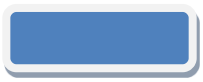
دراسات
في العلوم السياسة

تأثير التهديدات السيبرانية في الصراعات الإقليمية (نماذج مختارة)

الاستاذ الدكتور
بهاء عدنان يحيى
جامعة الكوفة ـ كلية العلوم السياسية

المدرس المساعد
شهد حمزة ميرعلي



تأثير التهديدات السيبرانية في الصراعات الإقليمية (نماذج مختارة)

The impact of cyber threats in regional conflicts (selected models)

الاستاذ الدكتور
بهاء عدنان يحيى
جامعة الكوفة ـ كلية العلوم السياسية

Prof. Dr. Bahae Adnan Yahya
College Political Science / University of Kufa
bahaa.alsabary@uokufa.edu.iq

المدرس المساعد
شهد حمزة ميرعلي

Shahad Hamza Mir Ali

الملخص :

شهد العالم المعاصر منذ مطلع القرن الحالي سباقاً بين مختلف القوى الكبرى والاقليمية لاستغلال الفضاء السيبراني والاستفادة من المزايا الكبيرة التي يوفرها في تحقيق مكاسب استراتيجية حيوية لم تكن تتوقع تلك القوى بتحقيقها عن طريق استخدام القوة العسكرية التقليدية. لقد اصبحت قضية "الهجمات السيبرانية" واحدة من اهم واعقد القضايا التي تثير قلق الدول الكبرى المتقدمة تكنلوجياً قبل غيرها من دول العالم الاخرى الاقل تقدماً، وذلك لما تسببه من اثار وانعكاسات خطيرة تهدد امنها القومي ومصالحها العليا ،و ان ظهور الفضاء السيبراني كقوة جديدة في العلاقات الدولية وفاعل مؤثر في تلك العلاقات معتمداً على التقدم التكنولوجي ، ونتيجة لانتقال جزء كبير من الصراعات الى مجال الفضاء السيبراني ، ودخول المجتمع الإقليمي مرحلة جديدة تحاول فيه الدول الى تعزيز قدرتها من اجل ممارسة الهيمنة والسيطرة والتأثير في البيئة الاقليمية والدولية ظهرت فيها التهديدات تسمى بالتهديدات السيبرانية ،وإن الأمن السيبراني يهدف الى ضمان تحسين الأمن الذي من شأنه الدفاع عن المنظمات من التعرض لهجوم من قبل المتسللين عبر الشبكة العنكبوتية ، وهذا مرده إلى أن العالم أصبح أكثر ارتباطاً بواسطة الشبكات العنكبوتية لتنفيذ المعاملات العامة ويقوم الأمن السيبراني بالحفاظ عليها .

الكلمات المفتاحية : الأمن السيبراني ـ الأمن السيبراني الإقليمي ـ تطور خصائص الهجمات السيبرانية .

Abstract:

Since the beginning of the current century, the contemporary world has witnessed a race between the various major and regional powers to exploit cyberspace and take advantage of the great advantages it provides in achieving vital strategic gains that those powers did not expect to achieve through the use of conventional military force. The issue of "cyber attacks" has become one of the most important and complex issues that concern the major technologically advanced countries before other less developed countries of the world, because of the serious effects and repercussions that threaten their national security and higher interests, and that the emergence of cyberspace as a new force in relations International and an influential actor in those relations, relying on technological progress, and as a result of the transfer of a large part of the conflicts to the field of cyberspace, and the entry of the regional community into a new phase in which countries try to enhance their ability to exercise hegemony, control and influence in the regional and international environment in which threats called cyber threats appeared, And cyber security aims to ensure the improvement of security that would defend organizations from being attacked by hackers through the Internet, and this is due to the fact that the world has become more connected by means of Internet networks to carry out public transactions and cyber security maintains them.

Keywords: cyber security – regional cyber security – the evolution of the characteristics of cyber attacks.

المقدمة :

بعد انتهاء الحربين العالميتين وما خلفتهما من آثار وخسائر بشرية ومادية، بدأت الدول بالبحث عن وسائل وأساليب أخرى للقتال من شأنها أن تحقق لها الميزة العسكرية على الخصوم، ومن دون تحمل الخسائر والمخاطر التي يتحملها القائم بالهجوم في إطار استخدامه للأسلحة التقليدية. وقد توصلت هذه الدول في العقد الأخير إلى أحدث هذه الوسائل التي تتسم بالتعقيد واجتياز الحدود التقليدية، وهي الهجمات السيبرانية التي من شأنها تدمير البنية التحتية للخصم، والتسبب بآثار فادحة على البنية العسكرية والمدنية للخصم، وذلك كله من دون الحاجة إلى الدخول في أي اشتباك حقيقي ومادي مع الخصم، ومن دون الحاجة لتحمل أعباء مالية ومخاطر المواجهة المسلحة التي يتحملها المهاجم في إطار استخدام الأسلحة التقليدية ، و يشهد العالم اليوم موجات من التغيرات و التطورات المتسارعة و لتعاظم وتيرة الابتكارات التقنية والإلكترونية والتي أضحت تضيف وبشكل يومي كل ما هو جديد ومتطور في عالم تكنولوجيا المعلومات ، و ان ما يميز الفضاء الالكتروني عن غيره من للصراعات التقليدية هو صعوبة تحديد هوية المهاجم في اغلب الهجمات الالكترونية، وبخاصة إذا ما اتسمت بدرجة عالية من التعقيد. فكلما زادت درجة تعقيد الهجوم الالكتروني، زادت صعوبة تحديد هوية المهاجم ولم يعد بالإمكان التخلي عن التقنيات الحديثة والتي دخلت في شتى المجالات وشكلت البنية التحتية لأغلب الدول المتقدمة ، حيث دخل الفضاء السيبراني كمجال جديدة في العلاقات الدولية وفاعل مؤثر في تلك العلاقات معتمداً على التقدم التكنولوجي الذي يعزز قدرة الدولة على ممارسة الهيمنة والسيطرة والتأثير في البيئة الاقليمية والدولية ، و مكنت من ان تحدث نقله في معيار ما تمتلكه الدول من قوة تمكنها من مواصلة الاستجابة و القدرة على مواجهة التهديدات السيبرانية في بيئة الفضاء السيبراني .

أهمية الموضوع:

إن أهمية الموضوع تنبثق من أهمية بيئة التطور التكنولوجي وانعكاساتها على البنية التحتية المعلوماتية للدول الاقليمية، ويعد الفضاء السيبراني مجالاً عاماً بين من يستخدمونه ويتفاعلون معه ، مع الأخذ بنظر الاعتبار على أهمية التركيز على مقدار الخطر المحدق بمستخدمي الفضاء الإلكتروني وهذا ما جعل الفضاء السيبراني بيئة جاذبة لمستخدميها، ويمكن توظيفها لتحقيق أهداف في غاية الأهمية من خلال:

١. فهو يسعى الى فهم وتفسير العلاقات الدولية والسياسة الإقليمية والعالمية المعاصرة، خاصة

في ظل الطبيعة المتغيرة للتهديدات الأمنية المختلفة.

٢. ويعد الفضاء السيبراني مجالاً عاماً، بسبب انتقال كافة مجالات الحياة الى الفضاء السيبراني أثرت على البيئة الأمنية فيه وأفرزت عدة تداعيات أثرت على أمن.

٣. ارتفاع مستوى التهديدات السيبرانية بعد الاعتماد الكلي للدول في استراتيجياتها في مجالات الأمن والقوة العسكرية على الفضاء السيبراني وتؤدي بالتالي الى زيادة انتشار الصراع الدولي.

