وزارة التعليم العالي والبحث العلمي

جامعة محمد بوضياف – المسيلة

كليـة الحقـوق والعلـوم السياسيـة

قســـم العلـــــوم السياسيـــــة

ميـدان الحقــوق والعلــوم السياسية

تخصص استراتيجية وعلاقات دولية

مذكرة مقدمة لنيل شهادة الماستر اكاديمي

إعداد الطلب : سليـــم دحمـاني

تحت عنـــــوان

أثــر التهديدات "السيبرانية" على الأمن القومي الولايات المتحدة الأمريكية ــ أنموذجا ــ (2017-2001)

لجنة المناقشة:

د. فـاتح النـور رحمــوني	جامعة محمد بوضياف – المسيلة	رئـــيـــــســا
د. إسماعيــل زروقـــــة	جامعة محمد بوضياف – المسيلة	مشرفـا ومقـــررا
د. إليـــــاس زويـــــن	جامعة محمد بوضياف – المسيلة	منـــاقـــشـــا

السنة الجامعية : 2017-2018م / 1438-1439هـ

مقدمة

أحدثت تكنولوجيا المعلومات والاتصالات ثورة شاملة في جميع نواحي الحياة، فعلى المستوى الاجتماعي كان لها وقع كبير على سلوكيات المجتمع وهويته، وانتشار آليات التشبيك بين المجموعات البشرية متمثلة في وسائل التواصل الاجتماعي، عبر أجهزة الحاسوب والهواتف المحمولة، مما ترتب عنه تغييرات كبرى في مرتكزات اجتماعية كبيرة كالخصوصية، الثقافة، الإعلام، التعارف وبناء العلاقات الاجتماعية.

وعلى المستوى الاقتصادي، ساعدت تكنولوجيا المعلومات والاتصالات على الانتقال السريع نحو الاقتصاد الرقمي المبني على المعرفة، ودخلنا بذلك للعصر الرقمي، إذ يتم استخدام البرمجيات والتطبيقات الذكية لتحقيق نجاحات متعددة في ريادة الأعمال والإدارة، بالإضافة إلى تزايد استخدام الابتكارات التكنولوجية في قطاعات اقتصادية حيوية كالطاقة، السياحة، الخدمات المالية والمصرفية.

وفي المقابل، تزداد المخاطر السيبرانية كلما زادت هيمنة تكنولوجيا المعلومات والاتصالات على النسق العام للحياة، فأصبحنا أمام جرائم حقيقية ومتكاملة الأركان، تتم عن طريق شبكة الإنترنت بأشكال مختلفة، كسرقة الأموال، النصب والاحتيال، التخطيط لعمليات إرهابية، ترويج الأخبار المضللة، وكذلك القرصنة باعتبارها الجريمة الأكثر شيوعاً في العالم الرقمي.

وفي هذا السياق، فإن البحث في قضايا التهديدات السيبرانية والتحديات الأمنية يقتضي الغوص في حيثيات العصر الرقمي الجديد، وتوصيف بيئة هذه التهديدات، حيث إن شبكة الإنترنت تتوفر على أكثر من مليار و700 مليون موقع إلكتروني[1] مع انتشار واسع

[1] حسب إحصائيات موقع Netcraft المتخصص، على الرابط : https://news.netcraft.com
تاريخ الاطلاع: 24-04-2018

للابتكارات بالشبكة، وفي تقرير لمؤسسة "Symantic" لسنة 2018، يتبيّن أن أكثر من 40 مليار جهاز سوف يتحوّل على الإنترنت متمثلة في سيارات ذكية وأجهزة منزلية رقمية[1].

واتصالاً بموضوع التهديدات السيبرانية، تشير عدة تقارير وإحصائيات إلى أن 95% من الشركات الكبرى متعددة الجنسيات تعترف بتعرضها للقرصنة، حيث اتخذت أكثر من 135 حكومة في العالم إجراءات حازمة تخص العالم الافتراضي والأمن الإلكتروني[2]، خاصة مع كثرة الاعتداءات الإلكترونية بين الدول، وأهمها تلك الهجمات المتبادلة بين الولايات المتحدة الأميركية من جهة، والصين وروسيا وإيران وكوريا الشمالية من جهة أخرى، ناهيك عن تزايد عمليات سرقة الملكية الفكرية وقرصنة المنشآت الاقتصادية والتجارية، الجامعات، المعاهد البحثية، والمؤسسات الإعلامية، علاوة على انتشار شبكات الإرهاب السيبراني التي توفر نقاط التلاقي والتنسيق بين التنظيمات الإرهابية وتبادل المعلومات والخبرات.

وعلى هذا النحو، يمكن اعتبار تحدي الأمن السيبراني أعلى تحديات الأمن القومي 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، السياسية والثقافية بين الدول، ما يضع السيادة الوطنية على المحك، خاصة مع اختراق المواقع الحكومية الرسمية والتجسس المعلوماتي على الدول.

