعات المسلحة وقد تطرقنا في بحثنا هذا الى (الحرب السيبرانية وأثرها على القانون الدولي الانساني) من خلال بيان مفهوم الحرب السيبرانية وطبيعتها القانونية وأنعكاساتها على القانون الدولي الانساني فضلا عن الاليات الوطنية والدولية لمواجهتها.

**الكلمات المفتاحية:ـ الحرب السيبرانية ، الامن السيبراني ، القانون الدولي الانساني ، الاليات الوطنية والدولية ، التهديدات السيبرانية، الفضاء السيبراني .**

***Abstract***
There is no doubt that the world is witnessing many profound transformations as a result of the rapid growth in electronic networks, which has led to the emergence of new forms of relationships and various activities. Modern information and communications technology has brought about a comprehensive revolution in all aspects of economic, social, political, cultural, military and security life. In contrast, cyber risks have increased as the dominance of communications and information technology over public life has increased, so we have become facing real challenges through the Internet in its various forms. On this basis, the development of the concept of cyber warfare in light of the development of information technology, where the challenge of cyber security can be considered the highest challenge to national and international security, considering that cyber threats cross national borders, in addition to the fact that these cyber attacks represent a serious challenge to the rules of international humanitarian law and have occupied a wide area of national and international interest, especially in light of the rapid technological developments in the world of communications

***Keywords: Cyber warfare, cyber security, international humanitarian law, national and international mechanisms, cyber threats, cyberspace***

**المقدمة**

**اولاً :- موضوع البحث**

في بحثنا الحرب السيبرانية واثرها في القانون الدولي الانساني استخدمنا مصطلح الحرب السيبرانية للدلالة على آليات وأساليب القتال المستخدمة في عمليات الفضاء السيبراني اذ ترقى الى مستوى النزاع المسلح او تجري في سياقه وفق المعنى المقصود في القانون الدولي الانساني حيث ان اللجوء المتزايد للدول في استخدام الفضاء السيبراني لشن هجمات سيبرانية خلال النزاعات المسلحة جعل قواعد القانون الدولي الانساني امام تحديات حقيقية حول مدى تطبيق هذه القواعد على هذا النوع من النزاعات المسلحة.

**ثانياً :- اشكالية البحث**

ان موضوع البحث يثير اشكالية قانونية تتعلق في بيان مفهوم الحرب السيبرانية ومدى تطبيق قواعد القانون الدولي الانساني عليها حيث لاتزال قواعد هذا القانون وفق مبدأ ابرام اتفاقيات جنيف الاربعة لعام ١٩٤٩ والبروتوكولين الاضافيين الملحقين بها عام ١٩٧٧ تعد قواعد واجبة التطبيق على كافة العمليات التي تقوم بها الاطراف اثناء النزاعات المسلحة والتي ينبغي احترافها مع العرض أن وسائل الحرب وأساليبها تتطور باستمرار مع مرور الوقت ومع التطورات التكنولوجية في مجال الاسلحة المستخدمة في النزاعات المسلحة الحديثة وتبرز اشكالية البحث في مدى امتثال التكنولوجيا الحديثة للحرب السيبرانية لقواعد القانون الدولي الانساني.

**ثالثاً :- اهمية البحث**

تكمن اهمية البحث في هذا الموضوع في الوقوف حجم التهديدات بالحرب السيبرانية ولا سيما في ظل التطورات التكنولوجية ومدى تطبيقها لقواعد القانون الدولي الانساني وتبدو اهمية البحث في تسليط الضوء على التبعات الانسانية التي من المتوقع ان تنشأ من خلال اللجوء الى الحروب السيبرانية في القضاء السيبراني اثناء النزاعات المسلحة بالمقارنة مع آليات وأساليب النزاع في الحروب التقليدية.

**رابعاً :- منهجية البحث**

ان طبيعة البحث تستوجب اتباع المنهج التحليلي من اجل تحليل القواعد العامة للقانون الدولي الانساني لبيان مدى امكانية تطبيقها على انشطة الدول على الحروب السيبرانية في الفضاء السيبراني.

**خامساً :-.هيكلية البحث**

لغرض الاحاطة بموضوع بحثنا ( الحرب السيبرانية وأثرها في القانون الدولي الانساني ) سنتناوله ضمن مطلبين يسبقهما مقدمة ستخصص المطلب الأول لمفهوم الحرب السيبرانية من خلال فرعين نبين في الفرع الاول تعريف الحرب السيبرانية وفي الثاني نبين طبيعتها القانونية إما في المطلب الثاني سنتطرق الى تداعيات الحرب السيبرانية على القانون الدولي الانساني وذلك من خلال فرعين نتناول في الفرع الاول تطبيق قواعد القانون الدولي الانساني على الحرب السيبرانية وفي الثاني الآليات الوطنية والدولية لمواجهة الحرب السيبرانية وسوف نختم بحثنا لأهم ماتوصلنا اليه من نتائج ومقترحات