الإشكالية:

في ظل تزايد الاعتماد على التكنولوجيا و توظيفها في القطاعات السياسية و العسكرية و الاقتصادية أصبحت هذه القطاعات عرضة للتهديد و الهجوم من خلال المنافذ الالكترونية، فأن إشكالية الدراسة تكمن في ان التهديدات السيبرانية أصبحت احد وسائل الدول و الفواعل الإقليمية و الدولية في فرض التهديدات و بذلك أضحت البنية الإقليمية متأثرة بتوظيف هذه الأسلحة السيبرانية في صراعاتها الإقليمية و يتفرع من هذه الإشكالية مجموعة تساؤلات.

١. كيف يمكن التعامل مع واقع التهديدات السيبرانية التي فرضت واقعاً جديداً يعرض الامن الإقليمي للخطر؟

٢. ما القدرات السيبرانية للدول وكيف وظفت استراتيجيات خاصة بالأمن السيبراني لتطوير قدراتها السيبرانية؟.

٣. كيف تؤثر الحروب الالكترونية على الامن الإقليمي؟.

الفرضية:

إن الدراسة تنطلق من فرضية مفادها أن في ظل الاعتماد المتزايد للدول على التكنلوجيا والبنية التحتية المعلوماتية، فأن الفرضية تحاول إثبات ما يأتي: ان تزايد التهديدات السيبرانية بين الفواعل من الدول تؤدي بالنتيجة الى زيادة حدة انتشار الصراع الاقليمي وذلك من خلال الاستخدام المتزايد من قبل الدول الكبرى والإقليمية والجماعات والأفراد للقوة السيبرانية .

منهاج الدراسة:

تقتضي ضرورة البحث العلمي عند دراسة أي ظاهرة، تحديد المنهج الانسب لها لكي يكون الوسيلة أو الطريق الصحيح للوصول الى النتائج، وقد تم الاستناد في هذه الدراسة على المنهج الاستقرائي، بوصفه منهجا اساساً، فضلا عن استخدام بعض المناهج الاستدلالية بطريقة علمية أساسا لتحقيق النتائج المرجوة من هذه الدراسة ، وضمن هذا السياق، لذلك كان لابد من استخدام المنهج الوصفي لغرض وصف الظاهرة وتحليلها. وبعدها تمت الاستعانة بالمنهج التحليلي عبر عرض إشكالية البحث ومناقشتها

والبرهنة عليها عن طريق معرفة المدخلات والمخرجات، وكيفية التأثير المتبادل فيما بينها وصولاً إلى الاستنتاجات .

المبحث الأول

مكانة التكنلوجيا في الأمن السيبراني الإقليمي

للأمن السيبراني أهمية بالغة في حياتنا المعاصرة ، نظراً لاعتمادنا الكبير على تكنلوجيا المعلومات في شتى عملياتنا اليومية ، والتي أصبح تتشكل عصب حياتنا القائمة ، إذ أضحت المعلومة سلاحاً ينافس الأسلحة التقليدية وغير التقليدية في عصرنا الحالي ، فهي قد تساهم في تعالي شؤون الدول ، أو ربما تؤدي إلى تهاوي دول كثيرة إذا ما تم الكشف عن جوهر معلوماتها الأمنية ، لذلك تهدف هذه الهجمات عادة إلى اختراق البيانات الدقيقة والأساسية على اجهزة الكمبيوتر التي تتمتع بسرية وتغييرها وتدميرها ، يمكن القول أن أمن المعلومات الإلكترونية هو عبارة عن محاولة تكثيف الجهود السياسية والاقتصادية والاجتماعية والتكنولوجية الرامية لحماية المحتوى المعلوماتي للأفراد والمؤسسات والحكومات والدول من أية ثغرات داخلية أو خارجية وهو يمثل تنفيذ تدابير لحماية النظم والشبكات وتطبيقات البرمجيات من الهجمات الرقمية.

وعلى هذا الأساس قسم المبحث الى مطلبين :-

المطلب الأول : ارتباط الأمن السيبراني بالأمن الاقليمي .

المطلب الثاني : تطور خصائص الهجمات السيبرانية .

المطلب الأول

ارتباط الأمن السيبراني بالأمن الإقليمي

فمفهوم الأمن السيبراني باعتباره مجموعة من العمليات التقنية الحديثة التي تحمي الشبكات وأجهزة الكمبيوتر والبيانات من الهجمات والأضرار والوصول غير المصرح به ، وفي ضوء التقنيات الحديثة ، عرف الأمن السيبراني بأنه مجموعة الاجراءات و الأدوات والاستراتيجيات والاطر القانونية و لأمنية و التنظيمية التي يتم وضعها من قبل الاجهزة الامنية للمحافظة على سرية المعلومات الالكترونية ، والأمن السيبراني يعد جهوداً مشتركة ما بين القطاع العام والخاص ، والجهود المحلية والدولية بهدف حماية الفضاء السيبراني والعمل على توفير انظمة معلومات رقمية تتميز بخصوصية عالية ، مقاومة للاختراقات الفيروسية وتتمتع سرية عالية من اجل تأمين التكنولوجيا من المخاطر والتهديدات لغرض حماية الفضاء الإلكتروني والتنظيم وموارد المستخدم[١].

عرفه الاتحاد الدولي للاتصالات بأنه: مجموعة من المهمات، مثل تجميع وسائل ، وسياسات ،

وإجراءات أمنية ، ومبادئ توجيهية ، ومقاربات لإدارة المخاطر ، وتدريبات ، و ممارسات ، وتقنيات ، يمكن استخدامها لحماية البيئة السيبرانية والمؤسسات والمستخدمين [٢]. فالأمن السيبراني هو عبارة عن التقنيات الالكترونية المستخدمة لحفظ سلامة الشبكات والبرامج والبيانات من الوصول غير المصرح به ، يعني مجموع القواعد التي يضعها مسؤولو الأمن في اي مكان والتي يجب ان يتقيد بها جميع الاشخاص الذين يمكنهم الوصول اليه فمفهوم الأمن مفهوم واسع يطال جميع عمليات الدخول والخروج والبقاء او التصرف في مكان ما وعليه يشمل الأمن في الفضاء السيبيري قواعد واصول ضبط الاتصال وانتقال المعلومات وتخزينها وحفظها كما يشمل أمن المواقع وامن الانظمة الالكترونية وعمليات استثمارها إضافة إلى امن الاتصالات [٣].

وإن الأمن السيبراني يهدف الى ضمان تحسين الأمن الذي من شأنه الدفاع عن المنظمات من التعرض لهجوم من قبل المتسللين عبر الشبكة العنكبوتية ، وهذا مرده إلى أن العالم أصبح أكثر ارتباطاً بواسطة الشبكات العنكبوتية لتنفيذ المعاملات العامة ويقوم الأمن السيبراني بالحفاظ عليها[٤].

لعب التسليح أهمية استراتيجية في توازن القوى على المستوى العالمي ، في ظل بيئة يسودها الشك وعدم اليقين وقابلية تدمير المصالح الاستراتيجية بسرعة الضوء ، وهو ما يحمل خطورة عسكرة الفضاء السيبراني ، وبتبني عديد الدول استراتيجية الحرب السيبرانية كحرب للمستقبل ، واعتبار أن النصر في المعركة حليف من يقدر على شل القوة والتشويش على المعلومة على الاعداء ، لقد بدأ سباق تسلح خطير لتطوير الأسلحة السيبرانية ، وعلى الرغم من صعوبة عملية الرقابة والتفتيش على الاسلحة السيبرانية ، فإن السعي نحو الحد من انتشار هذه الاسلحة ، يتطلب وجود اطار دولي تتشارك فيه العديد من الدول والجماعات عبر العالم ، إلى جانب وجود الاطار القانوني الدولي الذي يحدد الالتزامات والواجبات لجميع الفاعلين ، إن أي اتفاق من شأنه تنظيم الاستخدام العسكري للفضاء السيبراني ، و يجب أن يعمل على منع نشر الأسلحة السيبرانية في وقت السلم ، والسماح بالجهود الجماعية للدول أو المنظمات لتجنب التأثير على الاستخدام المدني للفضاء السيبراني[٥] .

