الأمن السيبراني وتحديات الجوسسة والاختراقات الإلكترونية للدول عبر الفضاء السيبراني

Cyber security and the challenges of espionage and penetration of countries through cyberspace

شريفة كلاع

جامعة الجزائر 3 (الجزائر)، cherifaklaa@gmail.com

تاريخ الاستلام: 2021/08/08 تاريخ القبول:2022/03/04 تاريخ النشر: 2022/04/27

ملخص:

سيتم في هذه الدراسة التركيز على موضوع الأمن السيبراني وتحديات الجوسسة والاختراقات الإلكترونية للدول عبر الفضاء السيبراني، حيث تهدف إلى تبيان مختلف التحديات والتهديدات السيبرانية التي تهدد أمن الدول، ومدى أهمية الدفاع والردع الإلكتروني لتحقيق الأمن السيبراني الوطني في ظل التحديات الراهنة، وتشير نتائج هذه الدراسة إلى أن من يمتلك القوة السيبرانية والتكنولوجيا المتقدمة ويتفرد بها سيحقق السيطرة في الفضاء السيبراني ويحقق الأمن السيبراني الذي يُدعِّم السيادة الوطنية الكاملة للدولة.

كلمات مفتاحية: الأمن السيبراني؛ التحديات؛ التهديدات؛ الجوسسة السيبرانية؛ الاختراقات الإلكترونية؛ الفضاء السيبراني.

Abstract:

This study focuses on the subject of cyber security and the challenges of espionage and electronic penetration of countries through cyberspace. It aims to clarify the various cyber challenges and risks that threaten the security of countries, as well as the importance of defense and electronic deterrence to achieve national cyber security in light of the current challenges, In the conclusion, this study clearly demonstrates the fact that the one who possesses a cyber-power and advanced technology will inevitably enjoy significant influence in the cyber space and achieve cyber security that underpins the national sovereignty and security of the state.

Keywords: cyber security; challenges; threats; cyber espionage; Electronic hacks; cyberspace.

1- مقدمة

تعتبر تكنولوجيا المعلومات محل اهتمام المؤسسات العسكرية والأمنية، وهو ما غير أشكال الحروب والمواجهة بين الدول خاصة في ظل التقدم الحاصل في الوسائل التكنولوجية والأنظمة المعلوماتية وتطور الأشكال الجديدة للحروب والتهديدات الأمنية، الأمر الذي جعل فضاء القوة السيبرانية ذا شأن وأهمية في الاستراتيجيات العسكرية والمدنية، وأصبح بذلك بعدا خامسا لا يمكن الاستغناء عنه في الوقت الراهن، لما له من أهمية قصوى يستطيع أن يأثر حتى مجالات القوة الأخرى البرية، البحرية، الجوية والفضائية، فقد تغيرت الحرب في عصر المعلوماتية من خلال ظهور مسرح جديد لها وهو الفضاء السيبراني، حيث لا يمكن عده فقط مجرد بعدا جديدا للفضاءات الأخرى، وإنما قد غير طبيعة الحرب بأكملها.

أهداف البحث:

يهدف هذا البحث إلى تقديم دراسة تحليلية تحاول الإلمام بمدى أهمية موضوع الأمن السيبراني وتحديات الجوسسة والاختراقات الإلكترونية للدول، وذلك من خلال التطرق إلى مختلف المفاهيم ذات الصلة كمفهوم الفضاء السيبراني، الجوسسة الإلكترونية، الأمن السيبراني، كما تستعرض مختلف التحديات الأمنية التي تحدث من خلال الفضاء السيبراني، وهو ما يستدعي اعتماد الدول لسياسات دفاعية سيبرانية وردعية لتحقيق أمنها السيبراني وتدعيم سيادتها الوطنية التي أصبحت مهددة في ظل فضاء لا وجود فيه للحدود ومجالاته منكشفة على بعضها البعض.

إشكالية البحث: وتتمثل فيما يلي:

*ما طبيعة التحديات الأمنية في الفضاء السيبراني وكيف يمكن تحقيق الأمن السيبراني الوطني؟

فرضية البحث: وتكمن فيما يلي:

*يعتبر الفضاء السيبراني مجالا يسهل من خلاله إلحاق التهديد والضرر بأمن الدول، لذلك كلما امتلكت الدول استراتيجيات وأدوات الردع والهجوم الإلكتروني، كلما استطاعت تحقيق أمنها السيبراني الذي يكمل سيادتها الوطنية.

منهج البحث: تم الاعتماد في هذا البحث على المنهج التاريخي وكذا الإحصائي، والتي تخدم موضوع البحث وتساعد على الإجابة على إشكالية الموضوع المطروحة.

عناصر البحث: سيتم معالجة موضوع: "الأمن السيبراني وتحديات الجوسسة والاختراقات الإلكترونية للدول عبر الفضاء السيبراني"، من خلال تناول النقاط التالية:

1 - مفاهيم ومضامين كل من: الفضاء السيبراني، الجوسسة الإلكترونية، الأمن السيبراني.

2 - التحديات الأمنية للدول في الفضاء السيبراني.

3 – الدفاع والردع الإلكتروني لتحقيق الأمن السيبراني للدول في ظل التحديات الراهنة.

2. مفاهيم ومضامين كل من: الفضاء السيبراني، الجوسسة الإلكترونية، الأمن السيبراني:

1.2 الفضاء السيبراني:

هو عبارة عن بيئة إلكترونية غير ملموسة معقدة التفاعل يتم فيها بناء نماذج لظواهر أو صور إلكترونية لظواهر شبه حقيقية في التفاعلات والتعاملات البعيدة، فالسَّيْبَرة عملية انعكاسية نشطة يعكس فيها مدخلات التفاعلات الإلكترونية في بيئة لا يستطيع الإنسان إدراكها، وبصورة أخرى هي عبارة عن شبكة إلكترونية لمجموعة من الخوادم الإلكترونية حيث تتفاعل هذه الشبكات التي تتوفر فيها قاعدة بيانات، فيما بينها باستخدام وسيلة تواصل افتراضية متجاوزة كل الحواجز الجغرافية والسياسية، سعيا وراء تحسين قدرة الاتصال والتعامل الإلكتروني، كما أنها محاكاة حاسوبية عادة ما تكون في صورة بيئة افتراضية لمستخدمي العالم الافتراضي[1].

وهناك من عرف الفضاء السيبراني أيضا بأنه عالم افتراضي يتشابك مع عالمنا المادي، يتأثر به ويؤثر فيه بشكل معقد، حيث تقوم العلاقة بين العالمين على نظرة تكاملية تحمل بين طياتها مزايا ومخاطر لا تتوقف، وهناك من وصفه بالذراع الرابعة للجيوش الحديثة إلى جوار القوات البرية والبحرية والجوية، خاصة وأن الأنترنت تشهد معارك حقيقية تدور في هذا العالم الافتراضي، وهناك من يرى أنه يمثل البعد الخامس للحرب، كما يعرف على أنه المجال المادي وغير المادي الذي يتكون من عناصر تتمثل في أجهزة الكمبيوتر والشبكات والبرمجيات وحوسبة المعلومات والمحتوى ومعطيات النقل والتحكم ومستخدمو كل هذه العناصر، حيث تعد هذه العناصر العامل المشترك في جميع محاور استخدام الفضاء السيبراني، سواء أكانت الجهات المستخدمة قادرة على تعظيم قيمها وقدراتها بما في ذلك رفع كفاءة العنصر البشري أم كانت في مرحلة متأخرة[2].

وتعرف وزارة الدفاع الأمريكية الفضاء السيبراني بأنه: "مجال يتسم باستخدام الإلكترونيات (أي تكنولوجيا المعلومات) والطيف الكهرومغناطيسي في تخزين البيانات وتعديلها وتبادلها عن طريق أنظمة شبكات الاتصال والبنية التحتية المادية المرتبطة بها"، وعلى هذا التعريف تعمل الكيانات المدنية والعسكرية والإرهابية في الفضاء السيبراني لتنفيذ أنشطتها وعمليتها[3]، وبالتالي فالفضاء السيبراني هو استخدام تقنيات التكنولوجيا وكل ما يتعلق بها من ذكاء صناعي من طرف الدول أو الوكلاء لتحقيق السيطرة على فضاء القوة السيبرانية، فبه يتم التحكم في كل ما يتعلق بالحياة المدنية والعسكرية، وبذلك يعتبر المجال الخامس لفضاء القوة الاستراتيجية.

---

1 - علي زياد علي، **الصراع والأمن الجيوسيبراني في الساحة الدولية: دراسة في استراتيجيات الاشتباك الرقمي**، (عمان: دار أمجد للنشر والتوزيع، 2020)، ص ص. 53 – 54.

2 - نورة شلوش، "القرصنة الإلكترونية في الفضاء السيبراني: التهديد المتصاعد لأمن الدول"، **مجلة مركز بابل للدراسات الإنسانية**، م.8، ع.2، (2018)، ص. 190.

3 - هربرت لين، "النزاع السيبراني في القانون الدولي الإنساني"، **المجلة الدولية للصليب الأحمر**، م. 94، ع. 886، (صيف 2012)، ص. 516.

ويمكن القول أن عناصر القوة السيبرانية وقدرة التحكم والسيطرة من خلال الفضاء السيبراني؛ ترتكز على وجود نظام متماسك يعظم من القوة المتحصلة من التناغم بين القدرات التكنولوجية، والسكان والاقتصاد والصناعة والقوة العسكرية وإرادة الدولة، وغيرها من العوامل التي تسهم في دعم إمكانات الدولة على ممارسة الإكراه أو الإقناع، أو ممارسة التأثير السياسي في أعمال الدول الأخرى بغرض الوصول للأهداف الوطنية، وقد أصبح للبعد التكنولوجي والإتصالي تأثير كبير في طبيعة القوة والتفاعلات في النظام الدولي، وقد تجلى ذلك في التطور الكبير في المجال العسكري، وفي بروز مجال جديد للصراع الدولي، كما أدى أيضا إلى تغيير معايير القوة القومية، من خصائص السكان والمساحة وعدد الجيش والموارد، إلى أبعاد جديدة تتعلق بدور الدولة في الابتكار والإنتاج التكنولوجي[1].

2.2 الجوسسة الإلكترونية:

يعني التجسس السيبراني تلك المحاولات المتعمدة لاختراق أجهزة الكمبيوتر والمواقع الإلكترونية التابعة للدولة المناوئة أو الخصم بهدف سرقة معلومات سرية[2]، ويهدف للحصول على بنك معلومات هائلة عن المنظومات والأسرار العسكرية والسياسية والأمنية والاقتصادية والصناعية، والتي تعتمد بشكل كامل في عملها على وسائل ومنظومات التواصل والاتصال التكنولوجي الحديث داخل الدول[3]، حيث أن التجسس المعتمد على المجال السيبراني يؤثر سلبا على المعلومات وأنظمة المعلومات، مما يتيح إمكانية تسريب أسرار ومعلومات حساسة للدول الأخرى، وتجدر الإشارة إلى أن أجهزة الاستخبارات السيبرانية لا يقتصر على وجهة النظر الرسمية للدول والحكومات، بل يتعدى ذلك لدور الأفراد في إنتاج المعلومات وترويجها، وفي توفير كم كبير للملفات السياسية والاقتصادية مع تعدي الحدود الدولية، عكفت أجهزة استخبارات الدول للحصول عليها أولا، والبحث فيها ثانيا، وتوظيف نتائجها ثالثا[4].