كما يبرز التحدي الثقافي والفكري كأحد أهم بوابات التهديدات السيبرانية، وذلك عن طريق الغزو الفكري في شبكات التواصل ونشر ثقافة العنف والإقصاء، والتحريض على الإجرام تحت ذرائع دينية، طائفية أو عصبية، هذا ما يستدعي العناية بالمحتوى الإلكتروني القائم على نشر العلم والتعريف بالحضارات.

---

[1] **Internet Security Threat report**, Symantec, Volume 23, 2018. Accessed at : https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf seen : 02-04-2018

[2] Ibid.

سيعرف مستقبل تكنولوجيا المعلومات والاتصالات تهديداتسيبرانية كبيرة وستتحول شبكة الإنترنت إلى ساحة كبيرة تكثر فيها المخاوف، التهديدات والهجمات، كما ستشكل هذه المخاوف فرصاً استثمارية لمؤسسات الأمن الإلكتروني، الأمر الذي يفرض التعامل مع قضايا الأمن السيبراني بمرونة تامة ومقاربة استباقية.

أهمية الموضوع :

أ. **الأهمية العلمية:** يندرج موضوع البحث ضمن الدراسات الأمنية والإستراتيجية، التي برزت كحقل مركزي في العلاقات الدولية، خاصة بعد نهاية الحرب الباردة، وما عرفته من نقاشات جديدة لتوسيع مفهوم الأمن ليشمل قضايا ومجالات متعددة : سياسية، اقتصادية، اجتماعية، ثقافية، بيئية وسيبرانية.

ب. **الأهمية العملية** :تكمن أهمية الموضوع في التصاعد المطرد للهجمات في الفضاء السيبراني الذي يتوسع يوما بعد يوم، وما لهذه الهجمات من تداعيات سلبية، هذا من جهة، ومن جهة أخرى، فإن الولايات المتحدة الأمريكية تعد النموذج الأمثل لدراسة التهديدات السيبرانية، كونها مهد الشبكات والانترنيت، وتمتلك أقوى الشركات التكنولوجية، مما يجعلها هدفا كبيرا لمجمل التهديدات والهجمات السيبرانية في العالم.

أهداف الدراسة :

- إبراز وتوضيح المفاهيم الجديدة في الفضاء السيبراني.
- توضيح العلاقة بين الأمن السيبراني والأمن القومي علاقة التأثير والتأثر.
- إبراز إسهامات وجهود الدول وخاصة الولايات المتحدة الأمريكية في مواجهة التهديدات السيبرانية.

مبررات اختيار الموضوع :

أ. **الأسباب الموضوعية:** تسعى الدراسة لتقديم تصور تحليلي للتهديدات السيبرانية وانعكاسها على الأمن القومي للدول من خلال توضيح السياسات السيبرانية الأمريكية كدولة رائدة في مواجهة هذه التهديدات.

ب . **الأسباب الذاتية:** تكمن المبررات الذاتية في رغبة الباحث كونه خبير كمبيوتر ومهتم بالتطورات التكنولوجية، إلى تنوير القارئ العادي والباحث على حد سواء، بالخطورة الخفية التي تحملها التكنولوجيا إذا استعملت دون أخذ احتياطات أمنية صارمة، إضافة إلى إثراء الجانب العلمي والمعرفي باللغة العربية.

إشكالية الدراسة :

في عصرنا الرقمي، تتزايد أعداد ومخاطر التهديدات السيبرانية، وتتباين آثارها وانعكاساتها في العالم عامة، وفي الولايات المتحدة الأمريكية خاصة، حيث امتدت هذه التهديدات لتطال مختلف القطاعات سواء العسكرية، السياسية، الاقتصادية، الاجتماعية و الثقافية مهددة بذلك الأمن القومي للدول، وبناء عليه، نطرح السؤال البحثي المركزي التالي :

كيف تؤثر التهديدات السيبرانية على الأمن القومي للولايات المتحدة الأمريكية؟

وتندرج ضمن السؤال البحثي المركزي الأسئلة الفرعية التالية :

1. كيف أثر الفضاء السيبراني على مفاهيم الأمن، القوة، الصراع، والحرب؟
2. ماهي مظاهر التهديدات السيبرانية؟ وما علاقتها بالأمن القومي؟
3. وما هي الآليات المتبعة لمعالجتها؟
4. كيف تعاملت الولايات المتحدة الأمريكية مع التهديدات السيبرانية؟

فرضيات الدراسة :

1. حدثت تغييرات كبيرة في مفاهيم الأمن، القوة، الصراع، والحرب بفعل تأثير الفضاء السيبراني.
2. كلما زادت شدة التهديدات السيبرانية كلما كان التهديد للأمن القومي كبيرا.
3. زيادة التنسيق والتعاون بين الدول في الفضاء السيبراني يقلل من مخاطر التهديدات السيبرانية.
4. قامت الولايات المتحدة بمجهودات كبيرة في المجال التقني والقانوني لمواجهة التهديدات السيبرانية.

