سياسة الدول وموقفها من الهجمات السيبرانية

م.م. بلسم سعد عبد الستار (*)

المقدمة

اصبحت الهجمات السيبرانية واحدة من السبل والاساليب المؤثرة من دون تكاليف كبيرة فبعد ان كان النظام التقليدي يعتمد على القوة العسكرية البشرية لمواجهة باقي الدول او السيطرة عليها براً او جواً او بحراً الذي كان يكلف الدول الكثير من الخسائر البشرية والمادية ويتطلب الوقت والجهد فأن النظام الدولي السيبراني يعتمد اساساً على الوسائل الالكترونية لكل شؤون الافراد والمجتمعات واصبح بأمكان الدول التأثير على الاخرى وشل نظامها الأمني والعسكري عن بعد دون تكبد العناء ومن دون وقوع خسائر بشرية في صفوفها ، الا ان ماتحققه من دمار في الدول المعتدى عليها قد يفوق اثار النزاع المسلح التقليدي سواء في خسارة الارواح البشرية ام دمار البنى التحتية .

أهمية البحث:

أهمية هذه الدراسة لبيان مفهوم الهجمات السيبرانية وتكيفها قانونياً وتحديد مسؤولية الدول عن الهجمات التي يشنها افراد تابعين لها او احد اجهزتها .

هدف البحث:

الهدف من هذا البحث هو تكوين صورة واضحة المعالم عن البيئة الجديدة للمجال الافتراضي والهجمات المرتبطة بهذا المجال الذي اصبح مصير الدول ومستقبلها مرهوناً بقدرتها على التعامل معه والعمل على استثماره لاعادة تشكيل منظوماتها الامنية والتقنية في عصر المعلومات .

اشكالية البحث:

الهجمات السيبرانية لها أنواع مختلفة وأثارها واسعة ، تتخذ من الفضاء السيبراني الوسيلة والطريقة في التنفيذ ، فما هي الجهود الدولية المتعلقة بتنظيم استخدام الهجمات السيبرانية ؟ وهل هذه الجهود كافية ؟

(*) كلية العلوم السياسية - جامعة النهرين
balsam.saad@nahrainuniv.edu.iq

فرضية البحث:

ان ظهـور الهجمـات السـيبرانية بأنواعهـا المختلفـه جعل منها مصدر تهـدد للبنى التحتية للدول المعلوماتية منها والحيوية ، حيث جعلتها ضمن اولويات السياسـة الخارجيـة للعديد من الـدول وضمـن اسـتراتيجيات الامـن القومي لديهـا ،العمل على اسـتحداث وحـدات للحرب السـيبرانية لتحسـين القدرات الدفاعية امام تلك الهجمات.

مناهج البحث:

تـم الاعتمـاد في هـذه الدراسـة علـى المنهج الوضعي والمنهـج التحليلي والمنهج المقارن ، اضافتاً الى المنهج التاريخي .

هيكلية البحث:

يتكـون البحث مـن مبحثـان ، المبحث الاول بعنوان ماهية الهجمات السـيبرانية ومستوياتها ، والمبحـث الثانـي بعنوان جهود الدول بشـأن الهجمات السيبرانية .

المبحث الاول

ماهية الهجمات السيبرانية ومستوياتها

التطور المتسـارع فـي تكنولوجيـا المعلومات والإتصالات أدى إلى إعتماد الدول في مختلف الأبعـاد السياسـية والأمنيـة و الإجتماعيـة و الاقتصاديـة ، على الفضاء السـيبراني، الا إن هـذا التطور لـم يكن خاليـا مـن المخاطر، إذ قلـة التكلفة وثغـرات برامج شـبكات الإتصال وصعوبة كشـف الهوية ، تسـمح للدول و حتى الجهـات غير الحكومية أو الأفـراد ، بمهاجمة شـبكات دول أخرى والإضـرار بالبني التحتية المعلوماتيـة والحيويـة التابعـة لهـا، كتعطيل شـبكات الكهربـاء و قطع نظـام الإتصالات و تحطيم الطائـرات ، و غيرها من البنى التحتية التي تعتمد في تشـغيلها و عملهـا على الفضاء السيبراني .

المطلب الاول: مفهوم الهجمات السيبرانية

حـول التطـور الفضاء السـيبراني إلى سـاحة للتفاعلات في البيئة الإسـتراتيجية ، برز العديد مـن الأنمـاط التوظيفيـة له سـواء على صعيد الاستخدامات ذات الطبيعة المدنية أو العسكرية، الأمر الذي جعل هذا الفضاء مجالا للصراعات الحديثة، سواء للفاعلين من الدول أم غير الدول لحيازة أكبر قدر من النفوذ والتأثير السيبراني[٢]

تدور الهجمات السـيبرانية فـي دائرة العمليات الإليكترونية التي قـد ترتقى في بعض الاحيان إلى مسـتوى النزاع المسـلح أو مـا يضاهيها، وعليه هـي هجمات ذكية أقـوى من أي هجوم بري أو جوي، وأقل تكلفة، وهي تطور طبيعي في مفهوم الحروب.