**المطلب الأول/ مفهوم الحرب السيبرانية**

ان الحرب السيبرانية يمكن ان تفهم الصورة واسعة على انها حرب تجري في الفضاء السيبراني باستخدام تكنولوجيا المعلومات والاتصالات والاعتماد المتزايد والمتسارع على الشبكات الالكترونية الذكية وانظمة المراقبة والرصد عن طريق منظومة الانترنت حيث تضع موارد الطاقة والدفاع والنقل والبنى التحتية في متناول الذين يسعون الى احداث الفوضى والتهديدات والاضطرابات والتوترات داخل الدول وعلى هذا الاساس فإن تعزيز الأمن السيبراني وحماية البنية التحتية تشكل حالياً عناصر حيوية في أمن كل دولة ورفاهيتها في المجالات كافة ([1]).والفضاء السيبراني يمثل العالم المادي والمفاهيمي الذي توجد فيه جميع الانظمة الالكترونية والبحث عن الامن السيبراني يعد من اهم مجالات الأمن في هذا العصر ،وعلى هذا الاساس تظهر اهمية البحث في تسليط الضوء على مدى انطباق القانون الدولي الانساني على الحروب السيبرانية في الوقت الراهن بالتطرق للجوانب القانونية المنظمة لتلك الحروب السيبرانية فضلاً عن كيفية تعامل القانون الدولي مع الاثار المترتبة للحروب السيبرانية ومحاولة القدرة على رصد جوانب هذه الحروب والمبادئ الحاكمة في ظل المتغيرات الحديثة ومحاولة كل دولة من دول العالم لتحقيق الامن السيبراني وسوف نتناول في هذا الاطار تعريف الحرب السيبرانية وانواعها وكالآتي:

**الفرع الاول/ تعريف الحرب السيبرانية**

السيبرانية في اللغة مصطلح مشتق من الكلمة اليونانية ( Kybernetes ) التي تعني القيادة والتحكم عن بعد ([2])، ومن الناحية الاصطلاحية فالحرب السيبرانية تعد عملية الكترونية سواء هجومية او دفاعية تتسبب في تدمير الاشخاص والاعيان وتتميز الحرب السيبرانية عن الحرب التقليدية في ان المفهوم التقليدي ينطوي على استخدام الجيوش النظامية ويسبقها اعلان واضح لحالة الحرب ( النزاعات المسلحة كما يسمى حديثاً ) وفي ميدان محدد لكن الحرب السيبرانية تمثل هجمات الفضاء الالكتروني غير محددة المجال وواسع نطاق وغامضة الاهداف كونها تتحرك وفق شبكات المعلومات والاتصالات العابرة للحدود الدولية فضلاً عن اعتمادها على ما يمكن وصفه بأسلحة الكترونية حديثة تتلائم وطبيعة السباق الالكتروني لعصر المعلومات اذ يتم التوجيه ضد المنشأت الحيوية ولذلك فإن أحد معايير التمييز بين الحرب السيبرانية

والحرب التقليدية يشير الى طبيعة السلاح المستخدم ومن ثم يمكن القول ان الحرب السيبرانية هي الحرب التي تستخدم فيها الاسلحة غير التقليدية طبقاً للآثار المترتبة على استخدام هذا النوع من الاسلحة الالكترونية ذات التدمير واسع النطاق ([3]).
وقد عرفت لجنة الاسلحة التقليدية للامم المتحدة الاسلحة غير التقليدية على انها اسلحة الانفجارات الذرية والاسلحة المصنوعة من مادة ذات نشاط اشعاعي واسلحة الفتك الكيميائية والبيولوجية واي نوع من الاسلحة الاخرى التي يتم تصنيعها في المستقبل والتي تتشابه خصائصها في الأثر التدميري مع القنبلة الذرية او الاسلحة الاخرى ([4])، ويلاحظ من التعريف ان ايراد اي نوع من الاسلحة الاخرى التي يتم تصنيعها في المستقبل يمثل اثر تدميري يقترب من تسمية الاسلحة غير التقليدية من اسلحة ذرية وبيولوجية وكيميائية ووردت لتشمل ماتخلفه الهجمات السيبرانية في اطار واسع النطاق مم اجتياز الحواسيب والشبكات الالكترونية العابرة للدول محل الهجوم وهذا يجعل المدنيين عرضة لخطر الحرمان من الاحتياجات والخدمات الاساسية اذا ماتعطلت تلك الانظمة عن العمل نتيجة الهجمات والحروب السيبرانية اذ يمكن ان تتعرض السدود والمحطات النووية والمنشآت العسكرية والمدنية وانظمة التحكم في الطائرات بشكل يصعب الحد من آثار تلك الهجمات السيبرانية مما يشكل آثار تدبيرية هائلة، وتعريف الحرب السيبرانية يثير مسألة على قدر من الأهمية تتعلق بوصف الهجمات السيبرانية كجزء من نزاعات مسلحة سواء أكان نزاع مسلح دولي ام غير دولي حيث القانون الدولي الانساني يمثل مجموعة من القواعد الاتفاقية او العرفية التي تسعى للحد من آثار النزاعات المسلحة لأسباب انسانية ومن ثم فإن ميدان القانون الدولي الانساني يشكل النزاع المسلح وعلى هذا الاساس ينبغي التمييز بين النزاعات المسلحة والنزاعات غير المسلحة وهذه العملية ليست من السهولة لاعتبارات الحرب السيبرانية ([5]). وجدير بالذكر ان مصطلح الحرب السيبرانية يستخدم للإشارة الى اشياء مختلفة بالإشارة الى آليات ووسائل واساليب القتال التي تتألف من عمليات في الفضاء الالكتروني ترقى الى مستوى النزاع المسلح او تدور في سياقه وفق المعنى المقصود في القانون الدولي الانساني ([6])، وتعرف اللجنة الدولية للصليب الاحمر الحرب السيبرانية على انها الافعال التي يتخذها اطراف النزاع لتحقيق ميزة على خصومهم في الفضاء السيبراني من خلال استخدام أدوات تقنية مختلفة وتقنيات تعتمد على البشر ومن الناحية النظرية يمكن تحقيق المزايا عن طريق اتلاف او تدمير او اعطاب او نهب انظمة الحاسوب لدى الخصم اي الهجمات السيبرانية او بالحصول على معلومات يفضل ان تكون سرية اي بالتجسس السيبراني([7]). من الاهمية بمكان القول من وجهة نظر قانونية ان المهم التمييز بين الحرب السبرانية بمصطلح العمليات الالكترونية المنفذة في اطار النزاعات المسلحة في القانون الدولي الانساني والعمليات الالكترونية خارج هذا الاطار حيث لا تنطبق قواعد القانون الدولي الانساني الا في ظل النزاعات المسلحة وبالتالي هذا يفرض قيوداً محدودة على الاطراف المشاركة في النزاع وعليه فان مصطلح الحرب السيبرانية يشير الى وسائل واساليب القتال التي تشمل العمليات الالكترونية التي تصل الى حد النزاع المسلح او تنفذ في سياقه في ظل المعنى المقصود في القانون الدولي الانساني فقط وتشمل الاسلحة المستخدمة في الحرب السيبرانية الفيروسات والديدان الحاسوبية وعمليات البيانات السيبرانية واجهزة تشويش اتصالات البيانات اللاسلكية وبرمجيات الحاسوبية المزيفة المشبوهة واسلحة النبض الكهرومغناطيسي وادوات استطلاعات الحاسوب والشبكات والقنابل الزمنية المدمجة لكون المعالم الدقيقة لاي حرب سيبرانية لا تزال غير محددة فان الهجمات السيبرانية ضد البنية التحتية للمعلومات وشبكات الانترنت تعطي صوراً عن النطاق المحتمل للنزاع في الفضاء السيبراني([8]).ومما سبق يمكن القول بان الحرب السيبرانية تمثل الاجراءات التي تتخذها الاطراف في نزاع مسلح لكسب الميزه العسكرية على خصومهم في الفضاء السيبراني باستخدام مختلف الادوات التكنولوجية والاشخاص التقنيين ضد البنى التحتية والشبكات الالكترونية للطرف الاخر تدميراً او اتلافاً او اختراقاً