الإطار المنهجي للدراسة :

المنهج الوصفي : يقوم المنهج الوصفي على تفسير ظاهرة التهديدات السيبرانية، وتحديد خصائصها،بالإضافة إلى وصف طبيعة ونوعية العلاقة بين الأمن السيبراني والأمن القومي، من خلال جمع البيانات الوصفية حول واقع التهديدات السيبرانية في العالم بشكل عام، والولايات المتحدة الأمريكية بشكل خاص، وصولا إلى تحليل وتفسير هذه البيانات.

منهج دراسة الحالة : وقد استخدم في الفصل الثالث من الدراسة، من خلال اعتماد الولايات المتحدة الأمريكيةكنموذج، لنوضح من خلاله مدى تأثير التهديدات السيبرانية على الأمن القومي الأمريكي ورصد أهم الحالات والأضرار الناجمة عن هذه التهديدات.

نهج تحليل المضمون: لتفسير مضامين أهم الخطابات والوثائق الرسمية والاتفاقيات الدولية لمواجهة التهديدات السيبرانية.

حدود الدراسة :

الإطار الزماني : شملت الدراسة في مجالها الزمني مراحل متعددة بداية من مرحلة ما بعد أحداث11 سبتمبر 2001، التي شكلت بداية التحول الجذري في مفاهيم الأمن، وتزامنت مع ظهور وانتشار التهديدات السيبرانية على المستوى الدولي، كما ركزت الدراسة على مرحلة ما بعد 2010 وظهور فيروس" STUXNET" الذي حول التهديد السيبراني من مجرد القرصنة وسرقة المعلومات إلى مهاجمة البنى المادية ذاتها ومحاولة تدمير الأجهزة.

الإطار المكاني : الفضاء السيبراني ، مع التطرق إلى الولايات المتحدة الامريكية كدراسة حالة.

أدبيات الدراسة:

1. **كتاب :** Richard A. Clarke & Robert knake, **Cyber War: The NextThreat to National Security and What to Do About It**, HarperCollins, 2010.

ويتناول الكتاب التعريف بمصطلح "حرب الفضاء الإلكتروني"، كما يقدم الكاتب خصائص الحروب السيبرانية، ويخلص إلى أن معظم الحروب الفعلية التقليدية في المستقبل ستصاحبها حروب فضاء سيبراني، كما يعرج على إنشاء الولايات المتحدة الأمريكية قيادة عسكرية جديدة تُعرف بقيادة حرب الفضاء السيبراني، وتتركز مهمتها في استخدام الإنترنت كسلاح للحرب.

كما يشير الكاتب إلى أن دولاً عدة في العالم أخذت تركز على تطوير قدرات حرب الفضاء السيبراني، كروسيا والصين التي يعتبرهما التهديد الأكبر للولايات المتحدة في مجال الفضاء السيبراني، ليخلص في الأخير، أنه على الولايات المتحدة مراجعة موقفها بشأن ضبط التسلح السيبراني، والتفكير في الفائدة التي يمكن أن تجنيها من خلال الاتفاقيات الدولية.

2. **كتاب:القوة الإلكترونية.. كيف يُمكن أنْ تدير الدول شؤونها في عصر الإنترنت، إيهاب خليفة، دار العربي ، 2016.**

يناقش الكتاب، التغيرات التي طرأت على مفهوم القوة في العصر الرقمي، وكيفَ ظهرت القوة السيبرانية، وتحديد عناصرها، وتعامل الولايات المتحدة الأمريكية مع الفضاء السيبرانيمن حيث المصالح والتهديدات.

ويَتطرق إلى الفواعل فيالفضاء السيبراني، ويعطى نماذج عملية على قيام دول مثل الولايات المتحدة والصين وإسرائيل وروسيا بإنشاء جيوش من هؤلاء القراصنة للقيام بإدارة الحروب عبر الفضاء السيبراني.

3. **كتاب :الفضاء الالكتروني والعلاقات الدولية :دراسة في النظرية والتطبيق ، عادل عبد الصادق، المكتبة الأكاديمية، القاهرة، 2016.**

يتناول الكتاب في مقدمته حقيقة تصاعد البعد التكنولوجي في العصر الراهن، والذي من اهم إرهاصاته ظاهرة الفضاء السيبراني كمجال جديد في العلاقات الدولية، وتأثيره فيها على مستوى النظرية والتطبيق، فيما يعرف بالسياسات السيبرانية، حيث تم المزج بين العلوم السياسية والفضاء السيبراني، وهو ما عمل على إعادة تشكيل المفاهيم الجديدة ويعتبر تحديا للمعرفة التقليدية .

وتناول المؤلف ظاهرة الفضاء السيبراني وإشكاليات نظرية العلاقات الدولية، حيث يرصد تأثير الفضاء السيبراني في التغير في البنية والهيكل والفاعل في النظام الدولي، وعلاقات القوى والتأثير في سيادة الدولة وتصاعد دور الفرد و دور المجتمع المدني العالمي ودور الجماعات الإرهابية في العلاقات الدولية.