إن الهجمات السـيبرانية أصبحت من التحديات الرئيسـة التي يتحتم على الـدول مواجهتها في العصر الراهن ومع تزايد الإعتماد على الإنترنت لاسيما في المجالات التي تتعلق بالأمن القومي كالشـبكات العسـكرية والأمنية تزايد الحديث عن أهميـة مواجهة هذه التهديـدات، و في هذا الإطار ظهر مفهوم الهجمات السـيبرانية و هي تصرفـات إلكترونية تقوم بها الدول أو الجهات التابعة لها ضد أنظمة و شبكات كمبيوترية تابعة لدول أخرى لأهداف أمنية او عسـكرية ، حيث تتضمـن الحرب السـيبرية عمليـات التخريب

والتجسس ، فالبيئة السيبرانية عبارة عن شبكة الكترونية لمجموعة من خوادم الكترونية فيما بينها قاعدة بيانات واحدة متاحة للجميع، تتفاعل هذه الشبكات فيما بينها باستخدام وسيلة تواصل افتراضية، متجاوزة كل الحواجز الجغرافية والسياسية سعيا وراء تحسين قدرة الاتصال والتعامل الإليكتروني، وهي أحد أكثر أنواع المجتمعات انتشارًا وحداثة.[٣]

تعرف الهجوم السيبرانية، بأنها التغلغل في شبكات الحواسيب في دولة، عبر شبكات الإنترنت والحواسيب التابعة لدولة أخرى أو منظمة ما، وتوصف الأنشطة الجارية في هذا الخصوص، بالهجوم السيبراني، كما تعرف بأنها إجراءات من قبل دولة أو كيان من غير الدول الاختراق أجهزة كمبيوتر أو شبكات دولة اخرى لأغراض التسبب في أضرار أو تعطيل نظام ما، ولكن تعريفات أخرى تشمل أيضا جهات فاعلة من غير الدول، مثل: «الجماعات الإرهابية والشركات الخاصة، والجماعات المتطرفة السياسية أو الأيديولوجية، والمنظمات الاجرامية عابرة للقومية» ، ومن هنا تبلورت مفاهيم جديدة في البيئة الإستراتيجية المسيبرة ان دخل سباق التسلح السيبراني، وظهور ساحات الحرب السيبراني، والجيش السيبراني، والهجوم السيبراني ، والمناورة السيبرانية ، والارهاب السيبراني .[٤]

المطلب الثاني: مستويات التعاطي مع الهجمات السيبرانية

إن التحدي الذي يواجه الدول في التعاطي مع الهجمات السيبرانية هو تحديد طبيعة ونطاق المجال الذي نتعامل، حيث يعد الفضاء السيبراني المجال الخامس بعد البر والبحر والجو والفضاء ، فالنشاطات التي تحدث في الفضاء السيبراني قد لا تتطابق مع المبادئ التقليدية التي تحكم النزاع المسلح والحرب، ولأجل ذلك يمكن القول إن الهجمات السيبرانية تنقسم إلى ثلاثة مستويات هي[٥]:

اولا: التجسس الإلكتروني

يعرف التجسس الإلكتروني على انه عملية اختراق شبكة أو جهاز إلكتروني، بهدف سرقة المعلومات المخزنة فيه، والتي عادة ما تكون على درجة كبيرة من الأهمية سواء أكانت معلومات عسكرية، سياسية ،اقتصادية، امنية ، وهو ما يترتب عليه آثار إستراتيجية فادحة للطرف الاخر هذا المستوى يوصف بأنه تجاوز الحدود الخصوصية الإلكترونية الفردية، مما يشكل اعتداء على الحقوق الشخصية للفرد، وانتهاكا لحرمة الحياة الخاصة، ومثال على ذلك ، "سرقة البيانات المالية ونشرها عبر الشبكة الإلكترونية للمعلومات" .

أصبحت العديد من الدول تلجأ إليها، لأن هذه الهجمات تستطيع إحداث خسائر كبيرة في وقت محدود، تلجأ اليها الدول إما اثناء قيام النزاعات السياسية والتوتر السياسي بين الدول، او في وقت الحروب بالتزامن مع العمليات العسكرية التقليدية.

ثانياً: الهجمات السيبرانية على المؤسسات

أن الدول ليست هي الهدف الوحيد للهجمات السيبرانية ، وانما أيضا المؤسسات سواء التجارية منها أم الخدمية، والمنظمات غير الحكومية التي اصبحت هي الاخرى عرضه للهجمات السيبرانية .

تعد المنظمات التجارية هدفًا رئيسيا كغيرها من المنشآت والأفراد المعرضين للهجمات السيبرانية ، حيث يمكن أن تتسبب الهجمات السيبرانية في عواقب وخيمة على أي عمل تجاري، لكن المنظمات الصغيرة معرضة للخطر بشكل أكبر عن غيرها، حيث تؤدي الهجمات السيبرانية الى صعوبة إمكانية وصول الموظفين إلى أنظمة الشركة التقنية ما إن لم تدفع الشركة المبلغ المقرر للمخترق حتى يسمح لهم بالوصول إلى أنظمة الشركة مرة اخرى وهو مايخلق عبئًا ماليًا كبيرًا ، كما يمكن أن تتسبب الهجمات السيبرانية في حدوث أضرار بالأجهزة والمعدات والأنظمة الخاصة بالمنظمة أو سرقة بيانات العملاء الشخصية وبيانات بطاقاتهم البنكية.

ثالثا : الهجمات السيبرانية العالمية

يضم هذا المستوى الحروب التي تحصل بين بعض الدول، أو الذي قد تشنه القوى الاقتصادية العالمية على بلدان بعينها ، وتوجيه تلك المعلومات توجيها مضادا لمصالحهم، حيث إن الدولة التي تمتلك هذه التكنولوجيا تحظى بالتفوق في ميدان المعركة، من خلال استخبارات نوعية وشاملة وقدرة هجومية دقيقة وخاطفة، وقدرة على الدفاع عن بنيتها التحتية الحيوية، إلى جانب قدرات عالية على السيطرة والتحكم وما يتبع ذلك مكن القول أن من الدوافع التي أدت إلى شن الهجمات السيبرانية، كونها نابعة من اهداف استراتيجية، اذ بدأت العديد الدول تعد العدة للتصدي لمثل هذه الهجمات ولشن هجمات أخرى مضادة ، كما حذر الخبراء من أن الفترة المقبلة ستشهد حرب جديدة، تتجلى بالحرب السيبرانية التي أصبحت اليوم واقع ملموس يثير قلق الكثير من دول العالم والعديد من المسؤولين وغيرهم من أصحاب الشركات ورؤوس الأموال ممن يخشون الوقوع بأيدي قراصنة الإنترنت، سواء أكانوا أفرادا أم مؤسسات استخبارية حكومية، تسعى إلى الحصول على بعض المعلومات المهمة عن الأعداء وتهدف إلى تدمير تقنياتهم عن طريق الهجمات الفايروسية المدمرة، اذ اجتاحت العالم أكبر موجة قرصنة عرفتها الدول حديثا، بعدما وجدت أكثر من ١٥٠ دولة حول العالم نفسها تحت رحمة سيل من الهجمات السيبرانية غير المسبوقة، التي أثرت على أداء العديد من المؤسسات والمنظمات الإستراتيجية حتى إن بعض المستشفيات والمدارس والجامعات لم تسلم من هجمات البرنامج الخبيثة لذا فان الاختراق السيبراني في البيئة الإستراتيجية هو قدرة الوصول إلى هدف تكنولوجي بطريقة غير مشروعة عن طريق ثغرات في نظام الحماية الخاص بالهدف.