إن الفضاء الإلكتروني قد فرض إعادة التفكير في مفهوم الأمن والذي يتعلق بتلك الدرجة التي تمكن الدولة من أن تصبح في مأمن من خطر التعرض الإرهابي، و المنشآت الحيوية للبنية التحتية للهجوم العسكري أو اجراءات الحماية ضد تعرض للأعمال العدائية من خلال

الاستخدام السيئ لتكنولوجيا الاتصال والمعلومات ، وأصبحت قضية امن الفضاء الإلكتروني تدخل في استراتيجيات الأمن القومي و الإقليمي للعديد من الدول من اجل الاستحواذ على مصادر القوة داخل الفضاء الإلكتروني ، للعمل على الحيلولة دون تعرض بنيتها التحتية الحيوية للخطر الذي ينجم جراء قطع خدمة الإنترنت أو ضرب مواقعها أو توقف رسائل البث الإذاعي أو التلفزيوني أو توقف موجات الراديو أو سقوط شبكات المحمول أو البث الفضائي ، وأصبح لها تأثير عميق على المجتمع والاقتصاد على النطاق الدولي [٦] . حيث بات ينظر للأمن السيبراني كرافد جديد للأمن القومي وجزء من الأمن الإقليمي ، بما أن العلاقة بين الأمن والتكنولوجيا علاقة متزايدة مع إمكانية تعرض المصالح الإستراتيجية ذات الطبيعة الإلكترونية إلى مخاطر إلكترونية ، الأمر الذي يهدد بتحول الفضاء الإلكتروني لوسيط ومصدر لأدوات جديدة للصراع الدولي المتعدد الأطراف ودورها في تغذية التوترات الدولية ، و ارتبط الأمن السيبراني بالأمن الإقليمي فلكما زادت الدولة تطوراً كلما قل احتمال تعرضها للتهديد [٧] . مع تصاعد مخاطر التهديدات السيبرانية على البنية التحتية للمعلومات وبما ان الأمن السيبراني يشمل كل أبعاد الدولة الاقتصادية ، السياسية ، الاجتماعية و العسكرية ، حيث أصبحت الدول تدخل ضمن حساباتها الإستراتيجية حماية أمنها السيبراني كما أن سيادة الدول تراجعت وذلك بتصاعد دور الفاعلين من غير الدول في العلاقات الدولية كالشركات التكنولوجية العابرة للحدود ، وشبكات الجريمة ، والقرصنة الإلكترونية ، والجماعات الإرهابية وهذا التراجع فرض تحديات عديدة للحفاظ على الأمن السيبراني العالمي ببروز اتجاهات عديدة لتحقيقه بين أصحاب المصلحة من الحكومات ، والمجتمع المدني ، والشركات التكنولوجية ووسائل الإعلام ، لذا أصبحت هناك مصالح وطنية إقليمية دولية للحفاظ على أمن الفضاء السيبراني على أساس أن الفضاء السيبراني صار جزءا من الأمن الإقليمي و العالمي وهو عرضة للطبيعة المتغيرة للتفاعلات السيبرانية خاصة مع تطور القدرات البشرية على إنتاج تقنيات جديدة [٨].

مع الثورة التكنولوجية التي شهدها العالم برز الفضاء الإلكتروني أو السيبراني (CyberSpace) كساحة للصراع العالمي ، ومع ظهور هذا الفضاء واجهت المفاهيم التقليدية ، مثل الصراع ، وأمن الدولة ، والقوة الكمية ، والسيادة ، تحديات واضحة ، خاصة من جهة تعاملها مع طبيعة التفاعلات في هذا الفضاء الافتراضي[٩].

اصبح الأمن السيبراني الهدف الأسمى للكثير من الدول لمقاومة التهديد والحماية من الاخطار والاضرار ، فبانت استراتيجيات الدول في مجال الأمن السيبراني من أهم أولويات الدول ، فالحروب السيبرانية بدأت تظهر تجلياتها بالدول الكبرى ، وأنهت الحروب التقليدية ذات النظريات الكلاسيكية والأسلحة الثقيلة واعلنت بداية حقبة جديدة من الحروب [١٠]. وتبدو العلاقة واضحة بين الأمن السيبراني والأمن الإقليمي لضمان حقوق الوصول الى البيانات والى مصادر النظام وذلك من خلال آلية التحقق من الهوية ورقابة حيث تسمح هذه بحصر مستخدمي النظام ضمن مجموعة من لأشخاص الذين اعطي لهم هذا الحق ، فالأمن في الفضاء السيبيري ليس الا مكونا من مكونات الأمن في المجتمع بشكل عام وهو كذلك الركيزة الأساسية لتحقيق الثقة في نمو وازدهار مجتمع المعلومات [١١].

يشمل الأمن السيبراني جميع المسائل الاقتصادية والاجتماعية والسياسية و الأنسانية ، على أنه قدرة الدولة على حماية مصالحها وشعبها ، في مختلف مجال حياته ومسيرته نحو التقدم بأمان ، من جهة ، ومن كونه يرتبط ارتباطا وثيقا بسلامة مصادر الثروة في العصر الحالي والمتمثلة في البيانات المعلومات والقدرة على الاتصال والتواصل ، وهي المحور الذي يتكون حوله الإنتاج والإبداع والقدرة على المنافسة من جهة ثانية [١٢].

ومع ثورة المعلومات ظهر شكل جديد من أشكال القوة وهي " القوة السيبرانية Cyber power " ، والتي بات تأثيرها واضحاً على المستوى المحلي والدولي ، فأدت هذه القوة الى الانتشار بين عدد كبير من الفاعلين مما جعل قدرة الدولة ضعيفة في السيطرة على هذه القوة ، فبات الأمن السيبراني الهدف الاسمى للكثير من الدول ، لمقاومة التهديد والحماية من الاخطار والاضرار ، فبانت استراتيجيات الدول في مجال الأمن السيبراني من اهم اولويات الدول ، فالحروب السيبرانية بدأت تظهر تجلياتها بالدول الكبرى ، وانهت الحروب التقليدية ذات النظريات الكلاسيكية والاسلحة الثقيلة واعلنت بداية حقبة جديدة من الحروب ، وبذلك دخل المجال الإلكتروني ضمن المحددات الجديدة للقوة وأبعادها الجديدة من حيث طبيعتها وأنماط استخدامها بل وأيضا طبيعة الفاعلين وهو ما كان له انعكاس على قدرات الدول وعلاقاتها الخارجية ، وهو ما أضفي خصائص جديدة للقوة [١٣].حيث بات صناع القرار في الولايات المتحدة الأمريكية والاتحاد الأوروبي وروسيا والصين والهند ، يصنفون الأمن السيبراني كأولوية في إستراتيجية سياستهم الدفاعية الوطنية ، وقد أعلنت أكثر من (١٣٠) دولة عن تخصيص

أقساما وسيناريوهات خاصة بالحروب والهجمات السيبرانية ضمن فرق الأمن الوطني ، فالدول اليوم تسعى إلى تطوير إستراتيجيتها للأمن السيبراني وحماية البنية التحتية للمعلومات الحساسة الخاصة بها ، وردع الجريمة السيبرانية عن طريق إنشاء تعاون وطني بين الحكومة ومجتمع صناعة الاتصالات والمعلومات ، بالإضافة إلى خلق قدرات وطنية لإدارة الحاسب الآلي [١٤].