**الفرع الثاني/ الطبيعة القانونية للحرب السيبرانية**

ان امكانية تطبيق قواعد القانون الدولي الانساني على الحرب السيبرانية قد يتطلب كأصل عام التكييف القانوني لها من حيث شرعية وعدم شرعية الحرب السيبرانية في ظل استخدام القوة في العلاقات الدولية فالعلاقة بين حق اللجوء الى الحرب وقانون الحرب تتميز بكونها علاقة توترات وصراعات لابد منها فالقواعد المعاصرة للقانون الدولي وفق ميثاق الامم المتحدة يحضر استخدام القوة او التهديد باستخدامها ([9]) باستثناء حق الدول في الدفاع الشرعي عن نفسها او بموجب([10]) استخدام تدابير انفاذ القانون التي يتخذها مجلس الامن([11]) وفي وقت نفسه فان قانون الحرب هدفه الاساسي التوازن والتوفيق بين ضرورات الحرب والقوانين الانسانية عن طريق فرض قيود واضحة وصريحة على سير العمليات العسكرية وعكس ذلك فان استخدام القوة في تسوية النزاعات الدولية والعلاقات الدولية يشكل عملاً غير مشروعاً طبقاً لميثاق الامم المتحدة وهذا اكدت عليه المادة ( ٤/٢ ) من ميثاق الامم المتحدة حيث نصت على انه ''يمتنع اعضاء المنظمة جميعاً في علاقاتهم الدولية عن التهديد باستعمال القوة او استخدامها ضد سلامة الأراضي او الاستقلال السياسي لأية دولة أو أي وجه آخر لا يتفق ومقاصد الامم المتحدة''([12]).ان الفضاء السيبراني لعب دوراً اساسياً في تعظيم الحرب السيبرانية والاستحواذ على عناصرها الاساسية في العلاقات الدولية حيث بات التفوق في هذا المجال يعد عنصراً حيوياً في تنفيذ عمليات ذات فعالية على الارض والبحر والجو والفضاء الخارجي من خلال الاستناد على القدرة القتالية في الفضاء الالكتروني وعلى نظم التحكم والسيطرة التكنولوجية وهذا الوضع يستوجب بالضرورة تغير مفهوم القوة حيث تعد القوة على انها مجموعة الوسائل والطاقات والامكانيات المادية وغير المادية المنظورة وغير المنظورة التي بحوزة الدولة ويستخدمها صانع القرار في فعل مؤثر يحقق مصالح الدولة وتؤثر في سلوك الوحدات السياسية الاخرى ([13])،وبالتالي فإن

عناصر القوة طبقاً لذلك يتمثل التناغم بين القدرات التكنولوجية والاقتصادية والعسكرية وارادة الدولة وغيرها مما يسهم في دعم امكانيات الدولة للوصول للأهداف سواء كانت تلك الاهداف مشروعة عندما تتوافق مع القواعد القانونية او غير مشروعة عند مخالفة قواعد القانون الدولي التي الزمت الجماعة الدولية من الامتناع في استخدام القوة او التهديد باستخدامها في العلاقات الدولية ومن ثم فان التغيير في مفهوم القوة سيؤدي بالضرورة الى تغيير في منظور الحرب حيث تحولت من سياق الحرب التقليدية المعتمدة على تدمير الخصم او الاستيلاء على موارده واحتلال ارضه الى حرب تسعى للاستحواذ على سباق التقدم التكنولوجي والتحكم بالمعلومات وسرقة الاسرار العلمية والاقتصادية فضلاً عن اختراق الامن القومي بدون طائرات او متفجرات او حتى انتهاك الحدود الوطنية وتدمير مواقع التجسس لمالها من تأثير يفوق الحرب التقليدية بما تشكله من نتائج واثار مدمرة على البنى التحتية والاقتصادية وعلى هذا الاساس فان مفهوم القوة في مجال الحرب السيبرانية له مدلولاته عن مفهومها التقليدي طبقاً لما ورد في ميثاق الامم المتحدة([14]). ومما تقدم فان الحرب السيبرانية المتمثلة بالهجمات السيبرانية تثير اشكالية تخص القواعد المتعلقة بحق اللجوء الى الحرب من حيث طبيعة تلك الهجمات في امكانية وصفها باستخدامها للقوة ومن ثم البحث في مشروعية او عدم مشروعيتها ووفقا للقواعد القانونية الدولية ولا سيما بعد انشاء منظمة الامم المتحدة والمتعلقة بعدم استخدام القوة او التهديد بأستخدامها في مجال العلاقات الدولية باستثناء حق الدفاع الشرعي او وفق قرار صادر من مجلس الامن بموجب الفصل السابع من ميثاق الامم المتحدة ([15]). حقيقة ان هذا الامر يزداد صعوبة في اطار عدم الاتفاق حول مفهوم القوة المستخدمة والتي تعد غير مشروعة وخاصة وان مجال الحرب السيبرانية ممكن تأخذ اشكال متعددة منها الثقافية والاقتصادية والعسكرية والأمنية والتي يمكن وصفها هجمات سيبرانية.