المطلب الثالث : تميز الهجمات السيبرانية عن المفاهيم الاخرى

ان السيبرانية من العناصر غير التقليدية في تركيبة البيئة الإستراتيجية العالمية، ان ظهور السيبرانية مع بداية عقد التسعينات من القرن العشرين الا ان التفاعلات السيبرانية اخذت تزداد اهميتها ويتسع نطاقها مع بداية الحادي والعشرين ، وهو ما اضاف تهديدًا إلى سلم التهديدات في البيئة الإستراتيجية العالمية، ومن هنا تشكل التفاعلات السيبرانية في البيئة الإستراتيجية جانبا كبيرا من التفاعلات العالمية، واخذت اشكال عدة، اذ تخطت التفاعلات التقليدية التي كانت سائدة، واخذت

ركنا كبيرا ومهما في حيز العناصر التي تتكون منها البيئة الإستراتيجية العالمية و من هنا يجب التمييز بين الهجمات السيبرانية عن المفاهيم الاخرى:

اولا: الحرب السيبرانية

الحرب السيبرانية هي الإخلال أو التدمير الكلي لأنظمة المعلومات والإتصالات التابعة للعدو، وفي الواقع إن الحرب السيبرانية تهدف الى الإخلال بتوازن المعلومات لاسيما في غياب التوازن العسكري و عليه إن استخدام التفوق العلمي في الحرب السيبرانية سيغطي النقص في التجهيزات و القوات العسكرية و بالتالي يمكن تحقيق النصر فيه ، وتعرف الحرب السيبرانية بأنها، "إستعمال الحواسيب كسلاح أو أداة للقيام بأعمال عنف بقصد ترعيب أو تغيير رأي مجموعة أو دولة ما"، ويتم إستخدامه لأغراض سياسية وأيديولوجية عن طريق إستهداف البني التحتية الحيوية كالطاقة ، النقل، الإتصال والخدمات الضرورية كالطوارئ و الشرطة، وقد جاء تعريف الحرب السيبرانية في قاموس جامعة كامبريدج ،"بأنها أي نشاط يستخدم الإنترنت لمهاجمة الأجهزة الإلكترونية التابعة لدولة ما بقصد الإضرار بأشياء كأنظمة الإتصالات والنقل و موارد المياه والطاقة" ، إن إستخدام الحرب السيبرانية قد يؤدي الى زعزعة استقرار الأنظمة المالية، نظام الهاتف أو شبكة الكهرباء، وقد يغير الأمن القومي بشكل جذري بسبب هجوم قد يأتي من أي مكان.[٦]

ان الهجمات السيبرانية تحدث اثناء السلم والحرب ، اما الحرب السيبرانية هي نوع من الهجمات السيبرانية التي تحدث أثناء نزاع مسلح حركي أو التي تنتج آثار مادية تشبه وتعادل في آثارها الهجمات المسلحة التقليدية، بينما الهجمات السيبرانية هي كل نشاط سيبراني ضار بالدول الأخرى سواء كان في وقت السلم أو في سياق نزاع مسلح حركي وسواء نتجت عنه آثار مادية او معنوية .

ساعدت عوامل عدة على تنامي مثل هذه التهديدات الإليكترونية لمصالح الدول، ومن ثم إمكانية بروز حروب سيبرانية، من هذه العوامل هي : [٧]

١-تزايد ارتباط العالم بالفضاء الإليكتروني

٢-تراجع دور الدولة في ظل العولمة كفاعل

٣-تزايد اعتماد الدول على الأنظمة الإليكترونية

٤-قلة تكلفة الحروب السيبرانية

٥-تحول الحروب السيبرانية إلى إحدى أدوات التأثير في المعلومات

٦-توظيف الفضاء الإليكتروني في تعظيم قوة الدول

٧-اتساع نطاق مخاطر الانشطة العدائية التي يمارسها الفاعلون

وفي بعض الحالات يحدث تداخل بين الهجمات والحروب السيبرانية كما حدث لدولة إستونيا في ٢٧ أبريل ٢٠٠٧ من هجوم سيبراني شامل استهدف المواقع الإلكترونية الحكومية والبرلمان وحسابات البنوك والصحف، وتسبب هذا الهجوم في عزل الدولة عن العالم.

ثانياً: الجرائم السيبرانية

يمكن تعريف الجريمة السيبرانية بانها أي

جريمــة يمكن ارتكابها على نظام حاســوبي أو شــبكة حاســوبية، وتشــمل من الناحية المبدئية جميــع الجرائــم التي يمكــن ارتكابها فــي بيئة اليكترونية .

والجريمة السيبرانية هي كل فعل أو امتناع عن فعل باســتعمال نظام معلوماتي معين للإضرار بمصلحة أو حق يحميه القانون من خلال جزاء جنائي.