ويتمثل أحد الأمثلة على التجسس العسكري في قيام "هاكرز" بالتسلل إلى جهاز أحد المتعاقدين مع الجيش الأمريكي وسرقة آلاف الملفات الخاصة بالمقاتلة "أف – 35"، وتتمثل المعلومات الاقتصادية التي يتم عادة استهدافها في براءات الاختراع وحقوق الملكية الفكرية، أو المواقف التفاوضية للدول[5]، وتجدر الإشارة أيضا إلى حالات تجسس أخرى يُذكر منها في هذا الإطار ما تناولته "مجلة دير شبيغل" الألمانية في 17 أوت 2014 من أن الاستخبارات الألمانية قد تجسست أكثر مرة على محادثات وزير الخارجية الأمريكية في تلك الفترة، بينما تجسست على تركيا لعدة سنوات،

---

1 - عادل عبد الرزاق، "القوة الإلكترونية: أسلحة الانتشار الشامل في عصر الفضاء الإلكتروني"، **مجلة السياسة الدولية**، م. 47، ع. 188، (أفريل 2012)، ص. 30.

2 - شادي عبد الوهاب منصور، **حروب الجيل الخامس: أساليب "التفجير من الداخل" على الساحة الدولية**، (القاهرة: العربي للنشر والتوزيع، 2019)، ص. 106.

3 - نضال ناجي بدوي بريوش، **"الصراع السيبراني مع العدو الصهيوني"**، دراسة منشورة مقدمة للحصول على دبلوم الدراسات الفلسطينية من أكاديمية دراسات اللاجئين، 2018/2019، ص. 14.

4 - أميرة عبد العظيم محمد عبد الجواد، "المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام"، **مجلة الشريعة والقانون**، ج، 3، ع. 35، (2020)، ص ص. 415 – 416.

5 - شادي عبد الوهاب منصور، **مرجع سابق**، ص. 106.

ونُشرت معلومات حول قيام وكالة الأمن القومي الأمريكية بالتجسس على نحو 35 من القادة على مستوى العالم، وأكثر من 60 مليون مكالمة هاتفية في دول مختلفة من بينها دول أوروبية، وهي حادثة كشفت عن أن التجسس لم يعد يشمل قاطني الدولة، بل يمتد إلى قاطني دول أخرى وقادتهم الذين هم بالأساس حلفاء مع الدولة، مما يزيد من عدم الثقة بين الحلفاء[1].

كما أعلن أمين مجلس الأمن الروسي "نيكولاي باتروشيف" في 26 أوت 2015 على العثور على برامج تابعة للاستخبارات الأجنبية في نظم المعلومات للمؤسسات الحكومية الروسية، وأكد على تزايد حالات التجسس على نظم المعلومات الحكومية، وفي واقعة مماثلة قامت شبكة دولية ضخمة للتجسس السيبراني تعمل تحت إشراف وكالة الأمن القومي الأمريكية بالتعاون مع أجهزة الاستخبارات في كندا وبريطانيا، وتجدر الإشارة إلى أنه لا يقتصر الرصد على المحطات الموجهة إلى الأقمار الصناعية والشبكات الدولية، بل يشمل الاتصالات التي تجري عبر أنظمة الاتصالات الأرضية[2]، ويُذكر في هذا المقام ما تناولته فضيحة برنامج "بيغاسوس" (Pegasus Project) الذي طورته شركة "Group NSO" الإسرائيلية، والذي استخدمته أنظمة سياسية عدة حول العالم ضد خصومها ومعارضيها[3]، وهو برنامج اختراق وتجسس تم تسويقه لحكومات دول العالم، ولديه القدرة على اختراق مليارات الهواتف التي تعمل بأنظمة تشغيل "IOS" أو "أندرويد" (Android)، وقد ازدادت قدرات برنامج "بيغاسوس" تقدما وأصبح بإمكانه الوصول إلى أهدافه عن طريق ما يسمى الهجمات "الخالية من النقر" (zero-click)، التي لا تتطلب أي تفاعل من مالك الهاتف ليتمكن من اختراقه، وغالبا ما تستغل هذه الهجمات ثغرات "الهجمات دون انتظار" (zero day)، وهي عيوب أو أخطاء في نظام التشغيل لا تكون الشركة المصنعة للهاتف المحمول قد اكتشفتها وبالتالي لا تتمكن من إصلاحها، وقد بذلت شركة "NSO Group" جهودا كبيرة حتى تجعل برنامجها صعب الكشف، وأصبح من الصعب جدا الآن التعرف على هجمات "بيغاسوس"[4]، وقد كشف تقرير نشرته عدة وسائل إعلام غربية كبيرة يوم 18 جويلية 2021 أن ناشطين وصحافيين وسياسيين حول العالم، قد تعرضوا لعمليات تجسس بواسطة برنامج "بيغاسوس"، ويستند التقرير إلى قائمة حصلت عليها منظمتا "فوربيدن ستوريز" و"العفو الدولية"[5]، حيث أظهر عن تسرب بيانات 50.000 من أرقام الهواتف، التي كان أصحابها مستهدفين للمراقبة منذ سنة 2016، ومن بين المستهدفين لهذا

1 - إيهاب خليفة، **القوة الإلكترونية: كيف يمكن أن تدير الدول شؤونها في عصر الأنترنت**، (القاهرة: العربي للنشر والتوزيع، 2017)، ص. 101.

2 - أميرة عبد العظيم محمد عبد الجواد، مرجع سابق، ص. 416.

3 - عادل رفيق، "من فضيحة بيجاسوس إلى فضيحة باراك: دلائل تورط الإمارات"، **سلسلة تقارير سياسية**، المعهد المصري للدراسات، (02 أوت 2021)، ص. 1.

4 - **"ما هو برنامج "بيغاسوس" الإسرائيلي للتجسس .. ولماذا يعد أقوى نظام لاختراق الهواتف في العالم؟"**، (2021/07/20)، سلسلة تحليلات، موقع عربي بوست، تاريخ الاطلاع (2021/07/31)، نقلا عن الرابط التالي: https://bit.ly/3xDPNNL

5 - **"فضيحة بيغاسوس: شركة إسرائيلية تجسست على صحافيين وقادة دول ومعارضين"**، (2021/07/20)، موق جريدة الجريدة، تاريخ الاطلاع (2021/07/31)، نقلا عن الرابط التالي: https://bit.ly/3rXSDM1

التجسس رؤساء دول، نشطاء، وصحفيون، بما في ذلك عائلة الصحفي السعودي "جمال خاشقجي"، ومن خلال البيانات المسربة والتحقيقات التي أجرتها منظمة "القصص المحظورة" وشركاؤها الإعلاميون، أمكن لهم تحديد العملاء المحتملين لمجموعة شركة "Group NSO" في 11 بلدا، هي: أذربيجان، والبحرين، والمجر، والهند، وكازاخستان، والمكسيك، والمغرب، ورواندا، والسعودية، وتوغو، والإمارات العربية المتحدة[1].

وتجدر الإشارة هنا إلى مصطلح الاستغلال السيبراني - له علاقة بالجوسسة - والذي يشير إلى الأنشطة المتعمدة المُصمَّمَة لاختراق أنظمة أو شبكات الحاسوب التي يستخدمها الخصم، وذلك بقصد الحصول على معلومات موضوعة على هذه الأنظمة والشبكات أو يجري تداولها من خلالها، ولا يسعى الاستغلال السيبراني إلى تعطيل التشغيل المعتاد لنظام أو شبكة حاسوب من وجهة نظر المستخدم، وإنما أفضل استغلال سيبراني هو الاستغلال الذي لا يلاحظه المستخدم أبدا، والمعلومات المطلوبة هي بوجه عام المعلومات التي يريد الخصم أن لا يتم الكشف عنها، وقد تقوم الدولة بعمليات استغلال سيبراني لجمع معلومات استخباراتية قيمة، مثلما قد تنشر جواسيس من البشر لأداء هذه المهمة، كما وقد تسعى إلى الحصول على معلومات من شبكة حاسوب شركة في بلد آخر لتستفيد منها شركة منافسة محلية في ذلك البلد، ومن بين المعلومات التي لها أهمية كبيرة تلك التي تتيح للبلد إجراء مزيد من الاختراقات لأنظمة أو شبكات حاسوب أخرى بغية جمع معلومات إضافية، أما بالنسبة للفاعلين الذين قد يقومون بمثل هذه العمليات، فإنه نظرا لطبيعة تكنولوجيا المعلومات فإن نطاق الفاعلين سواء على المستوى الوطني المحلي أو الدولي[2]، قد يكونوا من الفاعلين الدول أو الأفراد (القراصنة) أو الوكلاء السيبرانيون، أو جماعات إرهابية تعمل بشكل منفرد، أو القطاع الخاص المدني.

لقد اكتسبت الصراعات السياسية والعسكرية والاقتصادية بين الدول بعدا إلكترونيا بحيث يصعب التنبؤ بحجمها وتأثيراتها، بل أن الحروب التي تدور رحاها في الفضاء السيبراني أكثر أهمية من الأحداث التي تجري على أرض الواقع، ذلك أن الإنجازات المذهلة للتجسس السيبراني أظهرت المكاسب الكبيرة لعمليات اختراق أجهزة الكمبيوتر مقارنة بارتفاع أشكال التجسس التقليدية التي تتطلب ذكاء بشري وارتفاع نسبة الخطورة، مما جعل التجسس السيبراني على الساحة العالمية مصدر قلق للدول على أمنها الوطني، فالهجوم السيبراني ليس غاية في حد ذاته ولكنه وسيلة قوية لمجموعة متنوعة من الغايات من الدعاية إلى التجسس، ومن تعطيل الخدمات إلى تدمير البنية التحتية الحيوية، وتجدر الإشارة إلى أنه لم يحدث تغير في طبيعة التهديد للأمن الوطني، إلا أن الأنترنت قد وفرت آلية جديدة يمكنه من زيادة سرعة الهجوم وحجمه وقوته، ذلك أن انتشار الأنترنت وتزايد اعتماد العالم عليه سيترتب على الإضرار به تداعيات سياسية واقتصادية

---

1 - **"تسرب هائل للبيانات يكشف عن استخدام برمجيات التجسس لمجموعة إن إس أو الإسرائيلية في استهداف النشطاء والصحفيين والزعماء السياسيين على مستوى العالم"**، 18 جويلية 2021، منظمة العفو الدولية، تاريخ الاطلاع (2021/07/25)، نقلا عن الرابط التالي: https://bit.ly/37trYx6

1 - هربرت لين، **مرجع سابق**، ص ص. 519 – 520.

وعسكرية ملموسة، لا سيما بعد التطور اللافت للهجمات السيبرانية كنتيجة طبيعية للنزاعات في العالم الحقيقي، مما سيؤدي دورا رئيسيا في النزاعات المستقبلية[1].