**المطلب الثاني/ تداعيات الحرب السيبرانية على القانون الدولي الانساني**

ان وضع الحرب يقف موقف القانون الذي يحكمها وهو القانون الدولي الانساني فاذا ما دارت هذه الحرب في نزاع بين الدول فقد يأخذ وصف الحرب فيكون هذا القانون هو الذي يحكم سلوك اطراف النزاع وعلى هذا الاساس فانه لا ينطبق القانون الدولي الانساني الا اذا نفذت العمليات الالكترونية في ظل نزاع مسلح وكانت مرتبطة به وجدير بالإشارة ان ميثاق الامم المتحدة واتفاقيات جنيف لعام ١٩٤٩ ولاهاي لعامي ١٨٩٩ و ١٩٠٧ ومعاهدة حلف شمال الاطلسي لم تتناول النزاع السيبراني ويستخدم ميثاق الامم المتحدة ومعاهدة حلف الشمال الاطلسي مصطلحات من قبل السلامة الاقليمية وهجوم مسلح وهي مصطلحات لا تنسجم مع التطورات السيبرانية ثم يضعها ظاهريا خارج نطاق القانون الدولي ([16]) وجدير بالذكر ان عدد من العمليات التي يشار اليها على انها من قبيل الحرب السيبرانية قد لا تنفذ في سياق نزاع مسلحه على الاطلاق وسنبحث في هذا الاطار مدى انطباق قواعد القانون الدول الانساني على الحرب السيبرانية والاليات الوطنية والدولية لمواجهة الحرب الاستبرانية

**الفرع الاول/ تطبيق قواعد القانون الدولي الانساني على الحرب السبرانية**

لا شك ان هنالك حاجة ضرورية للقيام بموائمة الحرب السيبرانية مع القانون الدولي الانساني لكون اعمال الحرب السبرانية سينتج عنها حرق احكام عديدة في القوانين الحالية او ستكون خارج نطاق هذه مما يعني احترام الاتفاقيات والاعراف الدولية وخاصة اتفاقيات جنيف الاربعة لعام ١٩٤٩ والبروتوكول الاضافي الاول المتعلق بحماية ضحايا المنازعات الدولية المسلحة واتفاقيات لاهاي الخاصة باحترام قوانين واعراف الحرب البرية ونظام روما الاساسي للمحكمة الجنائية الدولية([17]). وهذا السياق يتطلب احترام قواعد القانون الدولي الانساني والتي من الممكن تطبيقها على الحرب السيبرانية وذلك من خلال توفير قدر كافي من الحماية الدولية للبنية التحتية الحيوية لمنع كافة اوجه التدمير والمعاناة فضلاً عن ضمان الحد الادنى من الاتصالات الاساسية ذات الصلة بحمايو المدنيين ومن الضروري على الطرف المسؤول على هجوم سيبراني اتخاذ الاجراءات الى اقصى قدر الممكن من اجل تجنب وتخفيف الاضرار العرضية التي تلحق بالبنية التحتية المدنية والمدنيين مما يتطلب التحقق من طبيعة النظام التي تتعرض للهجوم والاضرار المحتملة التي قد تنتج عن احد الهجمات مما يعني عندما يصبح وشيكاً ان هجوماً يحقق اصابات او اضرار مدنية عرضية ينبغي الغائه او العدول عنه([18])، فضلاً عن ذلك على اطراف النزاع الالتزام باتخاذ الاحتياطات المطلوبة من اثار الهجمات بحيث تكون نظام الحواسيب العسكرية منفصلة بما فيه الكفاية عن الحواسب المدنية لحماية السكان المدنيين من اثار الهجمات السيبرانية العرضية والعشوائية وقد تساهم تكنولوجيا المعلومات في الحد من الاضرار العرضية التي تلحق بالبنى التحتية المدنية فقد يلحق تعطيل خدمات معينة تستخدم لاغراض عسكرية ومدنية اضرار اقل مما يلحق تدمير البنية التحتية وفي هذه الاوضاع يلزم مبدأ الاحتياط القابل للجدل التزاماً على الدول باختيار الوسائل الاقل ضرراً بغية تحقيق الاهداف العسكرية([19]).

ويمكن القول ان انواع العمليات الالكترونية التي تخضع للقواعد الانسانية التي تحكم سير العمليات العدائية والمدرجة ادناه يمكن ان تكون محظورة او وقانونية في سياق نزاع مسلح

اولاً :- تعطيل شبكة الكهرباء المدنية او نظام معالجة المياه دون الحاق اضرار مادية بها.