إن الهجوم السيبراني" هو عبارة عن التصرفات الإلكترونيــة التي تتســبب في قتــل أو دمار أو أضرار مادية تقوم بها دولة أو مجموعة مسلحة ضــد دولة أخــرى"، بينما الجريمة الســيبرانية تشــمل مجالاً أوســع بكثير من ذلك أي تتضمن كل النشاطات الإلكترونية غير القانونية ، لذلك ظهــرت عــدة إتجاهات فــي تعريــف الجريمة الســيبرانية فمن الفقهاء من إعتمد على وســيلة إرتكاب الجريمة كأســاس لتعريفه ، و قد ذهب عدد من الفقهاء الى الأخذ بمبدأ شخصية المجرم ، واعتمــد بعضهــم علــى موضــوع الجريمــة كأساس لفهم الجرائم السيبرانية.[٨]

إن الجرائم الســيبرانية و إن كانت تشــترك مع الهجمات الســيبرانية في البيئة الاستراتيجية إلا إنها تختلف عنها من حيث الفاعلين و الأهداف، فغالباً ما يكون مرتكبي الجرائم الســيبرانية هم الأفراد و توجة ضد مؤسسات مالية أو شركات وحتــى أفــراد داخــل أو خــارج إقليــم الدولــة ،بخلاف الهجمات الســيبرانية التي تتم من قبل دول أومجموعــات حكوميــة او غيــر حكومية ضــد دولة اخرى ، امــا الإختلاف الآخر يكمن في إن الجرائم السيبرانية غالباً ما يكون الهدف منها تحقيق مكاســب شخصية كســرقة الملكية الفكريــة عــن طريق شــبكات الحاســب الآلي أو التســلل الــى أنظمــة المصــارف والتلاعب بأرقام الحســابات و تحويــل الأموال ، بخلاف الهجمات الســيبرانية التي يســتهدف مرتكبوها الأمن القومي والسياســي لدولــة معينة. [٩]ثالثاً: الارهاب السيبراني

ان للإرهاب الســيبراني مخاطر واسعة النطاق على الصعيدين الاقتصادي والأمني ، له عواقب عديدة منها تعطيل البنى التحتية الحيوية، ووقف الخدمــات الاساســية والحياة اليومية، وســرقة المعلومات وتسريبها، مما يؤثر على زعزعت الأمــن والاســتقرار فــي الأنظمــة الحكوميــة والاقتصادية والتأثير على الاســتقرار السياسي والاجتماعــي، كما يهدف الإرهاب الســيبراني إلى خلق الفوضى والدمار والتسبب في خسائر ماديــة واقتصادية والإضرار بالمصالح الأمنية والعســكرية والمدنية للدول والمؤسســات ، ان للإرهاب السيبراني أشكال متعددة اهمها:[١٠]

١.القصف الإلكتروني لتدمير المواقع والبيانات الإلكترونية والنظم المعلوماتية

إدارة العمليــات الإرهابية، وتبــادل المعلومات من خلال الشبكة المعلوماتية.٢

٣. نشر الاشاعات الكاذبة بين الافراد

٤.البرمجيات الخبيثة الفايروسات

٥.التجســس الإلكترونــي والحصــول علــى المعلومات السرية

٦.الحروب الإعلامية وتأثير على الرأي العام العالمي

رابعاً: الجيوش السيبرانية

ان تاريخ ظهور الجيوش الإلكترونية يعود إلى

الثمانينيـات، عندما اسـتخدم مصطلح الجيوش السـيبرانية لأول مرة لوصف استخدام شبكات الكمبيوتـر للهجـوم والدفـاع ضـد الأهـداف العسـكرية والحكومية، ففي التسعينيات وأوائل العقـد الأول مـن القرن الحادي والعشـرين بدأ المتسـللون بتنفيذ الهجمات الإلكترونية، وكانت تركز بشـكل عام على القرصنة أو التسبب في اضطراب بدلاً من التسـبب فـي ضرر مادي، في عـام٢٠١٠ أصبحت الجيوش السـيبرانية مصـدر قلق متزايد وتحضى بالأهمية بالنسـبة للحكومـات والجيوش في جميع أنحـاء العالم، حيث بـدأت الـدول بتطوير أسـلحة وتكتيكات إلكترونيـة متطـورة، وتـم الإبلاغ عـن العديد من الهجمات السـيبرانية البـارزة على أهداف حكوميـة وعسـكرية، وغالبًـا مـا كانـت لهذه الهجمات عواقب وخيمة وتعطيل البنية التحتية.

يمكـن ان نعرف الجيـوش السـيبرانية " بأنها مجموعة من الأفـراد يتمتعون بخبرة عالية في مجـال تكنولوجيا المعلومـات ويعملون لصالح حكومـات أو دول أو جهـات ذات توجهـات سياسية محددة ويعملون في الخفاء دون الظهور للعلن وتسـتخدمهم الدول لحفظ أمنها السيبراني الوطني وشـن الهجمات السيبرانية على اهداف معينة" .

يتمتـع الجيـش السـيبراني بالقـدرة على شـنّ الهجمـات الإلكترونيـة علـى مواقـع مختلفـة واختراقهـا لجمع المعلومـات والحصول على مـا يخدم مصلحة الجهة التي يعمل لصالحها أو إلحاق التخريب ، كما تعتمد الجيوش السيبرانية في تنفيـذ هجماتها على طـرق مختلفة يصعب التصدي لها . [١١]

المبحث الثاني

جهود الدول بشأن الهجمات السيبرانية

ان تزايـد الاعتمـاد علـى شـبكات الاتصـال الالكترونيـة في كل مجـالات الحياه قد زاد من المخاطر التي قد تتعرض اليها الدول لا سـيمى فـي المجالات الحيويه والامنيـه من قبل الدول المعاديه .

ان التطـور السـريع فـي مجـال تكنولوجيـا المعلومـات ادى الـى ظهـور متغيـرات بعيده المـدى في المجالين العسـكري و الامني حيث ظهرت ابعاد جديده في طرق القتال و اسـاليب بنـاء القـوات المسـلحة مما دفع الدول لاسـيما القـوى العظمى في تطوير مجالهـا المعلوماتي لحماية امنها من الهجمات السيبراني المعادية .