3.2 الأمن السيبراني:

ويعني مجموع الإجراءات الواجب اتخاذها من قبل الأجهزة الأمنية أو الأخرى غيرها ذات العلاقة، للمحافظة على سرية المعلومات الإلكترونية، ومنع الاختراقات الفيروسية من أجل ضمان وصول المعلومات الحاسوبية إلى الجهات المختصة في الوقت المناسب، وضمان عدم وقوعها في أيدي الأعداء أو الأصدقاء على حد سواء خصوصا بعد الثورة الهائلة في عالم الاتصالات والتداولات الإلكترونية، حيث شكل هذا النوع من الأمن هاجسا استراتيجيا للقوى العالمية والمتمثلة في الولايات المتحدة الأمريكية والصين وروسيا، إذ تدور في وقتنا الحالي حرب إلكترونية بين هذه القوى من أجل اختراق المعلومات والتأثير على أسعار البورصة والعملات وغيرها من المنشآت[2].

وتعتمد المجتمعات الحديثة بشكل متنامي على تكنولوجيا الاتصالات والمعلومات المتصلة بالشبكة العالمية، غير أن هذا الاعتماد المطرد ترافقه مجموعة من المخاطر الناشئة والمحتملة التي تهدد وبشكل أساسي الشبكات وأمن المعلومات والمجتمع المعلوماتي وأعضاءه، حيث أن سوء الاستغلال اليومي للشبكات الإلكترونية لأهداف إجرامية يؤثر سلبا على سلامة البنى التحتية للمعلومات الوطنية الحساسة لا سيما على المعلومات الشخصية، وهو ما جعل الأمن السيبراني يشكل جزء أساسيا من سياسة أمنية وطنية، وأصبح من المعلوم أن صناع القرار في الولايات المتحدة الأمريكية، دول الاتحاد الأوروبي، روسيا، الصين والهند وغيرها من الدول؛ يصنفون مسائل الأمن السيبراني كأولوية في سياساتهم الدفاعية الوطنية، إضافة إلى إعلان أكثر من 130 دولة حول العالم عن تخصيص أقسام وسياسات خاصة بالحرب السيبرانية ضمن فرق الأمن الوطني، إذ تضاف جميع هذه الجهود إلى الجهود الأمنية التقليدية لمحاربة الجرائم الإلكترونية والاحتيال الإلكتروني والأوجه الأخرى للمخاطر السيبرانية[3].

وعليه فإن الأمن السيبراني هو مزيج من العمليات والتقنيات الممارسة، والهدف منه حماية البرامج والتطبيقات والشبكات وأجهزة الكمبيوتر والبيانات من الهجوم، ويشمل الأمن السيبراني الأمن المادي للبرامج والتطبيقات والشبكات وأجهزة الكمبيوتر، وأمن غير مادي أو معنوي يتعلق بالبيانات والمعلومات من أي هجوم وأضرار متعمدة وسرقة المعلومات والتحكم في الوصول الصحيح للأجهزة والتطبيقات والشبكات لحمايتها من الضرر الذي قد يحدث عبر الشبكات[4] في الفضاء السيبراني سواء من طرف الدول أو الفاعلين السيبرانيون الآخرين.

---

2 - مصطفى إبراهيم سلمان الشمري، الأمن السيبراني وأثره في الأمن الوطني العراقي"، **مجلة العلوم القانونية والسياسية**، م. 10، ع. 01، (جوان 2021)، ص. 164.

2 - علي زياد علي، **مرجع سابق**، ص. 56.

3 - **نفس المرجع**، ص ص. 56 – 57.

4 - مصطفى إبراهيم سلمان الشمري، **مرجع سابق**، ص. 157.

ومن ثم يحظى الأمن السيبراني بأهمية بالغة ذلك أن الحكومات والمؤسسات العسكرية والشركات والمؤسسات المالية والطبية وغيرها تقوم بجمع ومعالجة وتخزين كميات كبيرة جدا من البيانات على أجهزة الكمبيوتر والأجهزة الأخرى، وإن كثير من هذه البيانات معلومات حساسة كونها تتعلق بالملكية الفكرية أو معلومات أمنية أو شخصية أو بيانات مالية، إذ أن الدخول غير المصرح به إلى هذه المعلومات والبيانات له عواقب وخيمة، ولاسيما وأن هذه المعلومات تنتقل بين المؤسسات والشركات عبر الشبكات إلى أجهزة أخرى، ونظرا لارتفاع الهجمات الإلكترونية فإن الدول والمؤسسات والشركات تجد نفسها مضطرة لحماية بياناتها ومعلوماتها، بل أصبحت الهجمات والاختراقات الإلكترونية والتجسس الرقمي يمثلان أكبر تهديد للأمن الوطني لأي دولة في النظام الدولي[1].

3. التحديات الأمنية للدول في الفضاء السيبراني:

لقد شكل الفضاء السيبراني ميدان المعركة الخامس بين القوى الدولية، وذلك بعد الأرض، البحر، الجو والفضاء، فاستهداف الهجوم للبنية المعلوماتية يمكن أن يشكل ضربة قاضية لاقتصاد بلد من البلدان، أو يمكنه إلحاق الضرر الفادح[2] في كل القطاعات التي يمكن التسلل لها إلكترونيا سواء كانت عسكرية أو مدنية، فمن خلال الاعتبارات السابقة الذكر حول طبيعة الفضاء السيبراني، يمكن أن تظهر توابع أخرى قابلة للنقاش، فلا تستطيع الدول أن تعبر عن سيادتها في الفضاء السيبراني، لأن اعتماد الناس على هذا البعد التكنولوجي يجعله عرضة بشكل خاص للأعمال العدائية، فلا يزال المهاجمون السيبرانيون يتمتعون بمميزات تفوق إمكانات المدافعين بسبب التأثير المفاجئ الذي لا يمكن أن يقلل من قوته أي أسلوب أمني أو دفاعي سلبي أو حتى إيجابي بشكل تام، كما أن هؤلاء المهاجمين يمتلكون القدرة على إخفاء آثارهم، ولا تسمح الحالة المعرفية بوضع توصيف دقيق للعمليات الهجومية التي تحدث في الفضاء السيبراني، الأمر الذي يجعلنا في مواجهة جميع الاحتمالات[3].

وفي الواقع لقد ساعدت عدة عوامل على تنامي التهديدات السيبرانية لمصالح الدول، ومن ثم إمكانية بروز حروب سيبرانية، من هذه العوامل ما يلي:

1 - تزايد ارتباط العالم بالفضاء الإلكتروني (السيبراني)، الأمر الذي اتسع معه خطر تعرض البنية التحتية الكونية للمعلومات لهجمات إلكترونية في الفضاء السيبراني.

2 - تراجع دور الدولة في ظل العولمة وانسحابها من بعض القطاعات الاستراتيجية مع تصاعد أدوار الشركات متعددة الجنسيات، خاصة العاملة في مجال التكنولوجيا كفاعل مؤثر في الفضاء السيبراني.

---

1 - مصطفى إبراهيم سلمان الشمري، **مرجع سابق**، ص ص. 158 – 159.

2 - باسكال بونيفاس، **الجيوبوليتيك: مقاربة لفهم العالم في 48 مقالا**، (ترجمة: إياد عيسى)، (دمشق: منشورات الهيئة العامة السورية للكتاب، وزارة الثقافة، 2020)، ص. 81.

3 - جوزيف هينروتين وآخرون، **حرب واستراتيجية: نهوج ومفاهيم (الجزء الثاني)**، (ترجمة: أيمن منير)، (الصفاة/ الكويت: المجلس الوطني للثقافة والفنون والآداب، جوان 2019)، ص. 71.

3 - تزايد اعتماد الدول على الأنظمة الإلكترونية في جميع منشآتها الحيوية، الأمر الذي جعل من الممكن الإضرار بمصالحها من خلال الهجمات الإلكترونية في حالات العداء.

4 - قلة تكلفة الحروب السيبرانية مقارنة بنظيراتها التقليدية، مع إمكانية شن الهجوم في أي وقت، بحيث لا يتطلب تنفيذه سوى وقت محدود.

5 - تحول الحروب السيبرانية إلى إحدى أدوات التأثير في المعلومات المستخدمة في مستويات ومراحل القتال الإلكتروني والصراع المختلفة، سواء على الصعيد الاستراتيجي أو التكتيكي العملياتي بهدف التأثير بشكل سلبي على هذه المعلومات ونظم عملها .

6 - توظيف الفضاء السيبراني في تعظيم قوة الدول، من خلال إيجاد ميزة أو تفوق أو تأثير في البيئات المختلفة، وبالتالي ظهر ما يسمى الاستراتيجية السيبرانية للدول.

7 - اتساع نطاق مخاطر الأنشطة العدائية التي يمارسها الفاعلون، سواء من الدول أو من غير الدول في الحروب السيبرانية، فقد تشن الهجمات الإلكترونية عبر أجهزتها الأمنية الدفاعية، كما قد تلجأ إلى تجنيد قراصنة أو موالين لشن هجمات ضد الخصوم دون أي ارتباط رسمي[1] .

وهو ما جعل مختلف دول العالم تتعرض إلى عمليات اختراق إلكترونية وجوسسة في الفضاء السيبراني للحصول على معلومات عسكرية كانت أو مدنية، وحتى القيام بالتعرض لعمليات إتلاف للبيانات وتدمير المنشآت، ونظرا لأن الدول تختلف فيما بينها من حيث أنظمة الحماية والدفاع الإلكتروني، وتبيان قدرات الدول الكبرى في مجال التحكم في الفضاء السيبراني ومحاولات الهيمنة والسيطرة عليه، ما خلق تحديات أمنية تتعرض لها الدول دونما استثناء، وفيما يلي يمكن تبيان مختلف تلك التحديات:

1 - استهداف البنية التحتية للدول: حيث يتم استهداف البنية التحتية للدول، سواء كانت مدنية أو عسكرية بهجمات إلكترونية[2]، بما يؤدي إلى شلل أنظمتها وتدمير أنظمة التشغيل الخاصة بها، والتأثير على تدفق المعلومات بما يؤدي إلى إرباك عمل البنية التحتية الحيوية، وينشأ عن مثل هذه الهجمات تعطيل العديد من مرافق الحياة في الدول وسيادة الفوضى[3]، مثل استهداف محطات الطاقة والوقود والخدمات المالية والمصرفية ونظم الاتصالات والمواصلات، ومن أبرز الأمثلة على ذلك تعرض أوكرانيا خلال شهر جوان 2017 لهجمة إلكترونية شملت محطات الطاقة، بالإضافة إلى المؤسسات المالية وأحد أكبر محطاتها، ولقد شهدت السنوات القليلة الماضية العديد من الهجمات الإلكترونية على بعض البنى التحتية الحرجة والمؤسسات العسكرية، مثل محطات الطاقة النووية، كما هو الحال في قيام فيروس "ستاكسنت" (Stuxnet) بتعطيل حوالي ألف من أجهزة الطرد المركزي في منشأة لتخصيب اليورانيوم في مفاعل

1 - علي زياد العلي، **مرجع سابق**، ص ص.79 – 78 .

2 - إيهاب خليفة، "تنامي التهديدات السيبرانية للمؤسسات العسكرية"، **مجلة اتجاهات الأحداث**، ع. 22، (جويلية/ أوت 2017)، ص. 56.