ويتناول الباحث في هذه الدراسة ظاهرة مهمة في العلاقات الدولية، وهي أثر التهديدات السيبرانية ككل، بما فيها الحروب السيبرانية على الأمن القومي، حيث يركز على الولايات المتحدة الأمريكية، خلال الفترة 2001-2017، كما يعالج سبل مواجهة هذه التهديدات.

مصطلحات الدراسة:

السيبرانية* : مشتقة من كلمة " سايبرCyber" وتعني : كل ما يتعلق أو يرتبط بالحواسيب وتكنولوجيا المعلومات والواقع الافتراضي، أصل الكلمة يوناني،**Kybernetes** وتعني القيادة أو التوجيه، ومصدرها **Cybernetics** الذي يعني : "علم الاتصالات وأنظمة التحكم الآلي في كل من الآلات والأشياء الحية"[1].

الإنترنت العميق(The Deep Internet) : مجموع المواقع الإلكترونية التي لم تدرج في محركات البحث، بعضها أسواق ،تمكن من شراء أو التوسط في شراء المخدرات والأسلحة والبيانات المخترقة،كما تمكن من التعاقد مع الخدمات الرقمية أو الجنائية، مثل هجمات تعطيل الخدمة، أو حتى قتلة محترفين[2].

ستكسنت "Stuxnet": عبارة عن برنامج كومبيوتر خبيث يهاجم أنظمة التحكم الصناعية المستخدمة على نطاق واسع في مراقبة الوحدات التي تعمل آليا، يقوم بعد اختراق الأجهزة والحواسيب بالتفتيش عن علامة شركة "سيمنز الألمانية"، ليبدأ بالعمل على تخريب وتدمير المنشأة المستهدفة ، البرنامج مشفّر جيدا ومعقد، ويوظّف تقنيات ذكية وجديدة[3].

---

* يستعمل الباحث في الدراسة مصطلح "السيبرانية"، وذلك لعدم وجود إتفاق على ترجمة عربية للمصطلح الانجليزي "Cyber"، إضافة إلى ورود المصطلح في الترجمة العربية للوثائق الدولية.

[1] **معجم أكسفورد**، على الرابط : https://en.oxforddictionaries.com/definition/cyber

[2] **الانترنيت المظلم أرض الخدمات المخفية**، مؤسسة إيكان، على الرابط : https://www.icann.org/news/blog/ar-421519a4-57e7 تاريخ الاطلاع : 28-04-2018.

[3] **المجال الخامس.. الحروب الإلكترونية في القرن الـ21**، مركز الجزيرة للدراسات، على الرابط http://studies.aljazeera.net/ar/issues/2010/20117212274346868.html تاريخ الاطلاع : 25-04-2018.

البنية القومية للمعلومات: عملية ربط البنى التحتية للدولة في بيئة عمل تشابكية واحدة، وتتكون من شبكات الاتصالات ، والخدمات التفاعلية ، والأجهزة والبرامج الحاسوبية القابلة للتشغيل المتبادل ، وأجهزة الكمبيوتر ، وقواعد البيانات ، والإلكترونيات استهلاكية من أجل توفير كميات هائلة من المعلومات لكل من القطاعين العام والخاص.

الخادم (Server):نظام كمبيوترمتصل بشبكة حواسيب، ومتخصص في أداء وظيفة محددة وتلبية الطلبات التي ترده من حواسيب أخرى على الشبكة،له إمكانات متفوقة وتصميمات خاصة لتحمل العمل لفترات طويلة[1].

أنونيموس (المجهولون): مجموعة غير مركزية من القراصنة المنتشرين في العالم، ذات ثقل كبير في الحروب السيبرانية، وتعني كلمة(Anonymous)المجهول، سربت آلافا من رسائل البريد الإلكتروني الخاصة بالرئيس السوري بشار الأسد، واخترقت مواقع حكومية أميركية وبريطانية وتركية وإسرائيلية، شعارها : "لن نسامح، لن ننسى ... احذرونا"، لهم عدة عمليات مشهورة، من بينها دعمهم لموقع "ويكيليكس"[2].

تقسيم الدراسة:

قسمنا الدراسة الى ثلاثة فصول رئيسية كما يلي:

الفصل الأول:تحت عنوان الإطار النظري والمفاهيمي للدراسة، حيث قمنا بتأصيلاتمفاهيمية ونظرية حول تطور مفهوم الأمن القومي والفضاء السيبراني، وكيف حدث إعادة تشكيل لمفاهيم القوة والصراع، كما تم التطرق إلىمفهوم الأمن السيبراني والتهديدات السيبرانية.

---

[1] **أنواع خوادم الشبكة**، على الموقع :http://www.networkset.net/2014/02/19 تاريخ الاطلاع : 2018/04/21.