المطلب الاول

الهجمات السبرانية اثناء النزاعات المسلحه

اولاً : سوريا ـ اسرائيل ٢٠٠٧

قـام سـلاح الجـو الاسـرائيلي فـي سـبتنبر ٢٠٠٧ بتنفيذ هجوم سـيبراني اسـتهدفه انظمه الاتصالات والرادارات السـوريه مما ادى الى تعطيلها بلكامل وذالك تمهيداً لغاره جوية نفذتها اسـرائيل لقصف مناطق زعمت اسرائيل بأنها كانت لانشـاء مفاعل نـووي وذالك قرب مدينه دير الزور[١٢] .

ثانياً : روسيا ـ جورجيا ٢٠٠٨

قامت القوات الروسـيا بشـن هجوم سـيبراني علـى جورجيـا في اب عـام ٢٠٠٨ اثر التوتر الذي شهده اقليم اوسـيتا الجنوبيه بسبب اعلانه الانفصـال عـن جورجيـا حيث اضعفـه قدره

وسـائل الدفـاع الجويـه الجورجيـا فضلًا عن الاضرار بمواقع الكترونيه كوسـائل الاعلام ، البنى التحتيه ، المواصلات ، مما ادى الى ارباك واسع في جورجيا وتزامناً مع تلك الهجمات قام الجيش الروسـي بتنفيذ عمليات عسـكريه على جورجيـا و يعد هاذا النزاع المسـلح الاول من نوعة الذي تزامنت فيه الهجمات السيبرانيه مع الهجمات العسكريه بهاذا الشكل الواسع [١٣] .

المطلب الثاني

الهجمات السيبرانيه خارج النزاعات المسلحه

اولا: الهجوم على المنشأت الايرانيه النووية

هجوم سـيبراني تدميري على المفاعل النووي الايراني بوشـهر و نطنز من قبل تحالف دولي اشـتركت فيه اسرائيل و الولايات المتحده ، ان هاذا الهجوم عمل على زياده سـباق التسلح في الفضاء السـيبراني اذ الاشـك في ان الهجوم قد جسـد الطاقه الهائله الكامنه للسلاح الالكتروني عبر الفضاء السـيبراني و اعتبره حدثاً مؤسساً في تطوره كامجال لشأن هجمات مدمره[١٤] .

ثانيا: الولايات المتحدة ـ الصين

منذ قيـام الصين الشـعبية وهي تحلـم بالريادة فـي العالـم وهذا مـا تؤكـده اصلاحاتهـا عام ى١٩٧٨التي جعلتهـا الثانية اقتصاديا والاولى عالميا في كثير مـن الجوانب وهذه الطموحات تعـد تحديا كبيـرا لواشـنطن التي تخشـى من انهـاء ريادتهـا ونفوذها العالمـي وانتقال القوة من الغرب الى الشـرق لذلك اصبحت الهجمات السيبرانية ساحة حرة للصراع بين القوتين دون دماء او خسائر في الارواح[١٥] .

ومنها هجوم سـيبراني قامت به لجان المقاومة الشـعبية الصينيـة المرتبطة بالجيـش الصيني عـام ١٩٩٩ اذا قامت بالهجـوم على العديد من المواقع الحكوميـة الامريكية في رد غير معلن علـى قيام الاخيـرة بمهاجمـة وتخريب الموقع الالكترونـي للسـفارة الصينيـة فـي بلغراد في ١٩٩٩. [١٦]

المطلب الثالث

تكييف الهجمات السيبرانية

تكييـف الهجمـات السـيبرانية يقتضـي تحديد مصـدر الهجمات واساسـها وبالذات بعد تنامي اسـتخدام شـركة المعلومـات والاتصالات في شتى المجالات وتنوع اشكال التهديدات الناجمة عنها وصورها بشـكل مطـرد مما يجعل مهمة حصرهـا وتكيفها امـرا صعبا للغايـة وهو ما يشـكل تحديـدا كبيـرا يواجهه التنظيـم الدولي المعاصر

اولا: مبدأ السيادة

ان فكـرة السـيادة والاعتـراف بها للـدول من المبـادئ المتفق عليها في ميثـاق الامم المتحدة والاتفاقيـات الدوليـة الا ان تشـعب العلاقـات والمصالح في المجتمع الدولي ادى الى اختراق هذه السيادة .

ظهور الهجمات السيبرانية يعد تحدي امام سيادة الدولة ونطاقها حيث ادت التغيرات التكنولوجيا الى تغيـر المفهوم التقليدي للسـيادة من خلال ظهـور مفاهيـم جديدة منها ما يعرف بالسـيادة الرقمية التي تعرف بانها بسط الدولة لسيطرتها على الفضاء الرقمـي المتمثل بالانترنيت الذي يجتاز حدود الدولة [١٧] .

ان اضمحـلال الحـدود الجغرافية فـي الفضاء

السـيبراني لايعنـي خروج الفضاء السـيبراني عن نطاق سـيطرة وسـيادة الدولـة ، حيث ان الفضـاء السـيبراني يتطلـب اجهـزة ومعدات مادية التي من دونها لا يسـتطيع المسـتخدمون الحصـول عليـه وبما ان هـذا الهيـكل المادي يقـع ضمن اراضـي الدولة فمـن الطبيعي ان يقـع ضمـن اختصـاص تلـك الدولـة وبالتالي تفرض سـيطرتها وسـيادتها عليـه ومن ناحية اخـرى ان الفضاء السـيبراني بحد ذاته يتطلب التنظيـم والرقابة من قبل الدولة لذلك شـرعت الدول بمعالجة مشـاكل السيادة لتلافي المخاطر المسـتقبلية نتيجة اسـتخدام الفضاء السـيبراني سـواء على الصعيد الوطنـي ام الدولي فقامت اغلبيتها بتطوير تشـريعاتها الوطنية لاستيعاب الجرائم التـي تحدث في نطـاق اقليمها وقامت بالتنسـيق مع الدول الاخرى عـن طريق ابرام اتفاقيات تعني بتنظيم الجرائم السـيبرانية وحل مشكلة السيادة من خلال الاتفاق على اليات تتبع مصادر الجرائم[١٨] .