كما تعتبر تركيا واحدة من الدول المستهدفة التي تتعرض للهجمات الالكترونية ، فعملت على تطوير نموذج الدفاع السيبراني الخاص بها ، فقد اعتمدت الحكومة التركية استراتيجية " الدفاع في العمق " او " الدفاع المتعمق " في مجال الأمن السيبراني و خلق طبقات متعددة لحماية انظمة المعلومات والبيانات من الاختراق والاستهداف ، واعتبرت تركيا ان هذه الاستراتيجية اكثر شمولاً وعملوا خبراء الأمن السيبراني على وضع استراتيجية شاملة للدفاع الالكتروني ، وفهم مناطق الضعف التي تتعرض للاختراق ، وتوفير هيكل اكثر ديناميكية ، وزيادة الوعي لدى الافراد واعتماد برامج التوعية الوطنية الشاملة وكذلك شملت الاستراتيجية في اعطاء التزامات من قبل مقدمي خدمة الانترنت حول مسؤولية انتهاكات المشتركين أكدت استراتيجية تركيا على عزل البني التحتية الحيوية وانشاء شبكة وطنية قائمة على تبادل المعلومات بين المؤسسات الحكومية مفصولة عن الانترنت [١٥].

دعا مجلس الأمن في ضوء الاعتراف بتحديات الأنشطة الخبيثة في الفضاء السيبراني جميع الدول للامتناع عن استخدام الفضاء الإلكتروني لأغراض عسكرية، وأعلن أنها "منطقة خالية من السلاح". كما اعتمدت الأمم المتحدة مجموعة من تدابير بناء الثقة الملزمة، بما في ذلك آلية التشاور الإلزامي، وذلك من أجل منع أي نزاع ينشأ عن استخدام تكنولوجيا المعلومات والاتصالات ، كما أنشأت هيئة لتسوية النزاعات في الفضاء السيبراني .[١٦]

ومن اجل الحفاظ على الأمن في المجال السيبراني وذلك نتيجة لعدم وجود أي أساس قانوني ينظم اللجوء إلى الحروب السيبرانية و نظرا لقصور القانون الدولي في هذا المجال ، حيث تم ابرام صك قانون ي عام ٢٠١٣ يدعى * دليل تالين " Tallin manual" [١٧] ، يحتوي دليل " تالين " على ٩٥ قاعدة ، وتتمثل تحدياته الرئيسية في ضمان توجيه الهجمات ضد الأهداف العسكرية فقط ، وتوخي الحذر لحقن دماء المدنيين والبنية التحتية الضرورية لحياتهم ، وهذا نتيجة وجود فضاء سيبراني واحد تتقاسمه القوات المسلحة والجيوش السيبرانية مع باقي المستخدمين المدنيين [١٨].

حيث أكد مبعوث الرئيس الروسي لشؤون التعاون الدولي في مجال أمن المعلومات " أندريه كروتسكيخ " على ضرورة توحيد الجهود المبذولة لمواجهة الهجمات الإلكترونية، معتبراً أنها " إرهاباً إلكتروني " مؤكداً على ضرورة بدء الحوار بين الخبراء الروس والأميركيين لوضع خطط مشتركة لمحاربتها، مشيرا إلى استعداد موسكو للحوار مع واشنطن في جميع القضايا العالمية التي تخص الهجمات الإلكترونية.

أما الصين فقد صرحت المتحدثة باسم وزارة الخارجية " هوا تشان بينغ " إن بلادها تحث المجتمع الدولي على العمل من أجل تعزيز مفهوم الأمن المشترك، وحماية السلام في الفضاء الإلكتروني ، ومنع ، التسلح الإلكتروني ، وضمان استخدام التقنيات السيبرانية لرخاء وتقدم البشرية ، وشكلت بداية الجهود التعاونية لمواجهة تهديد الحرب الإلكترونية ووضع معايير دولية للسلوك في الفضاء الإلكتروني تتمثل بما يلي [١٩].

اولاً: التشريعات و الاتفاقيات الوطنية و الإقليمية الخاصة بالأمن السيبراني .

ثانيا: سن العديد من دول العالم قوانين لمواجهة التهديدات السيبرانية ، بعد أن ظهر جليا مدى سرعة انتشارها وفداحة الخسائر الناتجة عنها ، وأجمع أغلب هذه القوانين أن هذه التهديدات ما هي إلا تعدي على الآخرين وعلى الممتلكات العامة والأنظمة بواسطة استخدام التقنية ، وخصص جزء كبير من هذه القوانين عقوبات رادعة [٢٠] .حيث تم تشكيل هيئات وطنية للأمن السيبراني سعت الدول إلى تشكيل هيئات متخصصة في الأمن السيبراني بما أن التهديدات السيبرانية لا تفرق بين مدني وعسكري، حيث تكون مهمتها هي، وضع أطر الاستجابة للحوادث والاختراقات ، وضع السياسات والمعايير الوطنية للتشفير ، إعداد الإستراتيجية الوطنية للأمن السيبراني والإشراف على تنفيذها ، و وضع السياسات وآليات الحوكمة والإرشادات المتعلقة بالأمن السيبراني وتعميمه ، وكذلك وضع أطر إدارة المخاطر المتعلقة بالأمن السيبراني ، رفع مستوى الوعي بالأمن السيبراني ، كما يحدد الإتحاد الدولي للاتصالات (ITU) خمسة معايير لتصنيف مستوى الأمن السيبراني للدول وهي معاير تشريعية ، تقنية ، تنظيمية ، بناء القدرات ، ومعيار التعاون [٢١].

لاتفاقيات الإقليمية والدولية التي تنسجم مع متطلبات مواكبة سرعة تطور التهديدات السيبرانية للأمن في الفضاء السيبراني ، ويسجل في هذا المجال عدد من المبادرات نذكر منها[٢٢]:

- ❖ وضعت مجموعة بلدان الكومنولث في عام ٢٠٠٢، قانوناً نموذجياً لمكافحة الجريمة السيبرانية ، إضافة إلى قانون الإثبات الرقمي .

❖ بادرت المجموعة الاقتصادية لغرب إفريقيا في عام ٢٠٠٩، إلى إقرار توصية لمكافحة الجريمة السيبرانية ، تشكل الإطار القانوني لعمل الدول الأعضاء .

❖ الاتفاقية العربية التي جاءت لمكافحة جرائم تقنية المعلومات عام ٢٠١١، من اجل لتعزيز التعاون بين الدول العربية لمكافحة الجرائم السيبرانية والحفاظ على أمنها وسلامة مجتمعاتها.

❖ وان اتفاقية بودابست ٢٠٠١ (الاتفاقية الأوروبية لمكافحة الجريمة السيبرانية) ، تعتبر خطوة رائدة على مستوى التعاون بين الدول ، وهي الوحيدة من حيث المدى وحجم الدول المنضمة إليها ، دخلت حيز التنفيذ عام ٢٠٠٤ ، وتعتبر أداة إقليمية ملزمة لمكافحة الجريمة السيبرانية ، عبر تحقيق الانسجام بين القوانين الوطنية ، وقد شددت على ضرورة تحسين تقنيات التحقيق والبحث ، وزيادة التعاون بين الدول ،إن التحولات العالمية اليوم جعلت من الدول تواجه هاجسا من مواجهتها لوحدها لما يمكن أن يهدد أمنها ، مما دفعها للتوجه نحو بناء التكتلات الإقليمية سواء من خلال أطر مؤسسية كالمنظمات عبر الوطنية في مجالات مختلفة ، أو من خلال إقامة علاقات تعاونية من اتفاقيات ومبادرات أمنية أو شراكة أو بالاعتماد المتبادل الذي جسدته حركة الاندماجيات بين الشركات الكبرى التابعة لمختلف الدول إذ أصبحت تتنافس في جميع فروع النشاط الاقتصادي في الدواء ، الطيران ، السياحة ، القطاع المصرفي .