3 - أميرة عبد العظيم محمد عبد الجواد، **مرجع سابق**، ص ص. 431 – 432.

"ناتانز" في وسط إيران سنة 2010، فضلا عن تعرض أنظمة الكمبيوتر لشركة كوريا الجنوبية للطاقة المائية والنووية التي تديرها الدولة لهجمات إلكترونية في شهر ديسمبر 2014، واتهمت الولايات المتحدة الأمريكية روسيا بالتورط في شن هجمات إلكترونية على شبكات الكمبيوتر في عدة محطات طاقة نووية[1]، كما رُبطت انقطاعات الكهرباء المتعددة في البرازيل بهجمات سيبرانية أيضا، ففي عام 2008 تمكن القراصنة من الدخول إلى الموقع الشبكي للحكومة والسيطرة عليه لمدة تزيد عن أسبوع، حيث توضح انقطاعات الكهرباء في البرازيل الاتساع المحتمل للأنواع الجديدة من الهجمات السيبرانية، وجاء في التقارير تشبيه المشهد بفيلم من أفلام الخيال العلمي حيث توقفت تماما قطارات الأنفاق وإشارات المرور وثاني أكبر محطة إنتاج قوى كهربائية وهو سد" إيتايبو"، وتأثر أكثر من 60 مليون شخص جراء ذلك[2]، كما تعرضت شبكات الكهرباء في الولايات المتحدة الأمريكية أيضا لمثل هذه الهجمات في شهر ماي 2009 [3]، وتجدر الإشارة أيضا إلى أحد الهجمات السيبرانية الشائعة والمعروفة على البنية التحتية الحيوية، والمتمثلة في الهجوم على خط أنابيب النفط التركي في 05 أوت 2008 والذي اشتعلت فيه النيران بطريقة غامضة دون إطلاق أي مستشعرات أو إنذارات، على الرغم من أن الانفصاليين الأكراد زعموا بأنهم من تسبب بالهجوم، إلا أن عدد من مسؤولي المخابرات الأمريكية قد أدانوا روسيا التي عارضت إنشاء خط أنابيب الغاز "باكو – تبليسي – جيهان" لأنه خارج الأراضي الروسية، ومن شأنه تقويض قدرتها على التحكم في تدفق الطاقة باتجاه أوروبا[4]، كما هاجم فيروس "الصخرة الدوارة" (Stone Drill) سنة 2017 السعودية من طرف قراصنة إيرانيين، حيث استهدف قطاع الطيران والبتروكيماويات، وقد أحدث هذا البرنامج الخبيث تأثيرات كبيرة على شركات الطيران وشركات البتروكيماويات في السعودية، وفي سنة 2019 تم تنفيذ هجمات سيبرانية متقدمة مستمرة تدعى (APT) وهي هجمات بالغة التأثير، مارسها قراصنة سيبرانيون إيرانيون لاستهداف شبكات المعلومات وبنيتها التحتية في كل من قطر، الكويت، السعودية، الإمارات والبحرين، خلال مدة زمنية متطاولة لضمان بلوغ أهدافها وتعميق مستويات تأثيرها[5]، وفي 2 جويلية 2020 شن هجوم على مفاعل "نتانز" النووي الإيراني نسب إلى جهات أمريكية و"إسرائيلية"، كما حدث انفجار في محطة "شهيد مدح زرقان"، وتسرب للغاز الكلور في مركز "كارون" للبتروكيماويات في مدينة "ماشهر" بتاريخ 04 جويلية، وانفجار داخل مصنع للأكسجين في بلدة "باقر شهر" بتاريخ 07 جويلية، وانفجار آخر في غرب مدينة "طهران" أصاب منشأة (مستودع) صواريخ تابع للحرس الثوري الإيراني بتاريخ 09 جويلية، وانفجار غاز مبنى سكني في طهران

---

1 - إيهاب خليفة، "تنامي التهديدات السيبرانية للمؤسسات العسكرية"، **مرجع سابق**، ص ص. 56 – 57.

5 - حمدون إ. توريه وآخرون، **البحث عن السلام السيبراني**، (جنيف: الاتحاد الدولي للاتصالات والاتحاد العالمي للعلماء للطبع، جانفي 2011)، ص ص. 7 – 8.

3 - مصطفى إبراهيم سلمان الشمري، **مرجع سابق**، ص. 165.

4 - حسين باسم عبد الأمير، "**تحديات الأمن السيبراني**"، (17 ماي 2018)، مركز الدراسات الاستراتيجية، كربلاء، العراق، تاريخ الاطلاع (2021/07/05)، نقلا عن الرابط التالي: https://bit.ly/37pinaG

5 - ياسمين بلعسل بنت نبي والحسين عمروش، "التهديدات الإلكترونية والأمن السيبراني في الوطن العربي"، **مجلة نوميروس الأكاديمية**، م. 02، ع. 02، (جوان 2021)، ص ص. 171 – 172.

بتاريخ 11 جويلية، وانفجار في مصنع "توندجويان" للبتروكيماويات في "ماشهر" بتاريخ 12 جويلية، وانفجار مجمع صناعي بالقرب من مدينة "مشهد" بتاريخ 13 جويلية، وحريق في مصنع للألمنيوم في بلدة "لامرد" يوم 15 جويلية، وانفجار في خط أنابيب نفط بمدينة "الأهواز" يوم 18 جويلية، وانفجار في محطة توليد الطاقة في مدينة "أصفهان" يوم 19 جويلية 2020، وفي جانب آخر أعلنت مجموعة "المنتقمون" الإيرانية مسؤوليتها عن هجوم سيبراني إيراني على شبكة المياه والكهرباء الإسرائيلية بتاريخ 16 جويلية 2020 [1]، وغيرها من الهجمات التي تستهدف البنى التحتية للدول.

3 – السيطرة على الأنظمة العسكرية وتعطيلها وإتلافها: وذلك من خلال قيام قراصنة محترفين أو جيوش نظامية إلكترونية ووكلاء سيبرانيين بشن هجمات إلكترونية بغرض السيطرة على نظم القيادة والسيطرة عن بعد، الأمر الذي يؤدي إلى إخراج بعض منظومات الأسلحة عن سيرة القيادة المركزية، وإعادة توجيهها نحو أطراف داخلية أو ضد دول صديقة، كما يمكن أيضا السيطرة على الطائرات من دون طيار، أو الغواصات النووية في أعماق البحار، أو السيطرة على الأقمار الصناعية العسكرية في الفضاء الخارجي وإخراجها عن سيطرة الدولة التابعة لها هذه الأسلحة والمعدات، إذ تزداد خطورة مثل هذه الهجمات إثر التطور التكنولوجي واعتماد اللوجستيات ونظم القيادة والتحكم وتحديد الأهداف، وإصابتها على برامج الكمبيوتر وشبكات الاتصال[2].

كما تقوم الهجمات السيبرانية بتدمير أنظمة إلكترونية لمنشآت حيوية عسكرية، وتعطيل أو إتلاف شبكات الدفاع العسكرية عن بعد، واختراق أو تعطيل أو تدمير شبكات القطاع الخاص ذا الصلة بالقطاع العسكري، وكذا التدخل في سلامة البيانات العسكرية الداخلية لدول أخرى، والقيام بمحاولات الإرباك والتشويش على أجهزتها[3]، وقد تحدث الهجومات السيبرانية من أجل سرقة تصميمات الأسلحة العسكرية والتقنيات التكنولوجية الحديثة، حيث قام قراصنة صينيون بشن هجمات على شركة "لوكهيد مارتين" الأمريكية، وسرقة معلومات عن تكنولوجيا تصنيع المقاتلة "أف – 35" التي استخدمتها الصين فيما بعد لدى تصميم وتصنيع مقاتلة "تي 20" الصينية، وشملت الهجمات السيبرانية أيضا مقاولين لدى وزارة الدفاع الأمريكية يعملون على صناعة وتطوير الطائرات من دون طيار الأمريكية، بهدف سرقة معلومات حول هذه الطائرات وكيفية صناعتها وتطويرها[4].

3 – سرقة المعلومات والبيانات العسكرية أو التلاعب بها: وذلك عبر اختراق قواعد البيانات العسكرية وسرقتها أو تزييفها أو تدميرها إلكترونيا، حيث تسعة الهجمات الإلكترونية في هذه الحالة إلى اختراق الشبكات الخاصة بالمؤسسات

---

1 - محجوب الزويري ويارا نصار، "إيران والهجمات السيبرانية: فصل جديد في الحرب غير المعلنة"، **مجلة رؤية تركية**، م. 09، ع. 04، (خريف 2020)، ص. 124.

1 – إيهاب خليفة، "تنامي التهديدات السيبرانية للمؤسسات العسكرية"، **مرجع سابق**، ص. 57.

3 - أميرة عبد العظيم محمد عبد الجواد، **مرجع سابق**، ص ص. 373 – 374.

4 - إيهاب خليفة، **مجتمع ما بعد المعلومات: تأثير الثورة الصناعية الرابعة على الأمن القومي**، (القاهرة: العربي النشر والتوزيع، 2019)، ص ص. 114 – 115.

العسكرية بهدف سرقة خرائط أنظمة التسليح أو التصميمات الخاصة بالمعدات العسكرية، وتجدر الإشارة في هذا الصدد إلى أنه قد انطلقت واحدة من أخطر الهجمات ضد أنظمة حواسب الجيش الأمريكي سنة 2008 من خلال وصلة (USB) كانت متصلة بجهاز كمبيوتر محمول تابع للجيش الأمريكي في قاعدة عسكرية موجودة في الشرق الأوسط، و لم يتم اكتشاف انتشار برامج التجسس في كل الأنظمة السرية وغير السرية في الوقت المناسب، مما شكل ما يشبه جسرا رقميا، تم من خلاله نقل آلاف الملفات من البيانات إلى خوادم خارجية (Servers)، وبالمثل تم استهداف أكثر من 72 شركة من بينها 22 مكتبا حكوميا و13 من مقاولي قوات الدفاع بهدف سرقة معلومات حول الخطط والمباني العسكرية[1]، وفي نفس السياق تعرض العراق في 26 و27 سبتمبر 2019 إلى هجوم سيبراني من قبل قراصنة طالت قرابة 30 موقعا حكوميا، أبرزها مواقع وزارة الدفاع والداخلية والخارجية والأمن الوطني والصحة، وقد استغل المهاجمون بعض الثغرات فعملوا على تطبيق التغييرات على بيانات مواقع البحث التي من شأنها توجيه المستخدمين إلى صفحة بحث مختلفة، وعلى الرغم من أن الجهات الحكومية العراقية قد نجحت في استعادة سريعة لبعض المواقع إلا أن بعضها استغرق وقتا أطول، علما أن المهاجمين تمكنوا من الدخول إلى أجهزة الحواسيب الحكومية واختراق قواعد بيانات من المفروض أن تكون محمية بشكل جيد مما سمح لهم بأخذ معلومات كثيرة[2].