يمكن القول ان سـيادة الدولة على البنى التحتية السيبرانية لاتقتصر على تلك الواقعة او المشيدة علـى اقليم الدولة بل تمتد الـى كل البنى التحية السـيبرانية التي تخضع لسيطرتها بشكل كامل وان كانـت فـي اقليم دولـة اخـرى وبذلك فأن الهجمات السـيبرانية التي توجـه من قبل دولة معينه ضد البنى التحتية السيبرانية التابعه لدولة اخرى يمكن ان يمثل خرقا لسـيادة دولة خاصتا اذا تسببت تلك الهجمات باحداث اثار مدمرة[١٩].

ثانيا: مبدأ سلوكيات الحرب

ان الهجـوم السـيبراني القائـم بذاته لا يشـكل نزاعا مسـلحا الا ان الهجمات السيبرانية قد يتم اسـتخدامها اثناء النزاعات المسـلحة او لتمهيد الطريـق لهجوم تقليـدي بهدف تحقيـق التفوق والميزة العسـكرية ان مبـادئ وقواعد القانون الدولـي الانسـاني المطبق في النزاع المسـلح تنطبق على جميع اشكال الحروب وعلى جميع انـواع الاسـلحة ، وبذلـك فان القانـون الدولي الانسـاني او مبدأ سلوكيات الحرب ينطبق على الهجمات السيبرانية التي تحدث في اثناء النزاع المسلح [٢٠] .

ان الهجمات السـيبرانية تعد تحدي جديد يواجه المجتمـع الدولي خاصتا في فتـرات النزاعات المسـلحة ان اللجـوء الى الهجمات السـيبرانية يجب ان يكون ضرورة لتحقيق هدف عسكري مشـروع وهنا يظهـر التحدي حيث ان مسـألة تحديد الاهداف والمنشأت العسكرية في الفضاء السيبراني تثير تحديا امام المجتمع الدولي وذلك لان المنشـأت التي تقدم خدمة للقطاع العسكري هي في الوقت نفسه تخدم القطاع المدني [٢١] .

كمـا ان تحقيـق التناسـب فـي اسـتخدام القوة المسـلحة يشـكل تحديا فريـدا من نوعـه امام التنظيم الدولي وذلك لان اثار الهجوم السيبراني عـادة مـا تكون غير مباشـرة ، حيـث ان مبدأ التناسـب يتطلب توقع النتائج المحتملة للنشـاط العدائي وهذا الامر مسـتحيل بالنسبة للهجمات السيبرانية [٢٢] .

ان التحـدي الاصعـب فـي تطبيق سـلوكيات الحرب على الهجمات السيبرانية هو مبدأ تميز الهجمات السـيبرانية وذلك لتشـابك الاستخدام المدني والعسـكري لنفـس الشـبكات ، لذا من الممكـن ان تكـون الشـبكات المدنيـة اهدافـا عسكريا جذابة.

الخاتمة :

ان اشـكال القـوة تتغير بتغيـر التكنولوجيا وقد اثـر الفضاء السـيبراني في الاشـكال التقليدية للقـوة وطـرح مفهوم وشـكلا جديدا هـو القوة الالكترونيـة وقـد كان هذا الشـكل الجديد دور في بلورة مفهوم انتشـار القوة وتعـدد الفاعلين الممارسـين لهـا سـواء من الـدول او من غير الـدول مما هدد الـدور التقليدي للدول وقلل من سيادتها في اقليمها ولم ينته الامر عند ذلك حيث ظهرت اشـكال جديدة من الاسلحة فعلى الرغم مـن صغرها الذي لا يتجاوز الكيلو بايتس وقلة تكلفتها فقد تسـبب خسـائر فادحة على مختلف المستويات الاقتصادية والسياسية والعسكرية .

وهكـذا، تُعـد قدرات الأمـن السـيبراني وانفاذ القانون هامة لحماية وضمان الفضاء السيبراني. اذ يلعب القانون دورًا أساسـيًا في تحقيق أهداف أمـان الإنترنـت، وذلك من خـلال التحقيق في مجموعة كبيرة مـن الجرائم الالكترونية إبتداءً من السـرقة والاحتيـال وصولا إلى اسـتغلال الأطفال، والقبض على المسؤولين ومحاكمتهم. ويبـرز مـن بيـن واجبـات وزارات الداخليـة والعدل لدى مختلف الدول أهمية تبني تحقيقات جنائيـة وإجـراءات فعالـة لعرقلـة مجرمـي الإنترنت وردعهـم، وإعطاء الأولوية لتوظيف وتدريـب الخبـراء التقنيين، وتطوير أسـاليب موحـدة، وتبادل أفضل الممارسـات والأدوات المتعلقـة بالاسـتجابة الالكترونيـة على نطاق واسـع. يعمل المحققون الجنائيون وخبراء أمن الشـبكات –ممن يمتلكون فهمـا عميقا للتقنيات التي تسـتخدمها الجهات الفاعلة الشريرة ونقاط الضعف المحددة التي تستهدفها- على الاستجابة الفعالة للحوادث السيبرانية والتحقيق فيها.

ومن ثـم يعد التهديد الالكترونـي من المخاوف المتزايدة للبنية التحتية الحيوية، والتي تتعرض بشـكل متزايد للإختـراق الإلكتروني المتطور الذي يشكل مخاطر جديدة. وكما باتت تكنولوجيا المعلومـات تندمج على نحو متزايد مع عمليات البنية التحتية المادية، أصبح هناك خطر متزايد مـن أحداث واسـعة النطـاق أو عاليـة النتائج يمكن أن تسبب الضرر أو تعطل الخدمات التي يتوقف عليها الاقتصاد والحياة اليومية للملايين في العالم المعاصر في ضوء المخاطر والنتائج المحتملة للأحـداث الالكترونية. وهكذا، أصبح تعزيز أمن ومرونة الفضاء السيبراني عمل هام للأمن الوطني بالنسبة لمختلف الدول.