[2] **أنونيموس**، موسوعة الجزيرة، على الموقع : http://www.aljazeera.net/encyclopedia/movementsandparties تاريخ الاطلاع : 20-04-2018

الفصل الثاني:والمعنون بـ: مظاهر تأثير التهديدات السيبرانية على الأمن القوميوآليات مواجهتها، وعالج العلاقة بين الأمن السيبراني والأمن القومي، مع إبراز أهم التهديدات السيبرانية الجديدة، وتتبع جهود الدول لمواجهة التهديدات السيبرانية.

الفصل الثالث:المعنون بـ: الولايات المتحدة الأمريكية بين الدفاع والهجوم السيبراني، وتم التركيز فيه على انعكاسات التهديدات السيبرانية على الأمن القومي الأمريكي، والسياسة السيبرانية التي وضعتها الولايات المتحدة الأمريكية واستراتيجية المواجهة، وانتهى الباحث إلى استشراف مستقبل الأمن السيبراني الأمريكي.

الفصل الأول:

الإطار النظري والمفاهيمي للدراسة

الفصل الأول:

الإطار النظري والمفاهيمي للدراسة

يتناول هذا الفصل دراسة الادبيات التي تناولت الأمن القومي والفضاء السيبراني، للبحث في العلاقة الارتباطية بينهما، هذه العلاقة أدت إلى تحولات في مفاهيم أساسية في الدراسات الأمنية كمفهومي القوة والصراع، مما أدى إلى تطور مفهوم الأمن، و ظهور الأمن السيبرانيالذي جاء كنتيجة حتمية للتهديدات السيبرانية الجديدة التي ظهرت على الساحة العالمية.

وفي هذا الإطار يقسم الفصل إلى ثلاثة مباحث كالتالي :

المبحث الأول : تطور مفهوم الأمن القومي.

المبحث الثاني :الفضاء السيبراني والتحول في مفاهيم القوة والصراع.

المبحث الثالث :مفهوم الأمن السيبراني والتهديدات السيبرانية.

المبحث الأول:تطور مفهوم الأمن القومي.

يتم في هذا المبحث دراسة الأسباب التي أدت إلى زيادة الاهتمام بالأمن القومي الذي أصبح فرعاً جديداً في العلوم السياسية، واستعراض التعريفات المختلفة التي أوردها الباحثون للمفهوم،كما تمت دراسة عوامل تهديد الأمن، وسماته، ومن ثم توضيح النظريات أو المدارس الأساسية التي عالجت القضايا الأمنية.

المطلب الأول: الأمن القومي جدلية المفهوم.

أولا : تطور ظاهرة الامن القومي.

نشأتوتطورت الظاهرة الأمنية في سياق الوجود الإنساني منذ القدم، حيث أعتبر الأمن شرطا مهما في البناء الحضاري، ومع تطور التنظيم الدولي ونشأة الدولة القومية تطورت الظاهرة الامنية، حيث تبلورت فكرة الامن القومي بالتلازم مع نشأة الدولة القومية،وخاصة بعد معاهدة **وستفاليا** عام 1648 التي أسست لولادة الدولة القومية أو الدولة – الأمة.

ومن ابرز النظريات التي تفسر نشأة الدولة وتربطها بالمتغير الأمني نجد **هوبز** الذي يميز بين حالة المجتمع وحالة الطبيعة، فالبحث عن الأمن دفع البشر إلى الانخراط في مجتمعات من خلال عقد اجتماعي تتخلى بموجبه عن حريتها لصالح سلطة مركزية مشتركة[1].

يتفق العديد من الباحثين على الحداثة النسبية للدراسات المتعلقة بظاهرة الأمن القومي كظاهرة علمية، حيث قامت بالتزامن مع الظروف السياسية والعسكرية التي أعقبت الحرب العالمية الثانية، والتوازنات التي أفرزتها بين القوى الدولية من بروز قوى جديدة،

[1] سليمان عبد الله الحربي، **"مفهوم الأمن: مستوياته وصيغه وتهديداته (دراسة نظرية في المفاهيم والأطر)"**،المجلة العربية للعلوم السياسية، العدد 19، 2008 ، ص 10.

ومن تغير في هيكل النظام الدولي ومستوى القوة في قيادته، كما أرتبط الاهتمام الفكري بالظاهرة بالعنف السياسي على المستويين الدولي والقومي، وبما ان الدولة هي الوحدة الرئيسية التي يقوم عليها النظام الدولي فإن الظاهرة ارتبطت بخصائص هذا النظام ومقومات الدول المشكلة له.

يعود استخدام مفهوم الأمن القومي لأول مرة في نهاية الحرب العالمية الثانية، حينما أنشئ مجلس الأمن القومي الأمريكي عام 1947، ومنذ ذلك الحين انتشر استخدام المفهوم بمستويات متعددة ومختلفة، كما ارتبط المفهوم في بدايات تعريفه بالقدرة العسكرية، حيث اعتبر**والتر ليبمان Walter Lippmann** أن الدولة الآمنة هي التي لم تبلغ الحد الذي تضحي بقيمها إن أرادت أن تتجنب الحرب، فأمن الدول حسبه مساو للقوة العسكرية ومرادف للحرب[1].

