مراجعة مقال:

مفهوم الحروب السيبرانية والأمن السيبراني

الكاتب د شويرب جيلالي د مراد فايزة

The concept of cyber warfare and cyber security

بحث منشور في مجلة الحقوق والحريات المجلد11 / العدد 1 / 2023

https://asjp.cerist.dz/en/article/219023

م د ياور عمر محمد*

جامعة كركوك – كلية القانون والعلوم السياسية

Article Review:

The Concept of Cyber Warfare and Cyber security

Authors: Dr. Chouireb Djillali & Dr. Mourad Faiza

Research paper published in the *Journal of Rights and Freedoms*,

.Volume 11, Issue 1, 2023

https://asjp.cerist.dz/en/article/219023

Dr. Yawar Omar Mohammad

University of Kirkuk – College of Law and Political Science

المقدمة:

أصبح الفضاء السيبراني ساحة للصراعات الدولية، وأصبح الأمن السيبراني أحد أهم القضايا المعاصرة لدول العالم، وأصبح بمقدور الدول والمنظمات الدولية، وحتى الافراد من التأثير على مقدرات الدول لا سيما البنية التحتية أو قاعدة البيانات والمعلومات التي تمتلكها والتي تتعرض لهجمات سيبرانية، تستهدف المعلومات البيانات مستخدماً الأسلحة الحديثة من فيروسات، وبرامج خبيثة وضارة متنوعة من أجل تخريب وتدمير وسرقة البيانات والمعلومات على أنظمة الحاسوب والأجهزة الأخرى، في الوقت نفسه أصبح الفضاء السيبراني مجالاً خاصاً

* . جامعة كركوك – كلية القانون والعلوم السياسية – قسم العلوم السياسية.

للتواصل والاتصال وربط الحياة السياسية والاقتصادية والاجتماعية، وعن طريق الفضاء السيبراني، وشبكات الانترنت أصبح قطاعات الدول تختزل في مجموعة من المعلومات والبيانات المسجلة على أنظمة الحاسوب والأجهزة الخاصة بالبيانات، لذا انتقل العلاقات الدولية الخاصة بالصراعات والنزاعات الى الفضاء السيبراني، واصبح أداة لشن الهجمات والدفاع السيبراني، وتبنت الدول إجراءات حماية البيانات والمعلومات من الهجمات السيبرانية، وأصبحت المعرقة والتكنولوجيا الحديثة هي القوة الحقيقية للدول.

ملخص الدراسة: بناء على ذلك فقد قدم الباحثان إشكالية الدراسة على النحو التالي: بالسؤل الرئيس حول كيف شّكل الفضاء السيبراني في العلاقات الدولية الحديثة في السلم والحرب ومنها تفرعت الأسئلة التالية: ما مفهوم الهجمات والدفاع السيبراني، هل تلاءمت خصوصيات النزاع السيبراني مع القواعد الإنسانية للنزاعات الدولية، ومنا قسم الباحثين دراستهم الى مبحثين تناول المبحث الأول: الحرب السيبرانية والامن السيبراني، ومن ثم قسم البحث الى مطلبين تناول في المطلب الأول مفهوم الحروب السيبرانية، والمطلب الثاني: تناول ماهية الامن السيبراني وابعاده، بينما المطلب الثاني تناول مفهوم الحرب السيبرانية من منظور القانون الدولي الإنساني.

المحور الأول: تحدث الباحثان في المبحث الأول حول مفهوم الحرب السيبرانية

اولاً. ذكرى الباحثان بأن العصر الحالي هو عصر المعرفة والمعلومات وعلى أثر ذلك تطور التكنولوجيا والتقدم التقني، لا سيما في مجال تقنية الاتصالات والمواصلات، ومن ثم ظهور الفضاء السيبراني، وشبكات الانترنت، فقد أنتج ذلك مسميات جديدة للحروب منها (الحروب الالكترونية، الاحتيال الالكتروني، حرب المعلومات، والامن المعلوماتي، والحرب السيبرانية،

والامن السيبراني) مسميات عديدة، واستوجبت على الدول في وضع سياسات أمنية جديدة تتماشى مع الوضع الدولي الجديد.