ومـع ذلك، يصعـب تأمين الفضاء السـيبراني بشـكل خاص بسـبب عدد من العوامـل: قدرة الجهـات الفاعلة الشـريرة علـى العمل من أي مـكان في العالم، ووجـود الروابط بين الفضاء السـيبراني والنظـم الماديـة، وأخيـرا صعوبة الحد من نقاط الضعف والعواقب في الشـبكات المعلوماتية المعقدة.

المصادر

الدراسات والبحوث:

خالـد وليد محمود، الهجمـات عبر الانترنيت : سـاحة الصراع الالكترونـي , المركز العربي للابحاث و دراسة السياسات ، قطر ، ٢٠١٣.

سـامر مؤيد عبد اللطيـف ، الحرب في الفضاء الرقمـي (رؤيـة مسـتقبلية) بحث منشـور في مجلة رسـالة الحقوق ، جامعة كربلاء ، السـنة السابعة العدد الثاني ,٢٠١٥.

د.علـي زيـاد العلـي ، د.علـي حسـين حميد ،

تكتيكات الحـروب الحديثة "الامن السـيبراني والحروب المعززة والهجينة" ، العربي للنشـر والتوزيع ، القاهرة، ٢٠٢٢.

د.محمـود عبابنـة، د.محمد معمـر الرازقي ، جرائم الحاسـوب وابعاده الدوليـة ، دار الثقافة للتوزيع والنشر ، عمان ، ٢٠٠٥.

د. حبيب وصفـي، تحليل الصراعـات الدولية " دراسـة نظريـة تطبقيـة، ط١، دار الحـوار للطباعة والنشر، القاهرة ٢٠١٦.

د.مصطفى محمد موسـى، التحقيق الجنائي في الجرائم الإلكترونية ، مطابع الشـرطة، القاهرة ، ٢٠٠٩

د.أحمـد خليفة الملط، الجرائم المعلوماتية ، دار الفكر الجامعي الإسكندرية، ط ثانية ٢٠٠٦٠

الاطاريح:

سـراب ثامـر احمـد ، الهجمات على شـبكات الحاسـوب فـي القانـون الدولـي الانسـاني ، اطروحـة دكتوراه ، فـي القانون العام ، جامعة النهرين ، كلية الحقوق ، ٢٠١٥ .

المصادر الاجنبية:

Jonathan a. ophard," cyber warfare and the crime of aggression; the need for individual accountability .on tomorrow battlefield" review

See Joshua e. kastenberg, nonintervention and neutrality in cyberspace; an emerging principle in the national practice of air force law ٦٤, international law .review

الموقع الالكتروني:

www.military.com\ html,.٠٠ ,٠١٥٢٤٠,٢١٠٤٨٦\features ٢٢.٢٠١٥.feb accessed

دوافـع تبقي الحـرب الالكترونية بيـن الصين وامريـكا مسـتمرة ، مقالة منشـورة ، ٢٠١٥، ٥\www.amnay.mag.com

اللجنة الدولية للصليب الاحمر ، القانون الدولي الانسـاني وتحديـات النزاعـات المعاصـرة ، تقرير تشـرين الاول \ اكتوبر ٢٠١١ www. icrc.org

حمايـة الاعيـان المدنيـة فـي القانـون الدولي الانسـاني ، ٢٠٠٨ بحـث منشـور علـى الموقـع : www.mezan.org\uploads\ pdf.٨٧٩٨\files

دسـند راهبردي بدافند سايبرى كشور سازمان پادافند غير عامل كشور، مركز بدافند سايبري كشـور التالي، ص ٢٤ منشـور علـى الموقع الرسمي :

http://d-padafand.farsp.ir/ att-pdf/٩٦/upload

محمد فخر الدين، حـدود المجال الخامس . ما هي الحروب السيبرانية مؤتمر حروب الفضاء السـيبراني مايـو ٢٠١٥ متوفـر علـى الموقع الالكتروني:

http://seconf.wordpress. ١٥/٠٥/٢٠١٥/com

م.م فاضـل عباس صبـاح ، تهديدات الارهاب السـيبراني في عصـر الـذكاء الاصطناعي ، جامعة كربلاء ، ٢٠٢٤ :

https://ukerbala.edu.iq/archives

د. وفـاء فـوزي ، مفاهيم الجيـش الالكتروني الذبـاب الالكترونـي وصناعـة الـرأي العام ، أوراق سياسية وبحثية ، مركز البيان للدراسات والتخطيط، ٢٠٢٣:

https://www.bayancenter.
٩٧٣٧/٠٥/٢٠٢٣/org

الهوامش

١- محل العمـل: جامعة النهريـن/ كلية العلوم السياسية- قسم الاستراتيجية

العنوان: بغداد

٢ - د.علـي زيـاد العلي ، د.علي حسـين حميد ، تكتيكات الحروب الحديثة "الامن السـيبراني والحروب المعززة والهجينة» ، العربي للنشـر والتوزيع ، القاهرة، ٢٠٢٢، ص ١٤٣

٣- دسـند راهبـردي بدافنـد سـايبرى كشـور سازمان پادافند غير عامل كشور، مركز بدافند سـايبري كشـور التالي، ص ٢٤ منشور على الموقع الرسمي :

http://d-padafand.farsp.ir/
att-pdf/٩٦/upload

٤- د.علـي زياد العلي ، د.علي حسـين حميد ، تكتيكات الحـروب الحديثة "الامن السـيبراني والحـروب المعززة والهجينة" ،مصدر سـبق ذكره ، ص ١٤٤

٥- د.محمـود عبابنة، د.محمد معمر الرازقي ، جرائم الحاسـوب وابعاده الدوليـة ، دار الثقافة للتوزيع والنشر ، عمان ، ٢٠٠٥، ص٣٨٤

٦- محمد فخـر الدين، حدود المجـال الخامس . مـا هي الحـروب السـيبرانية مؤتمر حروب الفضـاء السـيبراني مايـو ٢٠١٥ متوفر على الموقع الالكتروني:

http://seconf.wordpress.
١٥/٠٥/٢٠١٥/com

٧- د. حبيب وصفي، تحليل الصراعات الدولية " دراسـة نظريـة تطبقيـة، ط١، دار الحـوار للطباعة والنشر، القاهرة ٢٠١٦، ص ١٣٨

٨- د.مصطفى محمد موسـى، التحقيق الجنائي فـي الجرائـم الإلكترونيـة ، مطابع الشـرطة، القاهرة ، ٢٠٠٩، ص ١١٢.