لكن تطور المفهوم ولم تعد القوة العسكرية هي التهديد الرئيس للأمن، بل ظهرت تهديدات جديدة اقتصادية واجتماعية وسياسية وغيرها، مما دعى الباحثين إلى الدعوة لبناء مفهوم موسع للأمن، حيث سعى **باري بوازن Buzan Barry** إلى إيجاد أبعاد أمنية جديدة تتضمن الجوانب السياسية، والاقتصادية، والاجتماعية، والبيئية.

كما يرى البعض الآخر، أن ظاهرتي العولمة والتفكك تدعو إلى الاهتمام بالأمن المجتمعي، فالعولمة في محصلتها ستقوض أساس الدولة القومية، وتفكك الدول سبب مشكلات تتعلق بالحدود والأقليات الدينية، مما يدعو لمراجعة فعلية لمفهوم " الأمن القومي".

[1] نسيم بهلول، **فهم الأمن القومي الجزائري من مدخلي الأمن الوطني والدفاع الوطني**، دار حامد للنشر والتوزيع، عمان، 2015، ص 37.

ثانيا : تعريف الأمن القومي.

1- التعريف اللغوي للأمن: الأمن في اللغة هو نقيض الخوف، والفعل الثلاثي "أمِن" أي حقق الأمان، وقد ورد المفهوم في القرآن الكريم، في سورة "قريش" بقوله تعالى: "فليعبدوا رب هذا البيت الذي أطعمهم من جوع وآمنهم من خوف".

2- التعريف اللغوي للقومية:

المادة اللغوية لكلمة القومية هي **(ق.و.م)**، والقوم هم الجماعة التي ترتبط بمكان ما وتقيم فيه، وفكرة القومية قديمة قدم الاجتماع البشري، وقد عبّر عنها ابن خلدون بفكرة العصبية، وعناصر القومية هي الأرض المشتركة، والتاريخ، والثقافة المشتركة، والمصالح المشتركة.

3- أهم تعريفات الأمن القومي:

على الرغم من استخدامه على نطاق واسع، فإن مفهوم "الأمن القومي" يعني أشياء مختلفة لأشخاص مختلفين،ويعترف المفكرون بغموض وتشابك مفهوم الأمن، حيث يعتبر **دانييل كوفمن وآخرون** في كتابهم **الأمن القومي الهيكل التحليلي** أن "مصطلح الأمن يتسم بالغموض وشدة الاختلاف في المعنى من مجتمع لآخر بحسب ثقافته وموقعه"[1].

وفي ذلك يرى **باري بوزان** أنه مفهوم معقد، ينبغي لتعريفه الإحاطة بثلاثة أمور على الأقل هي[2]:

- السياق السياسي لمفهوم الأمن.
- الأبعاد المختلفة للأمن.
- الغموض والاختلاف الذي يرتبط به عند تطبيقه في العلاقات الدولية.

[1] جمال معين مظلوم ، **الأمن غير التقليدي** ، جامعة نايف العربية للعلوم الأمنية، الرياض، 2012، ص 15.
[2] سليمان عبد الله الحربي ، **مرجع سابق**، ص 10.

لقد ارتبط الأمن في المنظور التقليدي بكيفية استعمال الدولة لقوتها لإدارة الأخطار التي تتهدد وحدتها الترابية، واستقلالها، واستقرارها السياسي، وذلك في مواجهة الدول الأخرى بالاعتماد على القوة في شقها العسكري، ويعود ذلك إلى أن الدراسات الأمنية تطورت في إطار المدرسة الواقعية التي كانت ظروف الحرب الباردة مواتية لها لاحتكار هذا الحقل المعرفي.

وهنا نورد بعض التعريفات للأمن من المنظور التقليدي:

1. **تعريف الموسوعة السياسية:** "الأمن القومي هو ما تقوم به الدول للحفاظ على سلامتها ضد الأخطار الخارجية والداخلية التي تؤدي بها إلى الوقوع تحت سيطرة أجنبية نتيجة ضغوط خارجية أو انهيار داخلي"[1].
2. **تعريف دائرة المعارف البريطانية:** "الأمن هو حماية الدولة من السيطرة عليها بواسطة قوى أجنبية"[2].
3. **تعريف والتر ليبمان Walter Lippman:**"إن الأمة تبقى في وضع آمن إلى الحد الذي لا تكون فيه عرضة للتضحية بالقيم الأساسية، إذا كانت ترغب بتفادي وقوع الحرب وتبقى قادرة– لو تعرضت للتحدي– على صون هذه القيم عن طريق انتصارها في حرب كهذه"[3].