قدم الباحثان تعريفات عديدة للحرب السيبرانية، فقد عرف الحرب السيبرانية، لا سيما الهجمات السيبرانية، إذ ذكرى بأن "ميشال شميث"، عرف الهجمات السيبرانية بأنها: "تلك الإجراءات التي تتخذها الدولة من أجل الهجوم على نظم المعلومات العدو بهدف التأثير والاضرار بها والدفاع عن نظم المعلومات الخاصة بالدولة المهاجمة)، واعتر الحرب السيبرانية بانها حرب غير محددة المجال وغامضة الأهداف كونها تحدث عبر شبكات الانترنت العابر للحدود الدولية، وهي تحدث بسرعة تتطابق ودوافع سرعة المعلومات في هذا العصر، وهذا يسبب تدمير أوسع النطاق ضد المنشأة الحيوية والبنية التحتية للدول، هذا الهجوم السيبراني قد يؤدي الى تعطيل شبكات المعلومات للدول ، ويحرم المدنيين من الحاجات الأساسية، عندما تكون هجماته ضد مصادر المياه والرعاية الصحية ومحطات الكهرباء والمصارف الحكومية، بينما يرتبط الأنظمة الالكترونية ومواقع الأسلحة والمعدات ذات الارتباط بشبكات الكترونية لتؤدي الى الاضرار بالأجهزة المستخدمة للأنترنت مثل سرقة البيانات الخاصة، لذا عرف الحرب السيبرانية بأنه: "الإجراءات التي تتخذها أي دولة أو منظمة أو مجموعة لأختراق أجهزة الحاسوب أو الشبكات الخاصة بدول أخرى لغرض السيطرة عليها أو التحكم بها أو اتلافها أو تعطيلها عن العمل عن طريق إرسال رسائل مكتوبة باللغة الرقمية الثنائية المكونة من رقمي(1-0)، إلا إن ذلك لا يعني بان الحرب السيبرانية تلغي الحروب التقليدية (البرية، والبحرية، والجوية).

ثانياً. أشار الباحثان الى خصائص الحروب السيبرانية وهي تتميز عن الحرب التقليدية بانها

1. الحرب السيبرانية هي حرب تقنية متطورة أداته الرئيسة شبكات الانترنت الذي يمتاز بتطور مستمر وتنوع الابتكار في وسائلها وتقنياتها كما أنها ترتبط بالمصالح الحيوية للدول.

2. تتميز بالسرعة وإمكانية المراوغة والتي تعطي للمهاجم أفضلية واضحة على المدافع

3. حرب غير محددة الأهداف والتأثير قد تتعدى تهديداتها ومخاطرها ميادين القتال التقليدية لتشمل أكثر المواقع السيادية والحساسة والأكثر تحصيناً وبعيداً عن دائرة القتال.

4. تتميز الحرب السيبرانية بأنها تخلف دماراً قد يتضمن التجسس والتسلل والنسف البيانات والمعلومات وأنظمة الحواسيب بدون أراقة أي دماء.

5. أطرافها المهاجمة غير واضحة وتداعياتها خطيرة عن طريق تدمير مواقع على الانترنت عبر قصفها بوابل من الفيروسات، فضلاً عن المجال الواسع لهذا الفضاء مما قد يسمح بزيادة عدد المهاجمين وامتداد الصراع

ثالثاُ. أشار الباحثان الى ان الفاعلين في الفضاء السيبراني لا يقتصر على الدول فقط، إذ يمكن أن تكون الدول، الحكومات، الشركات المتعددة الجنسيات، الجماعات الإرهابية، الافراد، وجماعات أخرى منتشرة حول العالم من القراصة، لذا فإن خصوصية هذه الحروب تتصل بخصوصية الفضاء السيبراني، من سرعة وسهولة الاستخدام واللامحدودية في الانتشار، فضلاً عن سرية القيام بها، وصعوبة تتبعها أو الحصول على الأدلة لأثبات فاعليها، ومن هذا المنطلق ظهرت التحديات الدولية الجديدة والمتعلقة بأمن الدول وسميت "الامن السيبراني" إن والمتعلقة بحماية قواعد البيانات الحساسة لكل دولة لا سيما البيانات المتعلقة بمؤسسات الدول أو مواطنيها ما يشكل تهديد لأمنها القومي، لذا اتجهت الدول الى القيام بسن قوانيين وتوفير الوسائل والتقنيات اللازمة للحج من هذه الهجمات، فضلاً عن التعاون في ما بينها من أجل

الحد من أنواع الاختراقات التي تمس أمنها القومي أو تهديد اقتصادها أو المساس بحقوق الانسان بداخلها، فالأمن السيبراني شمل حماية بينات الأشخاص الالكترونية، حماية الشركات والمؤسسات الدول لبياناتها وعملائها ثم حماية الامن القومي للدولة.