4 – جمع معلومات اقتصادية استخباراتية: ويتحقق عن طريق اختراق قواعد البيانات المالية والمصرفية وقواعد بيانات الشركات والبنوك وجمع المعلومات التي قد تؤثر على الأمن الوطني للدول، وكذلك من خلال التجسس على المسؤولين الماليين ووزراء المالية ورؤساء الشركات الكبرى، وفي هذا الصدد أصدر الرئيس الأمريكي السابق "باراك أوباما" أثناء فترة إدارته الثانية أوامره بوقف التنصت على مقري صندوق النقد الدولي والبنك الدولي، وذلك في إطار مراجعة أنشطة جمع المعلومات الاستخباراتية وذلك في أعقاب التسريبات التي كشف عنها المتعاقد السابق مع وكالة الأمن القومي "إدوارد سنودن" بشأن برامج لجمع كميات كبيرة من البيانات عن حلفاء وأعداء الولايات المتحدة الأمريكية والمواطنين الأمريكيين[3]، كما أجرت كوريا الشمالية سنة 2014 هجوما إلكترونيا ضد شركة " Sony Pictures Entertainment"، مما جعل الآلاف من أجهزة كمبيوتر تلك الشركة (سوني Sony) غير صالحة للعمل، وتم اختراق المعلومات التجارية السرية للشركة، بالإضافة إلى الطبيعة المدمرة للهجمات؛ سرقت كوريا الشمالية نسخا رقمية لعدد من الأفلام التي لم يتم إطلاقها، بالإضافة إلى آلاف المستندات التي تحتوي على بيانات حساسة تتعلق بالشخصيات الشهيرة وموظفي شركة (سوني Sony)، ولقد كان هذا الهجوم السيبراني من أكثر الهجمات الإلكترونية تأثيرا على الولايات المتحدة الأمريكية، وقد أدى هذا الهجوم إلى مزيد من النقاش حول طبيعة التهديد السيبراني والحاجة إلى تحسين

1 - إيهاب خليفة، "تنامي التهديدات السيبرانية للمؤسسات العسكرية"، **مرجع سابق**، ص. 57.

2 - مصطفى إبراهيم سلمان الشمري، **مرجع سابق**، ص ص. 174 – 175.

3 - إيهاب خليفة، "تنامي التهديدات السيبرانية للمؤسسات العسكرية"، **مرجع سابق**، ص. 57.

الأمن السيبراني[1]، ومن ثم يرتبط هذا النوع من التجسس بالصناعات التقنية مثل البرمجيات والتقنية الحيوية وتقنيات الفضاء والاتصالات والموارد والطاقة[2].

ومن ثم فالحروب السيبرانية صراع يستخدم معاملات أو هجمات معادية غير قانونية على الحواسيب والشبكات في محاولة لتعطيل الاتصالات وغيرها من البنى التحتية، كإلحاق الضرر الاقتصادي، والسياسي وكذا العسكري، حيث تشمل الأسلحة السيبرانية المستخدمة من أجل تحقيق الأهداف الجيوسياسية مجموعة كبيرة من الأدوات، مثل تلك المتعلقة بالمراقبة، التجسس، التضليل، أو الهجمات المدمرة، وفي هذا الإطار يمكن تقسيم الهجمات السيبرانية إلى نوعين[3]:

1 – الاختراقات التي تستهدف جمع المعلومات (التجسس الرقمي).

2 – الهجمات على الأنظمة الأجنبية لإيقاف شبكات الخصوم أو إتلافها، مثل الهيئات الحكومية والأهداف الرمزية والبنية التحتية الحيوية.

وعلى هذا فيمكن اعتبار تحدي الأمن السيبراني أعلى تحديات الأمن الوطني في القرن الواحد والعشرين، مع الإشارة إلى أن المفهوم الحديث للأمن لا يقتصر فقط على الجوانب العسكرية، بل يواكب كل التهديدات والتحديات التي يمكن أن تشكل حجر عثرة أمام الاقتصاد الرقمي وتدفق المعرفة، فقد أسقطت تكنولوجيا المعلومات والاتصالات مفهوم الحدود الجغرافية بين الدول مما يضع السيادة الوطنية على المحك، خاصة مع اختراق المواقع الحكومية الرسمية والتجسس المعلوماتي على الدول[4].

وتجدر الإشارة إلى أنه وفي ظل التنافس الاستراتيجي الأمريكي – الصيني حول احتكار التكنولوجيا والتقنية، وحقوق الملكية الفكرية ونقل التكنولوجيا وتطوير تقنية الجيل الخامس والتي ترى فيها الولايات المتحدة الأمريكية مجالا سوف يمكن من توظيفها في مجال الأنشطة الاستخباراتية، سعت الصين بشكل دؤوب لفض ذلك الاحتكار وتحسبا في أن تتخلص من تبعيتها التكنولوجية للغرب، أنشأت الصين من خلال" الأكاديمية الصينية للهندسة "سنة 2013 فريقا ضم أكثر من 100 أكاديمي وعالم باحث اتجاه تطوير القطاع الصناعي الصيني، واستعراض إجراءات واستراتيجيات الدول الصناعية المتقدمة، وقضايا القطاع الصناعي الصيني وآثار التقدم الرئيسية، وبعد سنتين من الجهود قدم الفريق بحثا حول القطاع الصناعي الصيني استندت إليه الحكومة الصينية في صياغة استراتيجيتها "صنع في الصين 2025"، حيث تهدف إلى الارتقاء بالقطاع الصيني وتحويله إلى قطاع متقدم يسهم في تعزيز القدرة التنافسية الصناعية الصينية، لتنضم الصين إلى صفوف دول العالم المتقدم في القطاع الصناعي، من حيث تخفيض استهلاك الموارد ورفع إنتاجية العمل،

1 - علاء الدين فرحات، "الفضاء السيبراني: تشكيل ساحة المعركة في القرن الحادي والعشرين"، **مجلة العلوم القانونية والسياسية**، م. 10، ع. 03، (ديسمبر 2019)، ص. 93.

2 - أميرة عبد العظيم محمد عبد الجواد، **مرجع سابق**، ص ص. 418 – 419.

3 - علاء الدين فرحات، **مرجع سابق**، ص. 98.

4 - أميرة عبد العظيم محمد عبد الجواد، **مرجع سابق**، ص ص. 374 – 375.

وتعزيز القدرة على الابتكار وتحسين الهيكل الصناعي، والإسراع في تكامل المعلومات والتصنيع وزيادة عدد براءة الاختراع، والاستثمار في البحث والتطوير والعنصر البشري، ونسبة الربح من المبيعات على نحو يساعد في رفع القطاع الصناعي للصين على نحو شامل، ويجعلها في مقدمة الدول المنتجة لتكنولوجيا الثورة الصناعية الرابعة[1]، حيث تسعى الصين إلى السيطرة الرقمية، والاستثمار في تقنية الجيل الخامس (G5)، ومن شأن استخدام هذه التقنية أن تعمل على أن تصبح أجهزة الواقع الافتراضي موثوقة بما يكفي للاستخدام العالي الدقة في العمل، حيث أن هذا التطور في تلك التقنية لديه القدرة على زيادة إنتاجية العامل البشري بشكل كبير، وكذا السماح لهم بالعمل في تناغم أوثق مع الروبوتات، إذ يتم استخدام هذه التقنيات بالفعل على أرضيات المصانع[2]، وفي ظل التصعيد الأمريكي، تقوم الصين بتغيير عقيدتها الصناعية حاليا من أجل تحقيق الهيمنة في مجال التكنولوجيا الفائقة الذكاء وتحقيق مزيد من الاحتكار في الأسواق العالمية، بحيث تصبح في باكورة صفوف الدول المبتكرة للتكنولوجيا وليس المقلدة لها، وفي ذلك تصطدم بالولايات المتحدة الأمريكية ودول أوروبا من عدة جوانب، فهي من ناحية تمثل تهديدا للأمن القومي لهم خشية التعرض للاختراق في أثناء استخدام التكنولوجيا الصينية، ومن ناحية أخرى تمثل تهديدا مباشرا للاقتصاديات الغربية التي لا تزال تستحوذ على المراتب الأولى في هذه التقنيات[3].

ومما سبق ذكره يمكن القول بأن المجال السيبراني قد دخل ضمن المحددات الجديدة للقوة وأبعادها من حيث طبيعتها وأنماط استخدامها، بل وأيضا طبيعة الفاعلين وهو ما كان له انعكاس على قدرات الدول وعلاقاتها الخارجية، وأضفى خصائص جديدة للقوة والتي تمتد لتشمل كافة الوسائل والطاقات والإمكانات المادية وغير المادية، المنظورة وغير المنظورة التي بحوزة الدول، ويستخدمها صانع القرار في فعل مؤثر يحقق مصالح الدولة، بما سيؤثر به في سلوك الوحدات السياسية الأخرى، فالعلاقة بين الأمن السيبراني والأمن الوطني تزداد كلما زاد نقل المحتوى المعلوماتي والعسكري، الأمني، السياسي، الاقتصادي، الاجتماعي، الفكري، الخدمي، العلمي والبحثي إلى الفضاء السيبراني، خاصة مع تسارع الدول في تبني الحكومات الإلكترونية والمدن الذكية في العديد منها، واتساع نطاق وعدد مستخدمي الأنترنت في العالم، مما أدى إلى أن تكون قواعد البيانات الوطنية في حالة انكشاف خارجي، إضافة إلى حملات الدعاية والمعلومات المضللة ونشر الشائعات أو الدعوة لأعمال تحريضية أو دعم المعارضة أو الأقليات، مما يساهم في تلاشي سيادة الدولة ويشكك في قدرتها على الحفاظ على أمنها الوطني[4].

---

2 - إيهاب خليفة،" الصراع الأمريكي – الصيني على التكنولوجيا الفائقة الذكاء"، **مجلة السياسة الدولية**، م. 54، ع. 218، (أكتوبر 2019)، ص. 91.

2 - Marcus Lu, "Economy Visualized: Where 5G Will Change the World", 09/03/2020, Visual Capitalist, (22/03/2021), see the link: https://bit.ly/3C8U9jl

4 - إيهاب خليفة،" الصراع الأمريكي – الصيني على التكنولوجيا الفائقة الذكاء"، **مرجع سابق**، ص. 93 .

1 – أميرة عبد العظيم محمد عبد الجواد، **مرجع سابق**، ص ص. 434 – 435.

4. الدفاع والردع الإلكتروني لتحقيق الأمن السيبراني للدول في ظل التحديات الراهنة:

1.4 أهداف الدفاع في الفضاء السيبراني:

يهدف الدفاع الإلكتروني* إلى الحفاظ على قدرات الأمن الوطني التكنولوجي للدول، من خطوط اتصالات وشبكات كمبيوتر وبنية تحية سواء مدنية أو عسكرية، فضلا عن تأمين البيانات الحيوية بما يساهم في النهاية في تحقيق الأمن السيبراني للدول، وفيما يلي يمكن تحديد أهداف الدفاع الإلكتروني[1]:

1 – حماية الأهداف العسكرية: والتي تشمل تأمين نظم الإدارة والمراقبة ونظم التحكم والسيطرة، ونظم توجيه الأسلحة وقطاع الاتصالات الحربية والأسلحة الآلية القيادة، مثل الطائرات من دون طيار، فضلا عن حماية المنشآت العسكرية والحيوية مثل محطات الطاقة النووية من أي اختراق إلكتروني.