في السياق ذاته، قدم **آرنولد ولفرز Arnold Wolfers** تعريفا للأمن يتقاطع وتعريف "**ليبمان**": "يقدر الأمن بالمعنى الموضوعي بغياب التهديدات للقيم المكتسبة وبالمعنى الذاتي بغياب الخوف من أن هذه القيم ستهاجم".

---

[1] عبد الوهاب الكيالي وآخرون، **موسوعة السياسة**، الجزء الأول، ط3، المؤسسة العربية للدراسات والنشر، بيروت 1990، ص33.

[2] احمد فريجة، لدمية فريجة، **"الأمن والتهديدات الأمنية في عالم ما بعد الحرب الباردة"**،مجلة دفاتر السياسة والقانون، العدد 14، ورقلة، 2016.

[3] جون بيليس، **الأمن الدولي في حقبة ما بعد الحرب الباردة**، في: جون بيليس، ستيف سميث، **عولمة السياسة العالمية**، مركز الخليج للأبحاث، الإمارات العربية المتحدة، 2004، ص414.

إن التعريفات السابقة للأمن، وفي ضوء التطورات المتزايدة على الصعيد العالمي خاصة المتعلقة منها ببروز عمليات التكامل والتعاون الدولي، وازدياد نفوذ المؤسسات والشركات الدولية، كفاعلين جدد على الساحة العالمية، تعرضت لانتقادات عديدة أهمها أن الأمن لم يعد يقتصر على أمن الدول فحسب، كما لم يعد متعلقا بالإعدادات العسكرية لهذه الأخيرة، وهو ما أفسح المجال لإدراج أبعاد لا تقل أهمية وتأثيرا عن البعد العسكري في تحديدها لمفهوم الأمن،ويعد كتاب "**روبرت مكنمارا**" "**Robert Mcnamara**" "**جوهر الأمن**" تأسيسا لبعد جديد للأمن مفاده أن:" إن الأمن هو التنمية وبدون التنمية لا يمكن الحديث عن الأمن"[1].

أما "باري بوزان" "**Barry Buzan**" فعرّف الأمن بقوله: "في حالة الأمن يصبح النقاش حول مسعى التحرر من التهديد، وإذا نقلنا النقاش إلى النظام، يصبح الأمن متعلقا بقدرة الدول والمجتمعات على الحفاظ على هويتها المستقلة وتكاملها الوظيفي"[2].

ثالثا : سمات الأمن القومي.

يتسم الامن بثلاث صفات رئيسية تتمثل في :

أولا : التغير،فهو حقيقة متغيرة تبعا لظروف الزمان والمكان، وفقا لاعتبارات داخلية وخارجية، فمفهوم الأمن ليس مفهوما جامدا، بل مفهوم ديناميكي يتطور بتطور الظروف، ويرتبط ارتباطا وثيقا بالأوضاع والمعطيات والعوامل المحلية والاقليمية والدولية، فالأمن حالة حركية (ديناميكية) مركبة لا تتصف بالجمود[3].

ثانيا: النسبية، فالأمن حقيقة نسبية وليست مطلقة، فالنسبية هنا تنشأ من السعي المستمر للدول إلى زيادة قوتها، وهو ما يزيد شعورها بعدم الأمن بدلا من تحقيقه، وهذا ما يجعلها لا تقف عند مجرد تحقيق التوازن بل تسعى الدول إلى تحقيق التفوق والهيمنة، فالعلاقات

[1] عبد الجليل زيد المرهون، **أمن الخليج وقضية التسلح النووي**، المنامة: مركز البحرين للدراسات والبحوث، 2007، ص6.

[2] احمد فريجة، لدمية فريجة، **مرجع سابق.**

[3] سليمان عبد الله الحربي ،**مرجع سابق**، ص 10

الدولية تشوبها حالة من عدم اليقين وانعدام الثقة وهو ما يطلق عليه الواقعيون مصطلح "**المعضلة الأمنية**".

ثالثا : الأمن مفهوم مركب، متكامل، يحمل مضمونه معاني غامضة وواضحة، حقيقية ومضللة في آن واحد، فهناك مفهوم ضيق وآخر واسع للأمن، فالأول يتضمن الإجراءات الخاصة بتأمين الأفراد داخل الدولة ضد الأخطار المحتملة، ومن جهة ثانية يشمل مفهوم الأمن كل ما يحقق الاستقلال السياسي للدولة، وسلامة أراضيها، وضمان الاستقرار السياسي والاقتصادي والاجتماعي، فهو يشمل تحقيق الأمن ببعديه الداخلي والخارجي، فجوانب الامن مرتبطة ارتباطا وثيقا، فالأمن كل مركب ومتكامل لا يتجزأ[1].

المطلب الثاني: دراسات الأمن القومي.