عرف الباحثان في دراستهم الأمن السيبراني بانه (مجموعة من الوسائل التقنية والتكنولوجية والعمليات التي يتم استخدامها لحماية الشبكات والأجهزة والبرامج والبيانات من الهجمات أو التسلل غير المسموح به)، كما ويعرف بأنه (النشاط الذي يؤمن حماية الموارد البشرية والمالية المرتبطة بتقنيات الاتصال كما يحد من الاضرار في حال حصول هجمات أو تهديدات سيبرانية ويعيد الوضع الى ما كان عليه بأسرع وقت).

رابعاً. تطرق الباحثان الى أبعاد الامن السيبراني والذي يشتمل على:

1. ابعد العسكري: ويعني توفير الأمن السيبراني للقوات العسكرية للتواصل وتبادل المعلومات والاوامر عن بعد بشكل آمن مع القدرة على صد أي محاولة لاختراق يؤدي الى تدمير البيانات العسكرية لدولة العدو، بحيث يمس الأمن القومي وهذا ما حدث مع أيران عندما تم اختراق منشأتها النووية.

2. البعد الاقتصادي: أصبح الفضاء السيبراني اساساً في التأمل التجارية والمالية والاقتصادية وأصبح الحاسوب أداة لتسيير الصناعة والاقتصاد

3. البعد الاجتماعي: أصبح مواقع التواصل الاجتماعي أداة اتصال عالمية بين الدول والمجتمعات والافراد، وهي تمد بالمعلومات والأفكار، إلا أنها أصبحت أداة لنشر الأفكار الغربية والخطيرة التي تمس الهوية الوطنية للأشخاص ويهدد السلم المجتمعي، لذا لا بد العمل على توعية الافراد بالمخاطر والتهديدات التي تقع عليه عند استخدام هذه المواقع.

4. البعد السياسي: تشكل الامن السيبراني وسيلة لحماية المعلومات والوثائق الأساسية والحساسة في عمل بعض مؤسسات الدولة، وعليه لا بد من تحقيقه حتى لا تخلق خلافات دبلوماسية بين الدول.

5. البعد القانوني: يمثل القانون أداة ضبط المجتمعات وهو يحمل نفس الوظيفة بالنسبة للفضاء السيبراني، فلا بد للدول أن تكرس جهودها لوضع التشريعات والاطر القانونية لتحدد الاعمال القانونية وغير القانونية في الفضاء السيبراني.

المحور الثاني: تناول الباحثان مفهوم الحرب السيبرانية من منظور القانون الدولي الإنساني.

ذكر الباحثان بان فقهاء القانون الدولي استخدام أو تطبيق القواعد القانونية القابلة للتطبيق على النزاع التقليدي ومدى توافق هذه القواعد مع خصوصيات الحروب السيبرانية، لا سيما ما يخص المدنيين أو الافراد العاديين ضمن هذا الفضاء وضحى ذلك عبر مطالب المبحث

اولاً. ارتباط الحروب السيبرانية بالقانون الدولي الإنساني: تميزت الحروب التقليدية بالشراسة والعنف والأسلوب المدمر والذي لم يراعي فيه اعتبارات إنسانية اثناء الصراعات والحروب، فنجد مبادئ القانون الدولي الإنساني وما جاء به من قواعد لأسننة الحرب، لهذ أصبحت مبادئ دولية آمرة التطبيق في حال اندلاع الحروب والنزاعات سواء كان دولياً أو غير دولي، وأصبح إمكانية إخضاع الحروب الحديثة بما تحمله من خصوصية لقواعد هذا الأخير،

وقد ذكر الباحثان بأن فقهاء القانون الدولي الإنساني عرف الحروب السيبرانية بانها: (اعمال تقوم بها دولة وتحاول من خلالها أختراق أجهزة الكمبيوتر والشبكات التابعة لدولة أخرى بهدف تحقيق أضرار بالغة أو تعطيلها[1].

هنا طرح سؤال حول كيف يتم تطبيق القانون الدولي الإنساني على الحروب السيبرانية باعتبارها وجها معاصراً للنزاعات بين الدول؟ وما تأثيرها على السلم والامن الدوليين، نظراً لطبيعة هذه الحروب واختلافها الكبير عن الحروب التقليدية، ووفق التعريفات السابقة فإن هذه الحروب رغم استعمال الوسائل والاليات الالكترونية المتطورة، إلا أنها تستهدف الافراد عن طريق تأثير الدمار الذي يخلفه على حياتهم أو على باقي حقوقهم كحق العيش الكريم أو حقهم في العمل أو حقهم في التملك والتنقل، فضلاُ على انها تمس بمصالح المدنيين الذين ليس لهم دخل في الصراع السيبراني بين دولتين أو عدة دول مما يستدعي حمايتهم وفق قواعد القانون الدولي الإنساني.