المطلب الثاني

تطور خصائص الهجمات السيبرانية

شهد العالم المعاصر منذ مطلع القرن الحالي سباقاً بين مختلف القوى الكبرى والاقليمية لاستغلال الفضاء السيبراني والاستفادة من المزايا الكبيرة التي يوفرها في تحقيق مكاسب استراتيجية حيوية لم تكن تحلم تلك القوى بتحقيقها عن طريق استخدام القوة العسكرية التقليدية. لقد اصبحت قضية "الهجمات السيبرانية" واحدة من اهم واعقد القضايا التي تثير قلق الدول الكبرى المتقدمة تكنلوجياً قبل غيرها من دول العالم الاخرى الاقل تقدماً، وذلك لما تسببه من اثار وانعكاسات خطيرة تهدد امنها القومي ومصالحها العليا، في عصر تزايدت فيه الهجمات عبر الإنترنت، وتصاعدت النشاطات الإرهابية التي تتعدى اثارها جهات رسمية وغير رسمية واوقعت خسائر كبيرة وسببت انقسامات سياسية ومشاكل داخلية خطيرة للدول المستهدفة.

تتطور شكل الهجمات السيبرانية بصورة سريعة، فقد يكون مرة عبر أجهزة الحاسب، ومرة عبر إنترنت، ومرة عبر أجهزة الهواتف المحمولة، وقد يكون عبر نظم الذكاء الاصطناعي والروبوت،

بحيث يستهدف في أحدها الأموال، المواقع الحكومية، وفي غيرها العنف غير المبرر.

و يسجل لنا التاريخ المعاصر نماذج للهجمات السيبرانية ، ومنها الهجوم السيبراني الذي نفذته الولايات المتحدة الأمريكية ما صرحت به عام ١٩٨٢ ضد منظومة التحكم العالية صناعيا في أنبوب نفط (Chelyabinsk) التابع للاتحاد السوفياتي ، وهو ما نفاه الاتحاد السوفياتي آنذاك ، أما النموذج الآخر ، فهو ما تعرضت له أنظمة الاتصال الإلكترونية التابعة لوزارة الدفاع الأمريكي (Pentagon) ، ووكالة الفضاء الأمريكية (NASA) ، ووكالة الطاقة الأمريكية(Energy Department) ، من هجمات سيبرانية بين العامين ١٩٩٨ – ٢٠٠٠ ، والذي أدى إلى الاستحواذ على الآلاف من الملفات المصنفة بأنها عالية السرية ، وقد وجهت الولايات المتحدة التهمة رسميا إلى روسيا الاتحادية ، في حين أنكرت الأخيرة آنذاك مسؤوليتها عن هذا الهجوم[٢٣].

كذلك أدت الحرب الأهلية في سورية إلى نشاط هجومي مكثف قامت به منظمة تعرف باسم الجيش الإلكتروني السوري وهي مجموعة إنترنت تألف من قراصنة إنترنت يدعمون نظام "الأسد" وهم يهاجمون جماعات المعارضة السورية باستخدام تقنيات حجب الخدمات والمعلومات ، أو اقتحام مواقع إنترنت و تغير محتواها وقد نجحت المجموعة في القيام بعدة عمليات خبيثة ضد مواقع المعارضة السورية ، و أيضا ضد مواقع الإنترنت الغربية وكان آخر عمل للجيش السوري الإلكتروني يستهدف أساسا وسائل الإعلام ، والمواقع الثقافية والإخبارية على الشبكات الغربية وقد نجحت المجموعة في اقتحام أكثر من ١٢٠ موقعا [٢٤]. وإحدى الهجمات الأكثر أهمية وفعالية كانت في نيسان ٢٠١٣، عندما اقتحم الجيش الإلكتروني السوري حساب تويتر لوكالة أنباء "الأسوشيتد برس " ووضع "تغريدة " زائفة نقول إن البيت الأبيض قد قصف وأصيب الرئيس الأميركي بجروح في الهجوم. وكانت النتيجة المباشرة لهذا الإعلان هبوط حادة في الأسواق المالية الأميركية، وفي مؤشر داو جونز الصناعي لعدة دقائق [٢٥].

و الهجمات السيبرانية التي قامت بها باكستان ضد الهند ، واستهدفت " مركز الهبة للبحوث الذرية " في حزيران ١٩٩٨ ، و الهجوم الذي شن على المكسيك في تشرين الأول لعام ١٩٩٨ ، واستهدف مواقع الرئيس المكسيكي ، و الهجوم السيبراني على المانيا في ١٩٩٩ استهدف الشركات الاقتصادية لتعطيل المراكز المالية ، احتجاجاً على اجتماع قمة مجموعة الثمان "G8" ، الهجمات السيبرانية بين الصين وتايوان في عام ١٩٩٩ وقد أدى هذا النزاع السيبراني بينهما الى اختراق مواقع تايوانية ،

هجوم سيبراني عام ١٩٩٩ من قبل قراصنة صربيون في حرب كوسوفو من خلال استهداف سلاح الجو التابع لحلف شمال الاطلسي NATO () ، الحرب السيبرانية بين اسرائيل وفلسطين عام ٢٠٠٠ ، الحرب السيبرانية بين الصين واليابان في عام ٢٠٠١ واستهداف مواقع وخدمات الانترنت في اليابان ، و الحرب السيبرانية بين الصين والولايات المتحدة عام ٢٠٠١ والتي بدأت بعد تحطم طائرة التجسس الامريكية حيث تم استهداف الولايات المتحدة من قبل الصين ، الاختراق الذي حدث على وكالة ناسا الفضائية عام ٢٠٠٣ والذي اطلق عليها اسم " تيتان المطر " ، الحروب السيبرانية بين كوريا واليابان عام ٢٠٠٥ م ، بسبب الصراع الاقليمي حول " دو كدو " وهو الخلاف بين كوريا الجنوبية واليابان ، الحرب السيبرانية التي نشبت بين ماليزيا وإندونيسيا عام ٢٠٠٥ م ، حول قضية " امبالات " حيث تم استهداف المواقع العسكرية الحكومية الماليزية واختراقها[٢٦].

شنت اسرائيل في ١ / ايلول / ٢٠٠٧ هجوم السيبراني على سوريا عبر الانترنت، على انظمة الدفاع الجوية السورية، ومن ثم قصف محطة نووية مشتبه بها قيد الانشاء في سوريا، وتمكن الاسرائيليون من تنفيذ الهجوم واطلق اسم (عملية البستان Orchard)، حيث تم اختراق نظام رادار الدفاع الجوي السوري ، عن طريق برنامج حاسوبي يسمى سوتر (Suter) ، ولم يعطل " Suter " الرادار وانما عرقل وصول البيانات [٢٧].

حيث تعرضت استونيا التي تقع في أوروبا الشرقية، بعد خلافها مع روسيا الى اعنف الهجمات السيبرانية في عام ٢٠٠٧، اثر مشروع نقل نصب تذكاري يعود الى العهد السوفيتي، حيث تعرضت الى هجوم هدد الأمن القومي للدولة بأكملها [٢٨]، استمر الهجوم ثلاثة أسابيع ، شلت خلاله تكنولوجيا المعلومات والبنية التحتية في البلاد ، فقد استهدفت شبكات الاتصال ، وانظمة البنوك والمصارف والصحف والهواتف المحمولة.

الهجوم السيبراني عام ٢٠٠٨ الذي شن ضد جورجيا، بعد الصراع الذي نشب بين روسيا وجورجيا على أوسيتيا الجنوبية ، فالاختراق السيبراني أدى الى توقف خدمة الانترنت في جورجيا ، وتوقف الاتصالات الداخلية ، واتهمت جورجيا روسيا وراء هذه الهجمات [٢٩] .

وتم اختراق عام (٢٠٠٩) مواقع الكترونية ذات اهمية عالية ، من قبل المسلحين في العراق ، حيث كانت تستقبل هذه المواقع بيانات مهمة وتنقلها الى الطائرات بدون طيار لتحديد تحركات الجماعات المسلحة وأدى الاختراق الى مراقبة

التحركات العسكرية الامريكية الموجهة ضدهم [٣٠].