ثانياً :- توجيه هجوم يترتب عليه حرمان نظام مصرفي من خدمة الانترنت مما يكون له تأثير واسع النطاق على قدرة الملايين من عملاء المصرف على الحصول على الخدمات المصرفية. ثالثاً :- توجيه هجوم سيبراني ينتج عنه الحرمان من الخدمات المقدمة عبر نظام خاص لحجز رحلات الطيران عبر الانترنت لغرض التسبب في عدم تمكن السكان المدنيين من مغادرة مناطق النزاع.

رابعاً :- اغلاق شبكة الانترنت وشبكات الهاتف المحمول في منطقة معينة من الدولة لمنع الدعاية التي يطلقها الخصم([20]).

من القواعد الواجب تطبيقها من قبل الدول المتحاربة خلال النزاعات المسلحة يتمثل في احترام حياد الدول الاخرى غير الاطراف في النزاع وان لا تنقل اي نوع من الهجمات السيبرانية عبر البنى التحتية وهذا ما يتوافق مع اتفاقيات لاهاي لعام ١٨٩٩ و ١٩٠٧ التي تقيد نقل القوات وقوافل الامدادات او الذخائر عبر الاقليم او المياه المحايدة وعليه فان السماح للدول بشن الهجمات السيبرانية التي يمكن ان تجتاز من خلال العديد من شبكات الدول الاخرى دون علمها لا ينسجم مع القواعد الدولية للنزاع المسلح حيث يتطلب الحصول على تصريح من الدول الاخرى من قبل شن الهجوم السبراني ومن ثم العمل كحاجز ضد شن الهجمات السيبرانية[21].

ان القاعدة العامة لمبدأ التمييز كاحد مبادئ القانون الدولي الانساني يفرض على الدول بأن تميز في الاحوال كافة بين المقاتلين والمدنيين وبين الاعيان المدنية والاهداف العسكرية حيث لا يجوز توجيه الهجمات الا باتجاه المقاتلين او الأهداف العسكرية ويمكن القول انه عند تخطيط وتنفيذ العمليات الالكترونية فان الاهداف المسموح بها في مجال القانون الدول الانساني هي الاهداف العسكرية فقط كأجهزة الكمبيوتر او النظام الحاسوبية التي تحقق مساهمة فعالة في العمليات العسكرية المرئية ولا يجوز توجيه الهجمات السيبرانية عبر الفضاء الالكتروني نحو النظم الحاسوبية التي تستخدم في منشات مدنية بحتة .مما سبق تطرقنا لاهم قواعد القانون الدولي الانساني الواجب مراعاتها وتطبيقها اثناء الهجمات السبرانية وعلى اطراف النزاع الالتزام بتلك القواعد سواء كانت عرفية او اتفاقية

**الفرع الثاني/ الآليات الوطنية والدولية لمواجهة الحرب السيبرانية**

ان معظم الدول على المستوى الوطني تعترف بضرورة اعادة توزيع الموارد والقيام بإصلاح استراتيجيات الامن الوطنية في المستويات كافة والعديد من دول العالم تسعى الى زيادة التمويل وبحث الموارد التكتيكية والدبلوماسية لدعم امنها السيبراني بشكل يمكنها من اعداد اسلحة سيبرانية هجومية وقدرات دفاعية الكترونية والتي تعد الاسلحة السيبرانية بمثابة مضاعفات القوة التي يجب استعمالها بالتوافق مع الاعمال العسكرية التقليدية لغرض تعزيز قدراتها الحربية بشكل كبير وهذا النوع من التحويل ممكن يشمل تدريب القوات المسلحة وتحديث الخدمات الاستخباراتية والامنية للتركيز على التحري وجمع المعلومات العلمية والتكنولوجية ذات العلاقة بالحرب السيبرانية فضلاً عن اجراء برامج وعمليات محاكاة للحرب السيبرانية والمناورات العسكرية وبالتالي ايلاء اهتمام خاص للتطبيقات التكنولوجية الحديثة للمعلومات والاتصالات الالكترونية والاليات الوطنية لمواجهة الحرب السبرانية تتضمن استهداف وانشاء فرق حربية للانترنت تكون مكرسة لتحقيق الامن السيبراني الوطني وبالإمكان دمجها في وكالات الاستخبارات الوطنية[22].ولعل من ابرز الاليات الوطنية لمواجهة الحرب السيبرانية ان يصار الى تشريع قوانين وطنية للأمن السيبراني اما بالنسبة للآليات الدولية فإن المعايير القانونية الدولية الحالية غير معدة اعداداً قابلاً لمواجهة التحديات الجديدة التي يطرحها الأمن السيبراني والحوار العالمي والجهود الدولية من الامور الضرورية بهذا الاطار والطبيعة المتغيرة للأنظمة التكنولوجية الالكترونية الحديثة تجعل استراتيجيات جديدة تم اعتمادها والتعاون الدولي على قدر الاهمية لضمان السلام السيبراني[23].