وقد وضح الباحثان قواعد القانون الدولي الإنساني. وما نص عليه المادة 36 من بروتوكول الأول لاتفاقية جنيف عام 1949، نجده بانها تنص على إلزام كل الدول تقتني أو تطور سلاح جديد بالتأكيد إذا ما كان محظوراً بموجب القانون الدولي الإنساني، وهذا ما أكدته المادة 82 استكمالاً ما قضت به المادة 36 بنصها على وجوب استشارة مستشارين قانونيين لتقديم المشورة للقادة العسكرية بالنسبة لهذا الموضوع.

وهذا ما أثير جدلية حول مدى تطبيق قواعد القانون الدولي الإنساني على الحروب السيبرانية بما تحمله من خصوصية والتي أساسها عدم مرئية هذه الحروب من جهة وعدم تنظيمها القانون المحكم دولياً ووطنياً مما يصعب من التحكم فيها ومدى أضرارها، فقد انقسم الفقه القانوني الى مؤيد ومعارض ولكل منهم حجته في إمكانية تطبيق القواعد الإنسانية على أي نزاع سيبراني يحدث داخل الفضاء السيبراني وهذه الاتجاهات كانت على النحو التاي:

[1] . ريتشار كلارك وروبرت كيه كنيك، حرب الفضاء الالكتروني الخطر القادم على الامن القومي وسبل معالجته، ط1(أبو ظبي: مركز الامارات للدراسات والبحوث الاستراتيجية، 2012)، ص

الرأي الأول: القائل بعد إمكانية تطبيق القانون الدولي الإنساني على الحروب السيبرانية.

تزعم هذا الاتجاه بعض السياسيين والعلماء الأمريكيين الذين رفضوا اعتبار قواعد القانون الدولي الإنساني قواعد تستوعب هذه الهجمات والتي تشكل وجهاً حديثاً للنزاعات الدولية ومجتمعين في ذلك إن الفضاء السيبراني فضاء حر لا تمتلك أي سلطة لأي دولة التحكم فيه، كما يتعذر اخضاع هذه الحروب لقانون واحد مشترك نظراً لاشتراك جميع الدول في هذا الفضاء، فضلاً أن القانون الدولي الإنساني لا تحمل مبادئها أي تعامل أو تنظيم مباشر لهذا النوع من الحروب، لأنها لاتعد من ضمن النزاعات المسلحة والتي تخلف آثاراً مادية، فضلاً أن استخدام الحرب غير دقيق لأن الحرب ترتكز على استخدام الجيوش النظامية كما يسبقها إعلان واضح لحالة الحرب وميدان القتال، بينما تعد الهجمات السيبرانية غير محددة المجال أو الأهداف كونها تتعدى الحدود الدولية ، هذا يجعل أن تكون أقرب الى الإرهاب الدولي عن الحرب، لا سيما من ناحية استعمال الأسلحة المعلوماتية الي يتم نشرها في سرية تامة وبدون سابق انذار.

الرأي الثاني: القائل بإمكانية تطبيق القانون الدولي الإنساني على الحروب السيبرانية.

إن مؤيدي هذا الرأي يرى أنه باعتباره تنظيم القانون الدولي الانساني لوسائل اتصال مثل الهاتف والفاكس وشبكات الانترنت ومواقع التواصل الاجتماعي، وغيرها من في حالة النزاع المسلح، إذن فهي قادرة على تنظيم الهجمات السيبرانية ، كما يمكن تطبيق المبادئ القانونية الراسخة في القانون الدولي الإنساني على الحالات التي لا تغطيها اتفاقيات دولية خاصة، مثل حالة الهجمات السيبرانية وعلى هذا الأساس فكل تصرف او اعتداء يقع اثناء النزاع المسلح تغطيه قواعد القانون الدولي الإنساني، وبالعودة الى المادة 36 من البروتوكول الإضافي لاتفاقية

جنيف1949، نجدها تنص على(يلزم أي طرف سام متعاقد عند دراسة أو تطوير أو اقتناء سلاح جديد، أو أداة حرب أو اتباع أسلوب حرب، بأن يتحقق ما إذا كان ذلك الفعل محظوراً في جميع الأحوال أو في بعضها بمقتضى الملحق أو أية قاعدة أخرى من قواعد القانون الدولي التي يلتزم بها الطرف السامي المتعاقد)[1].