ففي عام (٢٠٠٩- ٢٠١٠) استهدفت إيران بواسطة فايروس الإلكتروني المعروف" Stuxnet " دودة إلكترونية ، مصممة خصيصا لتخريب المفاعلات النووية الإيرانية .

وفي عام ٢٠١٢ ، تم تدمير ٣٥ ألف جهاز كمبيوتر في شركة النفط السعودية " أرامكو " ، لتخريب صادرات النفط ، وألقت المخابرات الأمريكية اللوم على إيران ، حيث عطلت نشاط الشركة لمدة شهر في ما يشار إليه بأكبر اختراق في التاريخ [٣١].

أنه رغم اختلاف غرض وهدف كل حالة من الحالات السابقة ، إلا أنه من الواضح أن حجم الهجمات الالكترونية يتزايد بشكل حاد ، ولذا يصعب تحديد حجمها الحقيقي وبخاصة أن عديد منها لا يتم التبليغ عنه ، وتتمثل القواسم المشتركة بين تلك الحالات في صعوبة تحديد مرتكبي تلك الهجمات على وجه الدقة ، وغياب الرد المضاد ، كنتيجة لها ، والأهم أنها ليست حكراً على الدول المتقدمة ذات أنظمة المعلومات الهائلة والمتطورة فحسب ، مع انتشار الفضاء الإلكتروني ، وسهولة الدخول إليه ، اتسعت دائرة الصراعات السيبرانية ، وزاد عدد المهاجمين ، صار الصراع بين الفاعلين المختلفين حول امتلاك أدوات الحماية والدفاع ، لتعبر عن الصراع الممتد ، ولذلك في تطوير القدرات الهجومية الإلكترونية يستهدف حيازة القوة والتفوق والهيمنة وتعزيز التنافس حول السيطرة والابتكار والتحكم في المعلومات وتعظيم القدرات القادرة على زيادة النفوذ والتأثير في المستويين الاقليمي والدولي [٣٢].

وهناك امثلة كثيرة على هجمات تعرضت لها منشآت وقطاعات حكومية وغير حكومية ، ومنها في عام ٢٠١٣ استهداف بنوك الإمارات العربية المتحدة وسلطنة عمان حيث بلغت الخسارة أكثر من ٤٥ مليون دولار أمريكي بسبب عملية تعتبر واحدة من أكبر عمليات سرقة أجهزة الصراف الآلي الإلكترونية في المنطقة لهجمات السيبرانية لتنظيم الدولة الاسلامية " داعش الارهابي " .

و مع داعش عام ٢٠١٤ ، اتجه هذا التنظيم الى توظيف أدوات الفضاء الالكتروني ، من خلال استخدام المنصات الرقمية في الانترنت المظلم واستخدامه في جمع الاموال ، وشراء الاسلحة عبر الاسواق الالكترونية ، وتداول الكتب المتطرفة . استخدام الاعلام والمنصات الرقمية لنشر الافكار ، وإنشاء مقاطع الفيديو لمدة ١٣ دقيقة . وباللغة الانكليزية تحت عنوان " لا حياة بلا جهاد " والذي يضم شهادات لمقاتلين من استراليا بريطانيا ، وهو نوع من جذب الشباب في الولايات المتحدة الأمريكية و

أوربا ، والتشجيع على تجنيد النساء ايضاً ، واعلن التنظيم ايضاً مسؤولية عن اسقاط الطائرة الروسية في سيناء مصر في العام ذاته [٣٣].

وادى استخدام الهوية الطائفية إلى زيادة الصراع حول مكانة وحجم وحدود كل مكون أو طائفة وهذا ما سبب عدم الاستقرار وزيادة العنف ، وأصبحت كل جهة تحاول أن تضفي المشروعية على وجودها وأعمالها ، من خلال ممارسة العنف والقتال بدواعي الدفاع عن هويتها ووجودها[٣٤].

وفي شباط ٢٠١٦ تعرض النظام المصرفي الدولي للقرصنة في محاولة لسرقة مبلغ ٩٥١ مليون دولار من البنك المركزي في بنغلاديش ، فقد اعطى المهاجم خلال هذه العملية تعليمات زائفة بسحب أموال من حساب البنك المركزي في بنغلاديش لدى البنك الاحتياطي الفيدرالي في نيويورك باستخدام شبكة سويفت المصرفية لاستكمال التحويل ، ونجحت عملية القرصنة بسحب مبلغ ١٠٠ مليون دولار قبل أن يوقفها البنك الاحتياطي الفيدرالي في نيويورك [٣٥] .

وفي العام ٢٠٢٠ ، أعلنت إسرائيل عن هجوم سيبراني استهدف شبكات المياه الخاصة بها واتهم الإسرائيليون ايران بالمسؤولية عن الهجوم ، في حين أن إسرائيل والولايات المتحدة الأمريكية قد أطلقتا أكثر من فيروس لاستهداف المنشأة النووية الإيرانية ، وآخرها ما وقع في شباط وأيار وتموز من العام ٢٠٢٠ ، بحيث أقر وزير الأمن الإيراني (محمود علوي) بأن هناك أكثر من مليوني هجوم سيبراني وقع بين عامي ٢٠١٩ و ٢٠٢٠ ، وبحسب وزير الأمن ، فإن إسرائيل وأمريكا والسعودية مصدرها ، علما أن الأخيرة تعمل على تدريب ٥٠٠٠ عنصر في البانيا لهذا الغرض [٣٦] .

ونتيجة لذلك تستطيع الدول أن تحقق اهدافها باستخدام الاسلحة الالكترونية بدلا من القوى العسكرية دون الحاجة الى تحمل اية مسؤولية دولية تترتب على هذا الهجوم ، ودون قدرة الهدف على اثبات قيامها به .يمكن القول ، إن الجيل الحالي من الهجمات السيبرانية يتميز بخصائص أكثر تعقيداً وعنفاً عما سبقه والتي منها [٣٧]:

أ- سرعة تطور شكل الهجمات السيبرانية : حيث ان في هذا الجيل تتطور الهجمات السيبرانية بشكل سريع، فقد يكون مرة عبر أجهزة الحاسب ومرة عبر إنترنت ومرة عبر أجهزة الهواتف المحمولة ، ومستقبلاً قد يكون عبر نظم الذكاء الاصطناعي والروبوت ، يستهدف في أحدها الأموال ، وفي أخرى الاعتراض السياسي أو الإرهاب ، وفي غيرها العنف غير المبرر .

ب- ضيق الفجوة الزمنية بين الهجمات الكبرى : حيث يكون الفارق الزمني بين هجمة سيبرانية وغيرها قصيراً جداً ، فنشهد عدة

هجمات كبرى خلال عام واحد ، فمما يكاد العالم يخرج من تداعيات هجمة حتى تظهر له غيرها ، مختلفة في الآلية والنطاق والجمهور .

ت- دور بارز للفواعل من غير الدول : يلعب الفواعل من دون الدول دور هام ، قد يكون مساوياً لدور الدول ، سواء كانت مجموعة قرصنة أو حركات إرهابية أو مافيا دولية ، أو حتى أفرادا عاديين ، كما يتم تطوير العديد من برامج القرصنة التي لا تحتاج إلى مطورين ومختصين لاستخدامها ، بل يمكن شراؤها واستخدامها بصورة سهلة ، وهو ما يفتح الباب لقطاع كبير من غير المختصين للمشاركة في هذا النوع من الهجمات الاستعداد القيادة المعارك العسكرية .