ويمكن القول ان تعمل الدول على تنسيق اطرها القانونية لمكافحة الجرائم السيبرانية وتسهيل التعاون الدولي وينبغي على دول العالم ان تعمل في سبيل ايجاد نظام لتحديث القوانين على اساس منتظم لمعالجة الطبيعة المتغيرة للتهديدات السيبرانية التي يتعرض لها الامن السيبراني وقد سعت بعض الدول الى اصدار معايير دولية وقواعد سيبرانية كآليات لتحسين الامن السيبراني على المستوى الدولي ويستوجب لدى اصدار قواعد توجيهية لتحقيق الامن السيبراني بين الدول الأخذ بنظر الاعتبار الخصائص المميزة للفضاء السيبراني والتحديات المطروحة ووضع استراتيجيات لتطوير واستحداث تشريعات دولية تتعلق بالتهديدات السيبرانية خاضعة للتطبيق والتنفيذ على المستوى الدولي العالمي فضلاً عن الاسهام في تطوير الآليات القانونية الدولية للأمن السيبراني من خلال تنسيق الاطر القانونية وخاصة الموارد المختلفة المتعلقة بالتشريعات الدولية لمواجهة الجرائم السيبرانية[24]. وبناءً على ماتقدم وفي ظل الآليات الدولية لمواجهة الحرب السيبراني يتطلب ابرام اتفاقيات دولية على المستوى الاقليمي والعالمي للحد من التهديدات السيبرانية انطلاقاً من مبادئ ميثاق الامم المتحدة ولا سيما حظر استخدام القوة والتهديد باستخدامها في تسويه النزاعات الدولية فضلاً عن مهام مجلس الامن في الحفاظ على الامن والسلم الدوليين .

**الخاتمة**

**بعد ان بحثنا في الحرب السيبرانية واثرها في القانون الدولي الانساني توصلت الى جملة من النتائج والمقترحات سنوجز البعض منها وكالاتي:-**

**اولاً :- النتائج**

1- ان الحرب السيبرانية تعد حرباً حقيقية بمفهوم النزاعات في القانون الدولي الانساني لاعتمادها على الهجمات السيبرانية كما انها تلحق اضرار تفوق في حساباتها الحروب التقليدية مما يجعل الحاجة العاجلة في الوقت الحاضر في تحديد مجالات الحماية للاعيان والاشخاص المحميين من اثار هذه الحروب السيبرانية فضلاًعن نوع الحماية المقترحة لهذه الفئات المحمية

2- ان القانون الدولي الانساني بعد تطويره يمكن ان ينطبق على الحرب السيبرانية بعد ضبط مدلولها ومجالاتها بدقة ولا سيما في الفضاء السيبراني.

3- ان استخدام القوة أو التهديد باستخدامهم في تسوية المنازعات الدولية يعد عملاً غير مشروعاً وكما نصت عليه المادة ( ٢/ ٤ ) في ميثاق الامم المتحدة وهذا المبدا مطلق يسري على جميع الهجمات وحتى السيبرانية لما يترتب عليه من انتهاك وتأثير واضح على الامن القومي والدولي.
4- لوحظ عدم تحديد معايير واضحة وثابتة لاستخدام تكنولوجيا المعلومات الحديثة والتي تشكل هجمات سيبرانية اثناء النزاعات المسلحة وهذا سوف ينتج عنه تحدياً واضحاً امام تطبيق مبدأ الضرورة العسكرية حيث من المرجح استهداف منشات تقدم خدمات للجهد العسكري وتستهدف خدمة المدنيين في الوقت ذاته.
5- من الملاحظ ان هنالك صعوبات في تطبيق مبادئ وقواعد القانون الدول الانساني في خصوص الهجمات السيبرانية لكن في جميع الاحوال ينبغي لا تكون المقارنة طبقاً لحالة افتراضية فيما يتعلق بالحروب التقليدية ومن ثم امكانية تطوير تلك الاليات لتنسجم مع التطبيق الافضل لقواعد القانون الدولي الانساني.
6- من الملاحظ ان تطبيق مبدأ التمييز بين المقاتلين وغير المقاتلين على الهجمات السيبرانية للاغراض العسكرية مسألة معقدة وخاصة عندما تكون الهجمات السيبرانية بعيدة عن الاماكن المستهدفة.
7- لوحظ عدم وجود تشريعات وطنية صريحة تتعلق بالامن السيبراني الوطني وفي ظل التشريعات العراقية لا يوجد قانون خاص بالامن السيبراني ومكافحة جرائم المعلوماتية.
8- لوحظ استغلال المجاميع الارهابية التي ظهرت في عدد من دول العالم للفضاء السيبراني والتكنولوجيا الحديثة من اجل تحقيق اهدافها في الدعاية والاعلان عن افكارها الارهابية المتطرفة والابتزاز والقرصنة الالكترونية وبما يهدد السلم والامن الوطني والعالمي .
9- لوحظ ان الصلة بين الآليات القانونية والتكنولوجيا الحديثة المتطورة تعد علاقة متبادلة في التطورات الالكترونية تفترض الارتقاء بمستوى التشريعات القانونية لمواجهتها سواء على الصعيد الوطني أو العالمي.
10- لوحظ ان الآليات المتعلقة بالأمن السيبراني الدولي تتسم بصعوبات وتحديات جمة من جانب الدول الكبرى التي عادة ما تستخدم حق الفيتو في مجلس الأمن ضد القرارات التي تتعارض مع مصالحها وهذا ما يحدث من دعم الولايات المتحدة الامريكية للكيان الصهيوني في حربه ضد ابناء شعبنا الفلسطيني في غزة وضد شعبنا اللبناني واستخدامه لاحدث الاسلحة التكنولوجية الحديثة.