فعلى الدول التحقق من ذلك باعتبار الهجمات السيبرانية يعد سلاح حديث من أسلحة النزاعات الدولية والتأكيد من مشروعية استخدامها وفقاً لقواعد البروتوكول وهو ما أكد انطباق هذه الاحكام الآمرة على الهجمات السيبرانية وقد سارت محكمة العدل الدولية على مثل هذه القواعد في مسألة مدى مشروعية التهديدات بالأسلحة النوية، وعليه فإن مبادئ قواعد القانون الدولي الإنساني تنطبق على الهجمات السيبرانية على دولة أينما تمت ذلك.

الخاتمة: في الختام نجد إن الباحثان أرادا من هذا البحث التأكيد على ان التطور التكنولوجي وظهور شبكات الانترنت، أصبحت المخاطر والتهديدات الدولية قد انتقلت الى الفضاء السيبراني وأصبحت العلاقات الدولية تخضع لتأثيرات هذا الفضاء، واكتسبت الحروب والصراعات طابعاً أخر غير الحروب التقليدية، إذ قامت الدول والفواعل غير الدولية في استخدام الهجمات السيبرانية لتحقيق الأهداف والغاية عبر الهجوم على البنية التحتية وأنظمة الحواسيب وشبكات المياه ومصادر الطاقة ومحطات الوقود والتي تحدث تخريباً ودماراً كبيراً باستخدام الأسلحة المتقدمة من الفيروسات والبرامج الخبيثة، وبين ان الحروب السيبرانية هي امتداد للحروب التقليدية ، إلا إنها تختلف عنها فهي تحدث بصورة سريعة وبكلفة قليلة، محدثاً آثاراً وتخريب مدمر عبر سرقة المعلومات والبيانات أو الاضرار بالأجهزة وأنظمة الحواسيب للدول ولا يقتصر هذه الحروب على الدول بل امتدت لتشمل الشركات والافراد والجماعات الإرهابية المنظمة، والافراد من القراصنة وبين الباحثان مدى توافق قواعد القانون الدولي الإنساني مع الهجمات السيبرانية الحديثة، وقد وضحى ذلك حسب اراء الفقهاء الذين انقسموا الى اتجاهين مختلفين في

[1] . يحيى ياسين سعود، الحرب السيبرانية في ضوء قواعد القانون الدولي الإنساني، المجلة القانونية، مجلة متخصصة في الدراسات والبحوث القانونية، كلية الحقوق فرع الخرطوم، جامعة الازهر، المجلد3، العد4، 2018، ص90.

ذلك اولهما اكد على انعدام إمكانية تطبيق قواعد القانون الدولي الإنساني على الحروب السيبرانية معتبراً الفضاء السيبراني فضاءً حراً لا تملك أي سلطة لأي دولة التحكم فيه مما يتعذر لإخضاع هذه الحروب لقواعد القانون واحد مشترك نظراً لاشتراك جميع الدول في هذا الفضاء، والثاني، القائل بإمكانية تطبيق القانون الدولي الإنساني على الحروب السيبرانية مستنداً الى قيام القانون الدولي الإنساني تنظيم لوسائل الاتصال وغيرها في حالة النزاع المسلح لذا فهي قادرة على تنظيم الهجمات السيبرانية مستنداً الى المادة 36 من بروتوكول الإضافي الأول لإتقافية جنيف لعام 1949.

التحليل والنقد:

1. لم يذكر الباحثان الأمثلة على الحروب السيبرانية التي حدثة منذ اكتشاف الفضاء السيبراني وشبكات الانترنت
2. عدم قيامهم ذكر مفاهيم مقاربة للأمن السيبراني مثل: الجريمة السيبرانية، التجسس السيبراني، الإرهاب السيبراني...)
3. عدم ذكر الباحثان للمعاهدات والاتفاقات الدولية للحد من الهجمات السيبرانية مثل اتفاقية تالين للأمن السيبراني الذي وقعت من قبل جدول حلف الشمال الأطلسي (NATO)، وحماية البنية التحتية للدول.

المصادر:

1. ريتشار كلارك وروبرت كيه كنيك، حرب الفضاء الالكتروني الخطر القادم على الامن القومي وسبل معالجته، ط1(أبو ظبي: مركز الامارات للدراسات والبحوث الاستراتيجية، 2012)، ص

2. يحيى ياسين سعود، الحرب السيبرانية في ضوء قواعد القانون الدولي الإنساني، المجلة القانونية، مجلة متخصصة في الدراسات والبحوث القانونية، كلية الحقوق فرع الخرطوم، جامعة الازهر، المجلد3، العد4، 2018، ص90