ث- عدم القدرة على كشف الجناة : حيث يصعب تحديد موقع و شخصية القائم بالهجمات السيبرانية ذات التأثير العالي ، لكونها لا تترك اثر او دليل على حصولها ، عندما يكون من المستحيل اثبات الجاني علناً يكون من السهل على المشتبه ان ينكر ، ففي اعقاب النفي المتكرر للانخراط في خروقات الانتخابات الأمريكية لعام ٢٠١٦ صرح "فلاديمير بوتين" في النهاية انه من الممكن ان يكونوا قراصنة روسيين لكن اوكد انه ليس له علاقة بالحكومة الروسية وهذا يفسر (انت تعلم اننا فعلناها لكنك لا تسطيع اثبات ذلك وهذا هو الانكار) .

ج- التكلفة المتدنية نسبياً للهجمات السيبرانية : فهي هجمات تقنية متطورة ، تعكس قمة التطور الذي وصلت اليه ثورة المعلومات ، فهي لا تحتاج الدول إلى تخصيص ميزانيات ضخمة لإنتاج أسلحتها السيبرانية على خلاف الأسلحة المستخدمة في النزاعات العنيفة التقليدية ذات الكلفة العالية جدا كحاملات الطائرات والمقاتلات المتطورة ، لأن هذه الهجمات تتميز بالسرعة والمرونة[٣٨].

ح- ضعف السيطرة الحكومية و الحرية النسبية : إذ إن طبيعة المجال العام السيبراني يصعب على الحكومات السيطرة عليه ، ولذا ، يستطيع الأفراد والجماعات التعبير عن مواقفها وآرائهم في أي وقت ، أي مكان ، بما يشكل دافع أكبر لهم للمشاركة في النقاش والتفاعل حول ومن القضايا العامة ن والقدرة على بناء روابط افتراضية حيث تتيح الأدوات السيبرانية للأفراد ، والجماعات قدرة أكبر على التواصل والتشبيك وبناء مجتمعات افتراضية بأشكال مختلفة للتأثير في القضايا عبر وسائل التواصل الاجتماعي والمنتديات الإلكترونية وغيرها ، و ذلك الامر قد لا يتوافر في المجال العام التقليدي ، لاسيما مع القيود التي تفرضها الانظمة السلطوية على عملية التنظيم التي قد يقدم عليها الأفراد والجماعات [٣٩].

خ- الفضاء الإلكتروني لا حدود له : حيث لا تعرف الهجمات السيبرانية الحدود الجغرافية فهي متنوعه و متطورة بوسائلها بأكثر المجالات تطوراً ، يتشارك كل الفاعلين بما فيهم الدول من الاستخدام الشخصي إلى البرامج الاقتصادية إلى التطبيقات العسكرية ، كلها تعتمد على الفضاء الإلكتروني . وعلى العكس من التهديدات التقليدية الملموسة والممكن التنبؤ بها ، فإن تهديدات الفضاء الإلكتروني يمكن أن تأخذ شكل و مصدر افتراضي و تفرض أخطاراً لا يمكن التنبؤ بها ، و اضمحلال حدود الداخل والخارج أي اصحب هناك حالة من التأثير الشبكي المتزايد بين الدولة وخارجها[٤٠].

الخاتمة

إن الثورة التكنلوجية والمعلوماتية قد أوصلتنا إلى نتيجة مفادها أن أشكال التهديدات قد تتغير وذلك بظهور ما يعرف بالفضاء السيبراني الذي يعد بمثابة الميدان يتنافس عليه الدول من اجل زيادة قوتهم الالكترونية لاسيما في ظل اعتماد الدول بشكل تام على التكنلوجيا والمعلومات وربط أمنها القومي و الإقليمي بالفضاء السيبراني ، حيث خلقت هذه التطورات التقنية والتكنولوجية الحديثة العديد من التهديدات الأمنية والمعلوماتية، خاصةً على مستوى الأمن الاقليمي، والذي أصبح أكثر عرضةً للخطر نظراً لسهولة الانكشاف المعلوماتي الذ ي وفرته وسائل الاتصال والتواصل الحديثة، وانتشار مختلف أنواع المعلومات بزخم كبير على شبكات الإنترنيت، تحولت أدوات الإنترنت ، ووسائل الاتصال الحديثة، وصفحات المواقع الاجتماعية إلى أسلحة إلكترونية جندتها العديد من الدول لتخوض غمار حروبها الرقمية والمعلوماتية ، وان البيئة السيبرانية قد اثرت في تطور خصائص الهجمات و من جانب آخر عملت على زيادة الاعتماد على تكنلوجيا التقنيات الحديثة و ذلك بسبب سهولة تدفق المعلومات وأهمية البيانات التي تقدمها ، وقد أدى هذا الى ظهور تحديات عدة على المستوى الإقليمي منها عدم القدرة على الحفاظ على سلامة البنية التحتية المعلوماتية و المواقع والانظمة والبيانات الرقمية من خطر التجسس او تعديل المعلومات أو أتلافها .حيث اصبح ضرورياً على الدول امتلاك مصادر التكنلوجيا الحديثة لتستطيع امتلاك القوة الالكترونية والحفاظ على امنها السيبراني.

الاستنتاجات:

١) أن السيبرانية تعد مجالا أخرا لاستعراض القدرات الالكترونية ، وممارسة النفوذ وتحقيق التفوق والتنافس الاقليمي فان المواءمة بين

النمطين من ترسانات الأسلحة التقليدية وأسلحة السيبرانية التي تعد المعيار الاساسي لقياس القوة فضلاً عن الثورة التكنولوجية التي وفرت تكنولوجيا المعلومات والاتصال اسلحة من نوع جديد تفضي إلى احراز النصر وكسب المعركة متجاوزة الفواعل بذلك الحدود الجغرافية والتقليل من الخسائر المادية والبشرية.

٢) عملت الدول الإقليمية استراتيجية موحدة ومحكمة لمواجهة خطر الإرهاب من خلال حملات الدعاية ضد الفكر المتطرف مع التركيز على استراتيجية العمل بالضد من الأفكار الإرهابية و اصدار التشريعات القانونية بما يتناسب وحجم العمل الجرمي نتيجة النشاطات الإرهابية في الفضاء السيبراني والعمل على ملاحقة مرتكبي الجرائم السيبرانية عبر أجهزة الامن وكذلك انشاء فرق طوارئ للاستجابة للمخاطر والتهديدات السيبرانية .

٣) هناك ارتباط بين امن المعلومات و الامن الإقليمي باعتبار ان المعلومات هي ركيزة أساسية للأمن الإقليمي لأن هذه المعلومات جزء من السياسة الأمنية للدول واي اختراق قد يحدث يتسبب بتهديد وتوجيه هجمات تخترق البنية التحتية للدول ويخلق حالة من الاستقرار.

٤) يعد غياب الحدود المكانية والزمانية أحد السمات المميزة للفضاء الإلكتروني مقارنة بالمساحات التقليدية . فلن تتمكن أي دولة من تحديد دائرة أو محيط التهديد الخاصة بها في الفضاء الإلكتروني على عكس المساحات التقليدية التي يشكل القرب أو البعد الجغرافي عاملا رئيسيا في تحديد مصادر التهديدات فيها . وهو ما يعني انتفاء " القومية " فالتهديدات الإلكترونية " عالمية بطبيعتها ، أي عابرة للحدود ، ومن ثم لا يكون المكون الجغرافي حاضرا في رؤية الدولة لبيئة التهديد المحيطة بها ، فقد يأتي الهجوم من أي مكان في العالم ولا توجد أولوية للمخاطر الأمنية الإلكترونية الإقليمية عن تلك العالمية .

المصادر :

(١) علي زياد علي، الصراع والأمن الجيوسيراني في السياسة الدولية : دراسة في استراتيجيات الاشتباك الرقمي ، دار المجد للنشر والتوزيع ، عمان ، ٢٠١٩ ، ص ٥٧ .

(٢)الاتحاد الدولي للاتصالات ، تقرير عن تنفيذ خطة عمل الدوحة (DAP) : البرامج ولجان الدراسات والأنشطة والمبادرات في المنطقة العربية، مكتب تنمية الاتصالات ،دمشق، ٢٠١٠ ، ص ٩ .