**ثانياً :- المقترحات**

1- ان الحل الواضح في تطبيق قواعد القانون الدولي الانساني على الحرب السيبراني يتمثل في تطوير اتفاقيات القانون الدولي الانساني القائمة وجعلها اكثر ملائمة وقابلية لتشمل كل انواع الهجمات والمخاطر والاضرار الناتجة عن تلك الهجمات السيبرانية ولا سيما بعد ابرام معاهدات جديدة خاصة بالحرب السيبرانية.
2- من الضروري تحديد المقصود بالسلامة الاقليمية المنصوص عليها في ميثاق الامم المتحدة لتتضمن البنية التحتية الحيوية والسرية السيبرانية والتي بحاجة الى دقة في تحديدها ولا سيما وان الحرب السيبرانية قد تكون اثارها اعم واشمل.
3- يتطلب احداث تعديلات جوهريةعلى اتفاقيات لاهاي(١٨٩٩– ١٩٠٧)المتعلقة بتنظيم وسائل القتال لغرض تحريم استخدام القوات غيرالنظاميةفي القتال السيبراني وحظرنقل الهجمات السيبرانيةعبر شبكات الدول المحايدةوتحت اي ظرف.
4- من الضروري تعديل اتفاقيات جنيف لغرض تحريم الهجمات على البنية التحتية الحيوية التي يمكن ان تعطل الاتصالات الاساسية وتعرض المدنيين للخطر ولا سيما ان تدمير الشبكات الالكترونية وانظمة الاتصالات قد يحسن الانظمة الصحية وانظمة معالجة المياه ومنظومة الطاقة الكهربائية والبنية التحتية كافة الضرورية لبقاء المدنيين احياء.
5- ينبغي تكثيف الجهود الدولية للتعاون ضمن اطار دولي عالمي لضمان الامن في الفضاء السيبراني وتطوير ميثاق الامم المتحدة وقوات حفظ السلام ليستوعب مثل هذه الهجمات والحد منها مستقبلاً.
6- ندعو الى ابرام اتفاقيات دولية للعمل على تقييد استخدام تكنولوجيا المعلومات بصورة هجمات سيبرانية وفي اطار التوازن بين المصالح الوطنية والدفاع عن النفس وبين الاثار غير الانسانية المترتبة عن تلك الهجمات السيبرانية .
7- ندعو الى ابرام اتفاقيات دولية تعمل على تقييد استخدام تكنولوجيا المعلومات بصورة هجمات سيبرانية وفي اطار التوازن بين المصالح الوطنية والدفاع عن النفس وبين الاثار غير الانسانية المترتبة عن تلك الهجمات السيبرانية .
8- ندعو الى تشريع قوانين وطنية للأمن السيبراني ومكافحة الجرائم السيبرانية وخاصة بالنسبة للدول ومنها العراق التي تفتقد الى وجود تشريعات في مجال الامن السيبراني ومكافحة جرائم المعلوماتية الالكترونية.
9- من الضروري الدعوة لتبني ثقافة وطنية وفي كافة الوسائل الاعلامية لتنمية الوعي بالامن السيبراني وفي المجالات كافة وخاصة الاشخاص الذين يستخدمون الشبكات الالكترونية عليهم ان يتخذوا التدابير الامنية اللازمة لحماية تلك الشبكات ووفق الاطر القانونية فضلا عن ايجاد اليات رصينة لحماية سرية المعلومات الوطنية والشخصية
10- من الضروري حجب المواقع الالكترونية المشبوهة التي تدعو الى نشر الافكار المتطرفة والى الكراهية والقرصنة والابتزاز الالكتروني والتي تسهم في الترويج للتهديدات والاعتداءات السيبرانية.
11- ندعو الى تفعيل الآليات الوقائية والاحترازية لتجنب وقوع الهجمات والحرب السيبرانية وايجاد منظومة استراتيجية امنة لمواجهة تلك التهديدات وفي المجالات كافة .

**الهوامش.**

(1) امير فرج يوسف ، مكافحة الارهاب الالكتروني ، الارهاب الرقمي في ظل اتفاقية دول مجلس التعاون الخليجي ، دار الكتب والدراسات العربية ، ٢٠١٦ ، ص ٢٥٣.
(2) د.أحمد عبيس الفتلاوي ، الهجمات السيبرانيه مفهومها والسيبرانية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر ، مجلة المحقق الحلي للعلوم القانونية والسياسية ، جامعة بابل - كلية القانون ، العدد الرابع ، السنة الثامنة ، ٢٠١٦ ، ص ٦١٤.
(3) د.أحمد عبيس لفتة الفتلاوي ، الهجمات السبرانيه مفهومها والسبرانية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر ، مجلة المحقق الحلي للعلوم القانونية والسياسية ، جامعة بابل - كلية القانون ، العدد الرابع ، السنة الثامنة ، ٢٠١٦ ، ص ٦١٤.
(4) عمر بن عبد الله بن سعد البلوشي،مشروعية اسلحة الدمار الشامل وفقاً لقواعد القانون الدولي، منشورات الحلبي الحقوقية بيروت٢٠٠٧ص ١٧.
(5) عمر مكي ، القانون الدولي الانساني والارهاب ، اللجنة الدولية للصليب الاحمر ، ص ٩٣.
(6) محمد سعادي ، اثر التكنولوجيا المستخدمة على القانون الدولي العام ، ط١ ، دار الجامعة الجديدة ، الاسكندرية ٢٠١٤ ، ص ١٣.
(7) خالد وليد محمود ، الهجمات السيبرانية عبر الانترنت ساحة الصراع الالكتروني الجديد ، ط١ ، المركز العربي للابحاث ودراسة السياسات ، دون مكان نشر ، ٢٠١٣ ، ص ٢٠.
(8) عباس بدران ، الحرب الالكترونية والاشتباك في عالم المعلومات ، مركز دراسات الحكومة الالكترونية ، بيروت٢٠١٠ص ٢٢.
(9) ينظر المادة ( ٢/ ٤) من ميثاق الامم المتحدة لعام ١٩٤٥.
(10) ينظر المادة ( 51 ) من ميثاق الامم المتحدة لعام ١٩٤٥.
(11)ينظر المادة ( 42 ) من ميثاق الامم المتحدة لعام ١٩٤٥.
(12) ينظر المادة ( ٢/ ٤) من ميثاق الامم المتحدة لعام ١٩٤٥.
(13) جوزيف ناي المنازعات الدولية مقدمة للنظرية والتاريخ ترجمة احمد امين الجمل ووجدي كامل، الجمعية المصرية لنشر المعرفة والثقافة العالمية ، القاهرة ، ١٩٧٧ ، ص ٨٢.
(14)ينظر المادة ( ٢/ ٤) من ميثاق الامم المتحدة لعام ١٩٤٥.
(15) سراب احمدثامر،الهجمات على شبكات الحاسوب القانون الدولي الانساني،اطروحة دكتوراه كليةالحقوق جامعه النهرين،بغداد٢٠١٥ص١٠٧.
(16) امير فرج يوسف ، مصدر سابق ، ص ٢٥٣.
(17) ينظر اتفاقيات جنيف الاربعة لعام ١٩٤٩ ، والبروتوكول والاضافي الاول لعام ١٩٧٧
(18) نوران شفيق ، اثر التهديدات الالكترونية على العلاقات الدولية ، دراسة في ابعاد الامن الالكتروني ط١المكتب العربي للمعارف٢٠١٦ص ٩.
(19) كوردولا دروغيه ، المستشارة القانونية في اللجنة الدولية للصليب الاحمر ، مامن فراغ قانوني في الفضاء مقال منشور على موقع اللجنة الدولية للصليب الاحمر.
(20)عادل عبد الصادق ،الارهاب الالكتروني ، القوة في العلاقات الدولية ، نمط جديد وتحديات مختلفة ، مركز الدراسات السياسية و الاستراتيجية ، ط١ ، ٢٠٠٩ ، ص ١٥٦.
(21) امير فرج يوسف ، مصدر سابق ، ص ٢٥٤.
(22) عادل عبد الصادق ، مصدر سابق ، ص ١٦٥.
(23) يحيى مفرح الزهراني ، الابعاد الاستراتيجية والقانونية للحرب السيبرانية ، مجلة البحوث والدراسات ، جامعة الوادي / الجزائر ، المجلد / ١٤ / العدد / ١ / ص ٢٣٧.
(24) عادل عبد الصادق ، مصدر سابق ، ١٥٦.