2 – حماية البيانات العسكرية: والتي تشمل معلومات حول أفراد القوات المسلحة كالأسماء والرتب والمرتبات والوظائف داخل الجيش وأماكن الإقامة الشخصية، فضلا عن خطوط التسليح وتصميمات الأسلحة وخرائط انتشار القوات وتوزيع الأسلحة.

3 – حماية البنية التحتية الحرجة: كمثل قطاع الاتصالات والمواصلات ومحطات الطاقة، وقواعد البيانات الحكومية وخدمات الحكومات الذاتية والبنوك والمؤسسات المالية.

4 – دعم وحدات الحرب الإلكترونية: وهي تلك الوحدات الخاصة بإدارة الحروب السيبرانية للدول، حيث تكون مهمة الدفاع الإلكتروني هي تأمين الخطوط خلف هذه الوحدات، بما يحمي أهداف الدول الاستراتيجية في حالة شن هجوم إلكتروني مضاد عليها، وتوفير غطاء إلكتروني للوحدات المقاتلة بهدف التمويه والخداع وصعوبة تعقب مصدر الهجمة.

5 – تحقيق الردع الإلكتروني: وذلك من خلال رفع تكلفة الهجوم الإلكتروني للدولة المعتدية، عبر إنشاء نظم دفاع إلكترونية صعبة الاختراق التي تحتاج إلى وقت وجهد كبيرين لاختراقها، مع تطوير قدرات تتبع الهجمات الإلكترونية واكتشاف مصدرها بما يؤدي في النهاية إلى التأثير على قرارات الخصم وردعه عن شن هجمات إلكترونية على الدولة.

إنه رغم السياسات المعتمدة من قبل الدول من أجل التأمين من الهجمات السيبرانية، إلا أنه في السنوات الأخيرة ومع التقدم التقني قد لوحظ وجود وحدوث مجموعة واسعة من الهجمات باستخدام مستويات مختلفة من المهاجمين، ومن المتسللين من ذوي الخبرة إلى الحملات المدعومة من طرف الدول، مما أثار فكرة الردع السيبراني وعدم الاكتفاء بالدفاع السيبراني، وهو ما أدى حسب الباحث "محمد باسم عبد الأمير" إلى إحياء وصياغة عبارة "كلاوزوفيتز" الشهيرة: "الحرب هي استمرار للسياسة لكن بواسطة وسائل أخرى" بالعبارة التالية: "إن الحرب الإلكترونية هي استمرار

---

* الدفاع السيبراني: يقصد به مجموعة القدرات النظامية التي تمتلكها القوات العسكرية للحماية من تأثيرات الهجمات السيبرانية والتخفيف من حدتها والعمل على التعافي من تأثيراتها بسرعة.

2 - إيهاب خليفة، "تنامي التهديدات السيبرانية للمؤسسات العسكرية"، **مرجع سابق**، ص. 55.

للسياسة بوسائل أخرى، عندما لا ترغب الحكومات في ممارسة القوة الغاشمة والصلبة"[1]، وبناء على ذلك فإنه أصبح من الضروري عدم الاكتفاء بالدفاع الإلكتروني خاصة في ظل التحديات الراهنة مما استوجب دعمها بالردع الإلكتروني لتحقيق الأمن السيبراني.

2.4 الردع الإلكتروني لتحقيق الأمن السيبراني:

يهدف الردع إلى خلق مجموعة من المحفزات المانعة لقيام أحد أطراف الصراع من القيام باعتداء أو هجوم مستقبلا، وإذا كان ذلك هو هدف الردع في التفاعلات الدولية على أرض الواقع، فإنه مختلف جزئيا عن حالة الردع الإلكتروني، لأن أحد الفواعل غير قادر على إزالة تدمير الطرف الآخر كليا منا في حالة الردع النووي مثلا، كما أنه ليس من السهل تحقيق الردع الإلكتروني بسبب خاصية التخفي، والتي تمنع مستخدم القوة الإلكترونية من التعرف على خصمه أو التوقع من أين سوف تأتيه الضربة، وفي ظل نظام دولي يتميز بتعدد القطبية ما يزيد من حالات الصراع، فضلا عن تعدد الفاعلين من الدول وغير الدول الذين يستخدمون فضاء القوة السيبرانية في التفاعلات الدولية، بالإضافة إلى خاصية التخفي فإن احتمالات الصراع الدولي تزداد[2] مع التقدم التقني.

إنه في ظل تنامي التوتر والصراعات في العلاقات بين الدول على المستويين الإقليمي أو الدولي، يتوقع أن تلجأ الدول إلى توظيف الحروب الإلكترونية كأدوات إضافية في إدارة صراعها مع خصومها، خاصة مع تنامي أدوار الفواعل المسلحة من غير الدول، وهو ما يؤشر إلى زيادة التهديدات النابعة من الفضاء السيبراني مستقبلا، مما يتطلب من الدول كافة اتخاذ إجراءات لضبط سلوكها في الفضاء السيبراني، فضلا عن تطوير قدرات دفاعية لتأمين نفسها في مواجهة تلك التهديدات[3]، وفي هذا الصدد فإنه يمكن الإشارة إلى أن الدفاع السيبراني الوقائي يتحقق من خلال ثلاثة أساليب رئيسية وهي :

1 - الكشف المبكر عبر الهجمات في وقتها الحقيقي: وهو ما يتم من خلال استخدام "حساسات" (Sensors) على الشبكات والبرامج والتطبيقات، بالإضافة إلى توظيف المعلومات الاستخباراتية لرصد أي نشاط غير طبيعي قد يصنف على أنه هجمات سيبرانية، وبداية مواجهتها واحتواءها قبل أن تبدأ نشاطها في الشبكة أو النظم المستهدفة.

2 - الهجوم السيبراني الإستباقي: وذلك من خلال استخدام ونشر" الديدان البيضاء" (White Worms)، وهي برامج قادرة على اكتشاف التطبيقات الضارة وتدميرها قبل توظيفها في إطلاق هجمات سيبرانية محتملة، كما تقوم أيضا بتدمير أدوات وبرمجيات القراصنة، وهو ما يساعد في إحباط مخطط الهجمات نفسها، وتحديد هوية ومصدر الهجمة، بما يمكن من إطلاق هجمة إلكترونية مضادة فيما تعرف بـــ" الاختراق العكسي" (Hack-back).

1 - حسين باسم عبد الأمير، **مرجع سابق.**

2 - إيهاب خليفة، القوة الإلكترونية: كيف يمكن أن تدير الدول شؤونها في عصر الأنترنت، **مرجع سابق**، ص. 100.

3 - إيهاب خليفة، "تنامي التهديدات السيبرانية للمؤسسات العسكرية"، **مرجع سابق**، ص.57 .

3 - التضليل والإخفاء والخداع: وهو ما يتحقق عن طريق إخفاء هويات الأهداف الاستراتيجية للدولة على الأنترنت وتضليل الخصم أثناء محاولة الوصول إليها أو اختراقها، من خلال أدوات التمويه والخداع وتغيير ملامح الأهداف الاستراتيجية للدولة، بما يساعد على تضليل الخصم وتشتيت الانتباه عن الهدف الرئيسي[1].

وعلى إثر ذلك قامت كل من روسيا، الصين، "إسرائيل"، بريطانيا، فرنسا، الولايات المتحدة الأمريكية، إيران، كوريا الشمالية بتطوير عقيدتها الأمنية، وأصبحت تعتبر الفضاء السيبراني مسرحا للعمليات العسكرية، كما أوجدت قيادات خاصة ومستقلة لقيادة العمليات السيبرانية[2]، والتي لديها وحدات قتالية خاصة بالحرب السيبرانية، حيث تتميز بقدراتها الهجومية والدفاعية المتقدمة، ولعل أبرز تلك الوحدات القتالية: القيادة السيبرانية الأمريكية (US Cyber Command) والتي استحدثها البنتاغون في شهر جوان 2009، ومهمتها الرد على هجمات قراصنة المعلومات وتنفيذ عمليات في الفضاء السيبراني؛ الوحدة 61398 في الصين والتي تتسم بأنشطتها السرية داخل جيش التحرير الشعبي الصيني، حيث تقوم بعمليات التجسس الإلكتروني وقرصنة المعلومات والبيانات، وقد بدأت في شن أول هجماتها منذ عام 2006؛ قراصنة الظل التابعين للحكومة الروسية وهم من الطلبة المتميزين في استخدام الحاسب الآلي والذين أدمجتهم وزارة الدفاع الروسية في وحدات علمية خاصة، وتجدر الإشارة إلى أن روسيا تمتلك عدد كبير من القراصنة سواء المتطوعين أو الذين تم توظيفهم لخدمة أغراض عسكرية، وقد وظفتهم روسيا عان 2007 بشن هجمات سيبرانية سريعة ومدروسة شاملة على إستونيا أدت إلى دمار لوجستي كبير؛ الوحدة 8200 في "إسرائيل" والمسؤولة عن قيادة الحرب السيبرانية في الجيش الإسرائيلي وتشكل تحالفا مع وكالة الأمن القومي الأمريكية والقيادة السيبرانية الأمريكية، وتعتبر أهم وأكبر قاعدة تجسس إلكترونية إسرائيلية في منطقة "النقب" للتنصت على البث الإذاعي والمكالمات الهاتفية، الفاكس، البريد الإلكتروني في قارات آسيا وإفريقيا وأوروبا، ثم أضيفت إليها مهام الحرب السيبرانية في وقت لاحق، وقت أدت هذه الوحدة دورا رئيسيا في ضرب البرنامج النووي الإيراني من خلال تصميم فيروس "ستاكسنت"، مما جعل "إسرائيل" ثاني أكبر دولة في مجال التجسس والتنصت في العالم بعد الولايات المتحدة الأمريكية[3].

ولذلك تلجأ الدول المتمكنة من القوة السيبرانية إلى اعتماد الدفاع والردع السيبراني في آن واحد، حيث تتمحور أهداف الدفاع الردعي السيبراني في الحفاظ على قدرات الأمن القومي التكنولوجي للدولة، من خطوط اتصالات وشبكة كمبيوتر وبنية تحتية سواء مدنية أو عسكرية، فضلا عن تأمين البيانات الحيوية بما يساهم في النهاية في تحقيق الأمن الإلكتروني للدولة، ويمكن تحديد أهداف الدفاع السيبراني فيما يلي[4]:

---

1 – إيهاب خليفة، "تنامي التهديدات السيبرانية للمؤسسات العسكرية"، **مرجع سابق**، ص. 55.

2 - إسماعيل زروقة، "الفضاء السيبراني والتحول في مفاهيم القوة والصراع"، **مجلة العلوم القانونية والسياسية**، م. 10، ع. 01، (أفريل 2019)، ص. 1026.

3 - إيهاب خليفة، مجتمع ما بعد المعلومات: تأثير الثورة الصناعية الرابعة على الأمن القومي، **مرجع سابق**، ص ص. 151 – 155.

4 - إيهاب خليفة، "تنامي التهديدات السيبرانية للمؤسسات العسكرية"، **مرجع سابق**، ص. 55.

1 - حماية الأهداف العسكرية: والتي تشمل تأمين نظم الإدارة والمراقبة ونظم التحكم والسيطرة ونظم توجيه الأسلحة وقطاع الاتصالات الحربية والأسلحة الآلية القيادة، مثل الطائرات من دون طيار، فضلا عن حماية المنشآت العسكرية والحيوية، مثل محطات الطاقة النووية من أي اختراق سيبراني.