(٣)منى الأشقر جبور ، السيبرانية هاجس العصر المركز العربي للبحوث القانونية والقضائية، بيروت ،٢٠١٣، ص ٢٥ .

(4) Darko Galinec,Darko Mozinkand Boris Guberina ,Cybersecurity And Cyber Defence: National Level Strategic Approach, Journal For Control, Measurement, Electronics, Computing And Communications,Volume 58, Issue 3, England,2017 ,P275.

٥ عادل عبد الصادق ، أسلحة الفضاء الالكتروني في ضوء القانون الدولي الانساني ، مكتبة الإسكندرية ، ط٢ ، المركز العربي لأبحاث القاهرة ، ٢٠١٦ ، ص ٦٤ .

(6) Tim Jordan , Cyber power :The culture and politics of cyberspace and the Internet, Routledge,London,1999,p160-163.

(٧)نورة شلوش ، القرصنة لإلكترونية في الفضاء السيبراني التهديد المتصاعد من الدول ، مجلة مركز بابل للدراسات الإنسانية ، المجلد (٨) ، العدد (٢) ،٢٠١٨ ، ص ص ١٧٩-١٨٢ .

٨ايهاب خليفة ، القوة الإلكترونية كيف يمكن للدول ان تدير شؤنها في عصر الانترنيت ، مطبعة العربي ، القاهرة ،٢٠١٧ ، ص٢٣ .

(9)Arsenio Gumhad ،Cyber Troops And Net War : The Profession Of Arms In The Information Age ،War College Series , New York ,2015,p55-57.

١٠ الامن السيبراني : المفاهيم الإدارية ، موقع هارفارد بزنس ريفيو ، تاريخ الزيارة ٢٠٢٢/٣/٥،متاح على الرابط :https://hbrarabic.com/ .

(١١) حمزاوي ميلود ، الامن الالكتروني ، قسم العلوم السياسية والعلاقات الدولية ، كلية الحقوق ، جامعة الحاج لخضر باتنة ، الجزائر ، ٢٠١٤ ، ص ٦ .

(١٢) منى الأشقر جبور ، السيبرانية هاجس العصر ، مصدر سبق ذكره ، ص ٢٨ .

(١٣) جوزيف ناي، المنازعات الدولية ، ترجمة احمد امين ومجدي كامل، القاهرة، مصر، ١٩٩٧ ،ص٨٢.

(١٤) علي زياد علي، ، الصراع والأمن الجيوسيراني في السياسة الدولية : دراسة في استراتيجيات الاشتباك الرقمي ، دار المجد للنشر والتوزيع ، عمان ، ٢٠١٩ ، ص ٥٧ .

15 Kerim Goztepe and Recep Kilic ,Cyber Defense In Depth: Designing Cyber Security Agency Organization For Turkey,Journal Of Naval Science And Engineering 2014, Vol.10, No.1,Security Agency Organization, Turkey,2014. P.P. 8-11.

(١٦) باتريك باولاك بروسيلس وناثالي فان ريمدونك ، ماذا لو قادت " الشمس " إلى حروب . سيبرانية ؟، عرض صباح عبدالصبور ،(٢٠١٩) ، المستقبل للأبحاث والدراسات المتقدمة : تاريخ الزيارة ٢٠٢٢/٣/١٠ ، متاح على الرابط : . https://goo.gl/cLPBbU

١٧ سعيد درويش ، " ماهية الحرب الالكترونية في ضوء قواعد القانون الدولي " ،مجلة حوليات، العدد ٢٩ ، كلية الحقوق ،جامعة الجزائر، الجزائر ، ص ١١٩ .

١٨ اللجنة الدولية للصليب الأحمر ، ما هي القيود التي يفرضها قانون الحرب على الهجمات السيبرانية " ، تاريخ الزيارة ٢٠٢٢/٣/١٢ ، متاح على الرابط : https://www.icrc.org/ar/doc/resources/documents/faq/130628-cyber-warfare-q-and-a-eng.htm .

(١٩) علاء الدين فرحات ، من الردع النووي الى الردع السيبراني : دراسة لمدى تحقيق مبدأ الردع في الفضاء السيبراني ، مجلة المفكر ، كلية الحقوق والعلوم السياسية ، جامعة محمد خضير بسكرة ، قسم العلوم السياسية ، مجلد (١٦) ، العدد (١) ، ٢٠٢١ ، ص ٢٧٩ .

٢٠ حسن بن أحمد الشهري ، " الإرهاب الالكتروني - حرب الشبكات- " ، المجلة العربية الدولية للمعلوماتية ، ٢٠١٥ ، ص ١٩ .

٢١ مؤشر الأمن السيبراني العالمي ، الاتحاد الدولي للاتصالات ، ٢٠١٧ ، ص ١٧ ،تاريخ الزيارة ٢٠٢٢/٣/٢٠ ، متاح على الرابط : https://www.itu.int/pub/D-STR-GCI.01-2017

٢٢ منى الأشقر جبور ، السيبرانية هاجس العصر ، مصدر سبق ذكره ، ص ١٠٣-١٠٤ .

(23)Diego Rafael Canabarro And Thiago Borne , " Reflection On The Fog Of Cyber War " , National Center For Digital Government , Policy Working ,University Of Massachusetts Amherst ,Umass, March 1 , 2013, P.10.

24 Dylan Love , 10 Reasons To Worry About The Syrian Electronic Army , Insider , Date Of Visit 25/3/2022, At The Link: https://www.businessinsider.com/syrian-electronic-army-2013-5 .

25) Peter Foster , « ' Bogus ' AP tweet about explosion at the White House wipes billions off yoz US markets , Date of visit 30/3/2022, At the link: https://www.telegraph.co.uk/finance/markets/10013768/Bogus-AP-tweet-about-explosion-at-the-White-House-wipes-billions-off-US-markets.html .

(26) Robin Gandhi , Dimensions Of Cyber-Attacks: Cultural, Social, Economic, And Political , Issue Number1, Journa Lieee Technology And Society Magazine, New York,2011 . P 32-33.

(٢٧) فرد كابلان ، المنطقة المعتمة التاريخ السري الحرب السيبرانية ، ترجمة لؤي عبد المجيد ، عالم المعرفة المجلس الوطني للثقافة والفنون والآداب، الكويت ، ٢٠١٩ ، ص١٩٢-١٩٧ .

(28) Bidelmun , Scottw , difining and deterring Cyber war fare , strategy Research project , USA , 2000 , p 39.

(٢٩) ايريك هوسلي، روسيا جورجيا: ماذا تخفي معركة القوقاز، مجلة الانساني ،العدد (٤٤)،اللجنة الدولية للصليب الأحمر، القاهرة، ٢٠٠٨ ، ص٥ .

٣٠ احمد عيسى نعمة الفتلاوي ، الهجمات السيبرانية ،دراسة قانونية تحليلية ، بشان تحديات تنظيمها المعاصر ،منشورات زين الحقوقية ، بيروت ،٢٠١٨، ص ٢٠ .

(٣١) عبد الرحمن عاطف أبو زيد ، الأمن السيبراني في الوطن العربي .. دراسة حالة المملكة العربية السعودية المركز العربي للبحوث والدراسات ، ٢٠١٩ ، تاريخ الزيارة ٢٠٢٢/٣/٢٠ ، متاح على الرابط :

http://www.acrseg.org/list.aspx?r=24734

32Paulo Shakarian et al ,Introduction To Cyber Warfare A Multidisciplinary Approach , Syngress, New York , 2013,p68.

(٣٣) عبد الفتاح ، فاطمة الزهراء ، تطور توظيف جماعات العنف لـ الارهاب السيبراني ، مجلة السياسة الدولية المجلد (٥٢) ، العدد (٢٠٨)، ، القاهرة ، ٢٠١٧ ، ص ٢٦ .