**المصادر**

**اولاً :- الكتب العلمية**

1- اميرفرج يوسف،مكافحة الارهاب الالكتروني والارهاب الرقمي في ظل اتفاقيةدول مجلس التعاون الخليجي،دارالكتب والدراسات العربية٢٠١٦.
2- عمرو رضا بيومي ، مخاطر اسلحة الدمار الشامل الاسرائيلية ، ط٢ ،دار النهضة العربية ، ٢٠٠٢.
3- عمر بن عبد الله بن سعيد البلوشي ،مشروعية اسلحة الدمار الشامل وفقاً لقواعد القانون الدولي ، منشورات الحلبي الحقوقية ، بيروت ، ٢٠٠٧.
4- عمر مكي ، القانون الدولي الانساني ، والارهاب اللجنة الدولية للصليب الاحمر .
5- محمد سعادي ، اثر التكنولوجيا المستحدثة على القانون الدولي العام ، ط٢ ، دار الجامعة الجديدة ، الاسكندرية ، ٢٠١٤.
6- خالد وليد محمود،الهجمات السيبرانية عبر الانترنت ،رسالة الصراع الالكتروني الجديد ، ط١المركز العربي للابحاث ودراسة السياسات٢٠١٣.
7- عباس بدران ، الحرب الالكترونية ، والاشتباك في عالم المعلومات ، مركز دراسات الحكومة الالكترونية ، بيروت ،٢٠١٠.
8- جوزيف ناي ، المنازعات الدولية مقدمة للنظرية والتاريخ ترجمة امين الجمل ومجدي كامل، الجمعية المصرية لنشر المعرفة والثقافة العالمية ، القاهرة ، ١٩٩٧.
9- نوران شفيق ، اثار التهديدات الالكترونية على العلاقات الدولية ، دراسة في ابعاد الامن الالكتروني ، ط١ ، المكتب العربي للمعارف ٢٠١٦.
10- عادل عبد الصادق ؛ الارهاب الالكتروني في العلاقات الدولية ، مركز الدراسات السياسية والاستراتيجية ، ط١ ، ٢٠٠٩.

**ثانياً :- للرسائل والاطاريح والبحوث**

1- سراب احمد ثامر،الهجمات على شبكات الحاسوب القانون الدولي الانساني،اطروحة دكتوراه ، كلية الحقوق ، جامعة النهرين ، بغداد ، ٢٠١٥.
2- كوردولا دروغيه المستشارة القانونية في اللجنة الدولية للصليب الاحمر ، امن فراغ قانوني في الفضاء مقال منشور على موقع اللجنة الدولية للصليب الاحمر.
3- يحيى مفرح الزهراني،الابعاد الاستراتيجية والقانونية للحرب السيبرانية،مجلة البحوث والدراسات ، جامعة الوادي الجزائر المجلد/١٤العدد/١ /
4- احمد عبيس نعمة الفتلاوي ، الهجمات السيبرانية مفهومها والسبرانية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر ، مجلة المحقق الحلي للعلوم القانونية والسياسية ، جامعة بابل ، كلية القانون ، العدد / ٤ ، السنة / ٣ ، ٢٠١٦.

**ثالثاً :- الاتفاقيات الدولية**

1- ميثاق الامم المتحده لعام ١٩٤٥.
2- اتفاقيات جنيف لعام ١٩٤٩.
3- البروتوكول الاضافي الاول لعام ١٩٧٧.