2 - حماية البيانات العسكرية: والتي تشمل معلومات حول أفراد القوات العسكرية كالأسماء والرتب والمرتبات والوظائف داخل الجيش وأماكن الإقامة الشخصية، فضلا عن خطط التسليح وتصميمات الأسلحة، وخرائط انتشار القوات وتوزيع الأسلحة.

3 - حماية البنية التحتية الحرجة: مثل قطاع الاتصالات والمواصلات ومحطات الطاقة وقواعد البيانات الحكومية وخدمات الحكومات الذكية والبنوك والمؤسسات المالية.

4 - دعم وحدات الحرب السيبرانية: وهي تلك الوحدات الخاصة بإدارة الحروب السيبرانية للدولة، حيث تكون مهمة الدفاع السيبراني هي تأمين الخطوط خلف هذه الوحدات، بما يحمي أهداف الدولة الاستراتيجية في حالة شن هجوم سيبراني مضاد عليها، وتوفير غطاء سيبراني للوحدات المقاتلة بهدف التمويه والخداع وصعوبة تعقب مصدر الهجمة.

5 - تحقيق الردع السيبراني: وذلك من خلال رفع تكلفة الهجوم السيبراني للدولة المعتدية، عبر إنشاء نظم دفاع إلكترونية صعبة الاختراق والتي تحتاج إلى وقت وجهد كبير لاختراقها، مع تطوير قدرات تتبع الهجمات السيبرانية واكتشاف مصدرها بما يؤدي في النهاية إلى التأثير على قرارات الخصم وردعه عن شن هجمات سيبرانية على الدولة.

وما يمكن التركيز عليه في هذا المجال هو أن التهديدات الأمنية تبقى محتملة الظهور نتيجة التقدم الهام الذي أحدثته تكنولوجيا المعلومات، والتي تبين هشاشة الأمن الوطني على المدى الطويل خاصة بالنسبة للدول التي تستورد التكنولوجيا وذلك لاحتمال وقوعها في تبعية أمنية للدول التي تستورد منها، لتتحول بهذه التكنولوجيا المتطورة من وسائط تستخدمها الدول لزيادة التحكم في أمنها إلى وسيلة تقحم الدول في تبعية أمنية من جراء التسابق في اقتناء مضادات الفيروسات الإلكترونية وأنظمة منع التشويش، وهو ما يبرر استمرار قطاع الدفاع في الاستثمار ودعم البحوث العلمية وهذا للاستفادة من كل جهد يتم التوصل إليه دون الاعتماد على جبهة مصدرة، وبذلك يسمح البحث والتطوير في المجال العسكري بالتغلب على المفاهيم التقليدية في حماية الشبكات المعلوماتية والإلكترونية[1].

لقد أصبح تأمين الفضاء السيبراني جزءا من استراتيجيات الأمن القومي للعديد من الدول، إذ دفعت التهديدات المتزايدة لأمن هذا الفضاء للعمل على بذل الجهود الجماعي، مثل إنشاء هيئات لمواجهة الطوارئ المعلوماتية "CERT"، أو استحداث قوانين مكافحة الجريمة الإلكترونية، وقد قامت بعض الدول بإنشاء قيادة عسكرية لحماية الفضاء السيبراني واستحداث وحدات للحرب الإلكترونية داخل الجيوش العسكرية والمشاركة في مناورات إلكترونية

1 - رقية العاقل، "دور الثورة المعلوماتية في تطوير الاستراتيجية العسكرية للدول"، **المجلة الجزائرية للدراسات السياسية**، ع. 8، (ديسمبر 2017)، ص. 269.

لتحسين القدرات الدفاعية أمام الهجمات السيبرانية، ومن ناحية أخرى أطلقت منظمات حكومية وغير حكومية العديد من المبادرات، مثل الاتحاد الدولي للاتصالات، الذي أطلق مبادرة للأمن السيبراني (الإلكتروني)، ومبادرة الاتحاد الأوروبي للأمن الإلكتروني، كما تبنت الولايات المتحدة الأمريكية "الاستراتيجية الدولية للفضاء الإلكتروني"، وهي أول وثيقة سياسية من هذا النوع تبين الرؤية الشاملة لمستقبل التعاون الدولي المتعلق بالفضاء السيبراني، ومن ثمة فإنه من الأهمية ربط الأمن الشامل في الفضاء السيبراني ببذل الجهود الدولية العاجلة والمتكافئة لحل الصراعات بين الدول على أرض الواقع لمنع انتقالها إليه، إذ تبرز أيضا أهمية العمل على توفيق القوانين المتعلقة بالصراع والحرب في الفضاء السيبراني مع القانون الدولي، وأهمية المبادرات الدولية لحماية هذا الفضاء، فضلا عن البحث والتطوير في مجال الدفاعات ضد الأخطار الإلكترونية[1] .

ومن ثم أصبحت الاستراتيجيات السيبرانية تصاغ على مستويات مختلفة: الدفاع (المسلح)، والجهات الفاعلة في الدولة المدنية (وزارات العدل والداخلية والصناعة والاتصالات على سبيل المثال)، والجهات الفاعلة الاقتصادية (الشركات)، كما يمكن أن تختلف الاستراتيجيات السيبرانية تبعا لمعايير محددة كمثل:

1 – الثقافة الاستراتيجية التي تعتمد بشكل خاص على المعتقدات المشتركة والتصورات والتاريخ والهوية الجماعية والعلاقة مع الدول الأخرى، ومدى قبول المعايير الدولية، وبالنسبة إلى الدول الصغيرة، تعد الحرب غير المتماثلة جزءً من التاريخ العسكري، فهل ستدخل استراتيجية الدفاع السيبراني بشكل تلقائي في هذا المضمار؟ على العكس، لا يمكن للدول الكبرى اعتماد استراتيجيات غير متماثلة في الفضاء السيبراني.

2 – توصيف التهديدات والتحديات والأولويات.

3 – طبيعة الدولة: دولة كبيرة أو صغيرة، وهل لدى الدول الصغيرة الأهداف نفسها مثل الدول الكبيرة؟ وهل تستطيع الدول الصغيرة المطالبة باستغلال الفضاء السيبراني لمواجهة التحديات نفسها التي تواجهها الدول الكبيرة؟

4 – تأثير الدول المسيطرة: هل صيغت العديد من الاستراتيجيات الوطنية في السنوات الأخيرة على غرار النماذج التي فرضتها الدول المهيمنة؟ وهل يوجد تأثير وانتشار لقواعد ومبادئ تفرضها هذه الدول المهيمنة؟ إن التحليل المقارن للاستراتيجية الوطنية يجب أن يحدد ويحلل ويشرح أوجه الاختلافات والتشابهات القوية، ومن المحتمل أن تتضح من خلال الاستراتيجيات السيبرانية؛ مجموعة العلاقات الدولية وحقائق المشهد الدولي وكذا القيود التقنية.

5 – يعتمد تطوير المعايير الدولية للأمن السيبراني اعتمادا كبيرا على الاستراتيجيات الوطنية الكبرى[2].

وانطلاقا من النقطة الأخيرة؛ فقد حولت الدول بعض موارد الميزانية إلى مبادرات الفضاء السيبراني، حيث وضعت جانبا مبالغ كبيرة خصصتها للبحث وتطوير قدرات الحرب السيبرانية، كما أعلنت حكومات عديدة عن خطط وطنية متكاملة وبدأت تنفيذها للتصدي للتهديدات السيبرانية الجديدة، وتعبئة قطاعات متعددة وتحويل الموارد

1 - عادل عبد الصادق، "القوة الإلكترونية: أسلحة الانتشار الشامل في عصر الفضاء الإلكتروني"، **مرجع سابق**، ص ص. 34 – 35.

2 - جوزيف هينروتين وآخرون، **مرجع سابق**، ص ص. 71 – 72.

والاستراتيجية تحويلا تاما، ويمكن أن يشمل هذا النوع من التحويل تدريب الموظفين العسكريين (أو إعادة تدريبهم)، وتحديث خدمات الاستخبارات للتركيز على جمع المعلومات العلمية والتكنولوجية ذات الصلة وإجراء عمليات محاكاة للحرب السيبرانية، والمناورات العسكرية مع إيلاء اهتمام خاص لتطبيقات تكنولوجيا المعلومات والاتصالات، وقد بادرت دول عديدة إلى إجراء مسابقات وطنية لتحديد أفضل الأذهان (العقول) السيبرانية من بين سكانها المدنيين وتعيينهم، وشجعت الاقتصاديات المحلية على تطوير قدرات تكنولوجية معززة لدعم الاستراتيجية العسكرية الجديدة، وتعكف بعض الحكومات أيضا على إقامة مجموعة من القراصنة المدنيين من القطاع الخاص الذين يمكن اللجوء إليهم عند الحاجة، ويمكن أن تكون هذه الجهات الناشطة في مجال القرصنة، أفرادا متخصصين في مجال التكنولوجيا أو حتى قراصنة سابقين غير شرعيين تم تعيينهم وتدريبهم لاستخدام مهاراتهم لأغراض الأمن الوطني، وقد تلجأ بعض الدول إلى الاستعانة بوكلاء وقراصنة ومتخصصين من دول أخرى يعملون بالنيابة عنها، وتبين هذه التغيرات كلها التحول عن استراتيجيات رد الفعل إزاء التهديدات السيبرانية وإعادة توجيه نحو تطوير نُهج استباقية لحرب المعلومات للعمل بفعالية في ظروف التكنولوجيا العالية[1].

وفي ضوء حقائق العصر المعلوماتي، فإن حروب المستقبل ستعتمد على الذكاء الصناعي في ميدان التسلح العسكري ومنظومات الأسلحة التقليدية، البرية والحرية والجوية والفضائية، لتجعل ميدان المعركة حقيقة صورية وقوة حاسوبية تحدد الأهداف وطريقة معالجتها نظم عرض العمليات ونتائجها، والتقنيات المتعلقة بها، وكما يقول "جيري هاريسون" المدير السابق لمختبرات البحوث والإنماء في الجيش الأمريكي "أن البرمجة وحدها ستسمح بتحديد النتائج الباهرة في حروب المستقبل"، ومن ثمة برز الدور المؤثر للثورة المعلوماتية – الاتصالية في النظرية العسكرية، وذلك بفعل عاملين، الأول تمثل بربط نظم السلاح إلكترونيا، سواء عن طريق الربط المباشر اعتمادا على نظم آلية التحكم في أدائها، أم غير مباشر وذلك باستخدام وسائل الاتصال الحديثة لتمكين مراكز القيادة من القيام بهذا التحكم عن بعد، أما العامل الثاني فقد تمثل في تقليص عامل البعد الجغرافي والفارق الزمني الفاصل بين عمليات الوحدات العسكرية نتيجة زيادة مدى نظم السلاح ومعدلات سرعتها في الإصابة ودقة التهديف[2].