٩- د. أحمـد خليفة الملط، الجرائم المعلوماتية ، دار الفكر الجامعي الإسكندرية، ط ثانية ٢٠٠٦ ، ص ٨٥

١٠- م.م فاضـل عبـاس صبـاح ، تهديـدات الارهـاب السـيبراني فـي عصـر الـذكاء الاصطناعي ، جامعة كربلاء ، ٢٠٢٤

https://ukerbala.edu.iq/archives

١١- د. وفاء فوزي ، مفاهيم الجيش الالكتروني الذبـاب الالكترونـي وصناعـة الـرأي العام ، أوراق سياسية وبحثية ، مركز البيان للدراسات والتخطيط، ٢٠٢٣.

https://www.bayancenter.

/٩٧٣٧/٠٥/٢٠٢٣/org

12-www.military.com\features\015240,210486,00.html, accessed22 feb.2015.

13-Jonathan a. ophard," cyber warfare and the crime of aggression; the need for individual accountability on tomorrow battlefield" review,no .3 .p.2

١٤- خالد وليد محمود، الهجمات عبر الانترنيت : ساحة الصراع الالكتروني , المركز العربي للابحاث و دراسة السياسات ، قطر ، ٢٠١٣، ص١٩

١٥- دوافع تبقي الحرب الالكترونية بين الصين وامريكا مستمرة ، مقالة منشورة ، ٢٠١٥، ٥\www.amnay.mag.com

١٦- سامر مؤيد عبد اللطيف ، الحرب في الفضاء الرقمي (رؤية مستقبلية) بحث منشور في مجلة رسالة الحقوق ، جامعة كربلاء ، السنة السابعة العدد الثاني ,٢٠١٥ ,ص ٨٦.

١٧- سراب ثامر احمد ، الهجمات على شبكات الحاسوب في القانون الدولي الانساني ، اطروحة دكتوراه ، في القانون العام ، جامعة النهرين ، كلية الحقوق ، ٢٠١٥ ، ص١٠١.

18- See Joshua e . kastenberg ,non intervention and neutrality in cyberspace ;an emerging principle in the national practice of international law ,64 air force law review.

١٩- سراب ثامر احمد ، مصدر سابق الذكر ، ص١١٨.

20- cj nuclear weapons advisory opinion ,op .cit , para 86.

٢١- اللجنة الدولية للصليب الاحمر ، القانون الدولي الانساني وتحديات النزاعات المعاصرة ، تقرير تشرين الاول \ اكتوبر ٢٠١١ .www icrc.org

٢٢- حماية الاعيان المدنية في القانون الدولي الانساني ، ٢٠٠٨ بحث منشور على الموقع : www.mezan.org\uploads\ pdf.٨٧٩٨\files

الملخص

عالم اليوم أكثر ترابطًا من أي وقت مضى. ومع ذلك ، فبالنسبة إلى جميع مزاياه، فأن الترابط المتزايد أدى الى تزايد مخاطر السرقة والاحتيال والإساءة. ومع تزايد اعتماد الأشخاص حول العالم على التكنولوجيا الحديثة، أصبحوا أكثر عرضة للهجمات الإلكترونية مثل اختراق أمن الشركات، والتصيّد الاحتيالي، وممارسة الابتزاز والنصب والاحتيال عبر وسائل التواصل الاجتماعي. ويلاحظ أن الفضاء السيبراني والبنية التحتية الأساسية له عرضة لمجموعة واسعة من المخاطر الناجمة عن التهديدات والمخاطر المادية الالكترونية. إذ تستغل الجهات الفاعلة ألكترونيا وكذلك الدول القومية نقاط الضعف لدى خصومها لسرقة المعلومات والأموال وتطوير القدرات لتعطيل وتدمير أو فقط تهديد قدرة دولة الخصم على تلبية الخدمات الأساسية. كما أن هناك مجموعة من الجرائم التقليدية تُرتكب الآن عبر الفضاء السيبراني، ويشمل ذلك إنتاج وتوزيع المواد الإباحية

للأطفـال والأحـداث ومؤامـرات اسـتغلالهم، والاحتيـال المصرفـي والمالـي، وانتهـاكات الملكيـة الفكريـة، وجرائـم أخـرى، وكلها لها عواقب أنسانية واقتصادية وقانونية كبيرة.

Abstract

Today›s world is more interconnected than ever. However, for all its advantages, the increasing interdependence has led to an increased risk of theft, fraud and abuse. As people around the world increasingly rely on modern technology, they are becoming more vulnerable to cyberattacks such as corporate security breaches and phishing. And the practice of extortion, fraud and fraud through social media. It is noted that cyberspace and its core infrastructure are vulnerable to a wide range of risks arising from cyber physical threats and risks. Cyber actors as well as nation-states exploit the vulnerabilities of their adversaries to steal information and money and develop capabilities to disrupt, destroy, or only threaten the adversary›s ability to meet basic .services

A host of traditional crimes are now being committed through cyberspace, including the production and distribution of child and juvenile pornography and exploitation plots, bank and financial fraud, intellectual property violations, and other crimes, all of which have significant humanitarian, economic and legal .consequences