وبما أن الفضاء السيبراني يرتبط بالجغرافية فإنه حسب رؤية الباحثة "ابتسام عبد الزهرة العقبي" وفقا لدراسة قدمتها عام 2018 عنوانها "الصراع الجيوستراتيجي الأمريكي – الروسي في الفضاء الإلكتروني"، فإن الصراع سيكون حسب التطور التكنولوجي، من خلال علاقته بالمجالات الجغرافية التي يغطيها وهي (الأرض- الجو- البحر – الفضاء)، وعليه فإن نتيجة التوجه التكنولوجي تتجه نحو عولمة العالم اقتصاديا وثقافيا وسياسيا وخلق مركز القلب له، ليكون نقطة التحكم والتوجيه في المستقبل، حيث سيدفع إلى وضع نظرية أخرى ستكون قيد التطبيق مستقبلا، وهي تقوم على:

1 - حمدون إ. توريه وآخرون، **مرجع سابق**، ص ص. 80 – 81.

2 - محمد وائل القيسي، **مكانة العراق في الاستراتيجية الأمريكية تجاه الخليج: دراسة مستقبلية**، (بيروت/ الدوحة: الدار العربية للعلوم ناشرون ومركز الجزيرة للدراسات، 2013)، ص ص 151 – 152.

1 - أن من يسيطر على المعرفة ويمتلكها ويتحكم بها، سيسيطر على المجال الخامس (الفضاء السيبراني).

2 - أن من يسيطر على الفضاء السيبراني، سيسيطر ويتحكم في المجالات الجغرافية الأربعة (البر- البحر – الجو – الفضاء).

3 - ومن يسيطر على المجالات الجغرافية الأربعة، سيسيطر على العالم، (والمقصود هنا كل من آسيا وإفريقيا وأمريكا اللاتينية والجنوبية)[1].

وفي إطار التأكيد على أهمية فضاء القوة السيبرانية والذي تعتبر البعد الخامس من فضاءات القوة الاستراتيجية، يؤكد "جوزيف ناي" (Josef S.Nye) من خلال كتابه "مستقبل القوة" (The Future of Power) الصادر عام 2011، على أن؛ القوى الكبرى في العالم ستتعرض لضغوط شديدة لممارسة سيطرتها على المجال السيبراني في الطريقة التي اكتسبت بها التفوق على الجو والبحر والبر[2]

5. الخاتمة:

لقد أصبح الفضاء السيبراني كبديل عن الحروب المباشرة بين الدول، وذلك عبر استخدام شبكات الاتصال والمعلومات وأحدث التقنيات التكنولوجية والتي تتجاوز كل الحدود التقليدية المعروفة بين الدول، كما يعتبر مجالا يسهل من خلاله إلحاق التهديد والضرر بأمن الدول، لذلك تسعى الدول إلى استراتيجيات وأدوات لردع الهجومات الإلكتروني، من أجل تحقيق أمنها السيبراني الذي يكمل سيادتها الوطنية، ومما خلص إليه البحث ما يلي:

1 – لقد فرض الفضاء السيبراني تحديات مختلفة على دول العالم من دون استثناء، كما أوجد حدودا جديدة للقوة بين الدول.

2 – لقد خلق الفضاء السيبراني تهديدات جعلت من باب الالحاح أن تعتد الدول استراتيجيات مصممة لتحقيق الأمن السيبراني الوطني خاصة في ظل التحديات الراهنة.

3 – لقد فرضت الهجمات السيبرانية والجوسسة والاختراقات الإلكترونية على دول العالم فكرة النظر في سيادتها الكاملة، والتي أصبحت منكشفة وفي حالة انكشاف أمني إذا ما تم اختراقها والهجوم عليها.

4 – ستكون الحروب القادمة حروبا في الفضاء السيبراني، لصعوبة تحديد هوية المهاجمين عبره، ولصعوبة حدوث حروب تقليدية مباشرة على أرض الواقع.

5 – ستكون الغلبة في الفضاء السيبراني لمن يملك التقنيات المتقدمة ويتحكم بها بشكل منفرد، ما يجعل من يحقق ذلك يمتلك السيطرة في هذا المجال.

---

3 – إبتسام عبد الزهرة العقبي، "**نظرية قلب الارض بين الجغرافيا والفضاء الالكتروني (رؤية مستقبلية)**"، تاريخ الاطلاع (2021/02/10)، نقلا عن الرابط التالي: https://bit.ly/3ihYN6q

2 - Josef S. Nye, **the Future of Power**, (New York: Public Affairs, 2011), p. 150.

6. قائمة المراجع:

1 – باللغة العربية:

1 – الزويري، محجوب ونصار، يارا، "إيران والهجمات السيبرانية: فصل جديد في الحرب غير المعلنة"، **مجلة رؤية تركية**، م. 09، ع. 04، (خريف 2020).

2 – الشمري، مصطفى إبراهيم سلمان، "الأمن السيبراني وأثره في الأمن الوطني العراقي"، **مجلة العلوم القانونية والسياسية**، م. 10، ع. 01، (جوان 2021).

3 - العاقل، رقية، "دور الثورة المعلوماتية في تطوير الاستراتيجية العسكرية للدول"، **المجلة الجزائرية للدراسات السياسية**، ع. 8، (ديسمبر 2017).

4 – العقبي، ابتسام عبد الزهرة، "**نظرية قلب الارض بين الجغرافيا والفضاء الالكتروني (رؤية مستقبلية)**"، تاريخ الاطلاع (2021/02/10)، نقلا عن الرابط التالي:https://bit.ly/3ihYN6q

5 - القيسي، محمد وائل، **مكانة العراق في الاستراتيجية الأمريكية تجاه الخليج: دراسة مستقبلية**، (بيروت/ الدوحة: الدار العربية للعلوم ناشرون ومركز الجزيرة للدراسات، 2013).

6 – إ. توريه، حمدون وآخرون، **البحث عن السلام السيبراني**، (جنيف: الاتحاد الدولي للاتصالات والاتحاد العالمي للعلماء للطبع، جانفي 2011).

7 – بريوش، نضال ناجي بدوي، "**الصراع السيبراني مع العدو الصهيوني**"، دراسة منشورة مقدمة للحصول على دبلوم الدراسات الفلسطينية من أكاديمية دراسات اللاجئين،2018/2019 .

8 - بونيفاس، باسكال، **الجيوبوليتيك: مقاربة لفهم العالم في 48 مقالا**، (ترجمة: إياد عيسى)، (دمشق: منشورات الهيئة العامة السورية للكتاب، وزارة الثقافة، 2020).

9 - بلعسل بنت نبي، ياسمين وعمروش، الحسين، "التهديدات الإلكترونية والأمن السيبراني في الوطن العربي"، **مجلة نوميروس الأكاديمية**، م. 02، ع. 02، (جوان 2021).

10 - رفيق، عادل، "من فضيحة بيجاسوس إلى فضيحة باراك: دلائل تورط الإمارات"، **سلسلة تقارير سياسية**، المعهد المصري للدراسات، (02 أوت 2021).

11 - زروقة، إسماعيل، "الفضاء السيبراني والتحول في مفاهيم القوة والصراع"، **مجلة العلوم القانونية والسياسية**، م. 10، ع. 01، (أفريل 2019).

12 - خليفة، إيهاب، "تنامي التهديدات السيبرانية للمؤسسات العسكرية"، **مجلة اتجاهات الأحداث**، ع. 22، (جويلية/ أوت 2017).

13 – خليفة، إيهاب، "الصراع الأمريكي – الصيني على التكنولوجيا الفائقة الذكاء"، **مجلة السياسة الدولية**، م. 54، ع. 218، (أكتوبر 2019).

14 - خليفة، إيهاب، **مجتمع ما بعد المعلومات: تأثير الثورة الصناعية الرابعة على الأمن القومي**، (القاهرة: العربي النشر والتوزيع، 2019).

15 - خليفة، إيهاب، **القوة الإلكترونية: كيف يمكن أن تدير الدول شؤونها في عصر الأنترنت**، (القاهرة: العربي للنشر والتوزيع، 2017).

16 - شلوش، نورة، "القرصنة الإلكترونية في الفضاء السيبراني: التهديد المتصاعد لأمن الدول"، **مجلة مركز بابل للدراسات الإنسانية**، م.8، ع.2، (2018).

17 - عبد الأمير، حسين باسم، "**تحديات الأمن السيبراني**"، (17 ماي 2018)، مركز الدراسات الاستراتيجية، كربلاء، العراق، تاريخ الاطلاع (2021/07/05)، نقلا عن الرابط التالي: https://bit.ly/37pinaG

18 - عبد الرزاق، عادل، "القوة الإلكترونية: أسلحة الانتشار الشامل في عصر الفضاء الإلكتروني"، **مجلة السياسة الدولية**، م. 47، ع. 188، (أفريل 2012).

19 - عبد الجواد، أميرة عبد العظيم محمد، "المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام"، **مجلة الشريعة والقانون**، ج، 3، ع. 35، (2020).

20 – علي، علي زياد، **الصراع والأمن الجيوسيبراني في الساحة الدولية: دراسة في استراتيجيات الاشتباك الرقمي**، (عمان: دار أمجد للنشر والتوزيع، 2020).

21 - فرحات، علاء الدين، "الفضاء السيبراني: تشكيل ساحة المعركة في القرن الحادي والعشرين"، **مجلة العلوم القانونية والسياسية**، م. 10، ع. 03، (ديسمبر 2019).

22 - لين، هربرت، "النزاع السيبراني في القانون الدولي الإنساني"، **المجلة الدولية للصليب الأحمر**، م. 94، ع. 886، (صيف 2012).

23 - منصور، شادي عبد الوهاب، **حروب الجيل الخامس: أساليب "التفجير من الداخل" على الساحة الدولية**، (القاهرة: العربي للنشر والتوزيع، 2019).

24 – هينروتين، جوزيف وآخرون، **حرب واستراتيجية: نهوج ومفاهيم (الجزء الثاني)**، (ترجمة: أيمن منير)، (الصفاة/ الكويت: المجلس الوطني للثقافة والفنون والآداب، جوان 2019).

25 - **"ما هو برنامج "بيغاسوس" الإسرائيلي للتجسس .. ولماذا يعد أقوى نظام لاختراق الهواتف في العالم؟"**، (2021/07/20)، سلسلة تحليلات، موقع عربي بوست، (2021/07/31)، نقلا عن الرابط التالي: https://bit.ly/3xDPNNL

26 - **"فضيحة بيغاسوس: شركة إسرائيلية تجسست على صحافيين وقادة دول ومعارضين"**، (2021/07/20)، موقع جريدة الجريدة، تاريخ الاطلاع (2021/07/31)، نقلا عن الرابط التالي: https://bit.ly/3rXSDM1

27 - **"تسرب هائل للبيانات يكشف عن استخدام برمجيات التجسس لمجموعة إن إس أو الإسرائيلية في استهداف النشطاء والصحفيين والزعماء السياسيين على مستوى العالم"**، 18 جويلية 2021، منظمة العفو الدولية، تاريخ الاطلاع (2021/07/25)، نقلا عن الرابط التالي: https://bit.ly/37trYx6

2 – باللغة الأجنبية:

28 – Lu, Marcus, "**Economy Visualized: Where 5G Will Change the World**", 09/03/2020, Visual Capitalist, (22/03/2021), see the link: https://bit.ly/3C8U9jl

29 – S. Nye, Josef, **the Future of Power**, (New York: Public Affairs, 2011).