انطلاقاً من نسبية الأمن القومي، على المستوى النظري كمفهوم، وعلى المستوى العملي كإطار استراتيجي، تعددت المدارس والاتجاهات في تحليل ماهية الأمن القومي،نذكر فيما يلي أهم الاتجاهات في الدراسات الامنية :

أولا:الاتجاه الاستراتيجي (التقليدي) للأمن القومي:

ينظر أصحاب هذا الاتجاه إلى الأمن القومي كقيمة استراتيجية مجردة، يرتبط بقضايا السيادة والاستقلال، ومصالح الدول وكيانها وقيمها الوطنية، وفي بعده الواقعي ينطلق من أن الدولة هي الفاعل الرئيسي فيالنظام الدولي الذي يتسم بالفوضوية، وأولوية الأمن القومي على غيره من مستويات الأمن، وتقدم البعد العسكري على غيره من الأبعاد باعتباره من قضايا السياسة العليا، ولذلك تتولى الدول قضية الأمن بنفسها، وتدافع عن مصالحها، وذلك من خلال امتلاك وزيادة القوة وكذلك استخدامها.

[1] فاتح النور رحموني، **محاضرات الإستراتيجية والأمن الدولي**، ألقيت على طلبة الماستر، قسم العلوم السياسة، جامعة المسيلة ، 2017-2018، ص5.

كما اعتبرت المدرسة الواقعية أن القوة العسكرية عامل رئيسلتحقيق أمن الدولة، ولأنخيار الحرب على الصعيد التكتيكي أو الاستراتيجي ما يزال قائماً، أقامت هذه المدرسة علاقة ترابط بين الأمن والقدرة العسكرية[1].

وتتمثل أهم عناصر مفهوم الأمن القومي لدى النظرية الواقعية فيما يلي[2]:

– أن مفهوم الأمن يرتبط بالقدرة العسكرية للدولة، كما يرتبط بمفهومي الردع والقوة.

– أن التهديدات التي تواجه الدولة ذات طابع عسكري بالأساس ومصدرها خارجي.

– أن مسئولية تحقيق الأمن تتولاها الجيوش وأجهزة المخابرات التابعة للدولة.

ومن أبرز المفكرين الذين ساهموا في ترسيخ مفهوم الامن وفق هذا الاتجاه، **ولتر ليبمان، أرنولد وولفرز، هانس مورغانثاو، كينيث ولتز** وغيرهم.

ثانيا:الاتجاهالتنموي (الحديث) للأمن القومي:

مع بروز عمليات التكامل والتعاون وبروز المؤسسات والشركات الكبرى كفاعلين جدد على الساحة الدولية، توسع مفهوم الأمن ليشمل أبعادا أخرى غير البعد العسكري، ليشمل كما يرى الليبراليون المسائل الاقتصادية والاجتماعية والثقافية، وفي هذا السياق يرى **روبرت مكنمارا Robert McNamara** في كتابه "**جوهر الأمن**" أن الأمن مرتبط بالتنمية، حيث يقول: " إن الأمن ليس هو المعدات العسكرية، وإن كان يتضمنها، والأمن ليس القوة العسكرية، وإن كان يشملها، ... ، إن الأمن هو التنمية، ومن دون تنمية لا يمكن أن يوجد أمن"[3].

---

[1] أمينساعاتي،**الأمنالقومي العربي** ، المركز السعودي للدراسات الإستراتيجية،القاهرة،1993.

[2] علاء عبد الحفيظ، **العلاقة بين الأمن القومي والديمقراطية**، رسالة دكتوراه في الفلسفة غير منشورة، قسم العلوم السياسية، جامعة القاهرة ، 2009، ص 50.

[3] سليمان عبد الله الحربي، **مرجع سابق**، ص 17.

فالأمن حسب هذا الاتجاه أكثر شمولا وتماسكا، وله أطر داخلية وخارجية متعددة ومتكاملة، فهو يركز على أمن الأفراد والمجتمعات وليس الدولة فقط، فأمن الدولة هو نتاج لأمن مواطنيها، فمحوره عند النقديين هو الأمنالإنساني (حق الإنسان في حياة كريمة)، والأمن المجتمعي كما ينادي به البنائيون (استقرار المجتمع وحفاظه على هويته)، ومن المفكرين الذين ساهموا في ترسيخ مفهوم الأمن التنموي الشامل (المجتمعي–الهوياتي، الإنساني) نجد **باري بوزان، اولي ويفر، روبرت كوكس** وغيرهم.

وتأسيسا على ماسبق، نرى سيطرة الفكر الواقعي على الدراسات الأمنية، حيث طورت الوعاء الفكري الخاص بالدراسات الأمنية، بيد أنها تعرضت للتحدي بعد التغيير في هيكل النظام الدولي، وبروز فواعل جديدة، وعمليات التكامل والتكتلات الاقتصادية، مما أدى إلى إضعاف دور الدولة القومية والقوة العسكرية، ذلك ان النمو الاقتصادي، وعمليات الاعتماد المتبادل، والثورة التكنولوجية غيرت مفاهيم الأمن، وقدمت مفاهيم جديدة للحرب مثل حرب الفضاء وحروب الشبكات، لكن أحداث 11 سبتمبر أعادت من جديد سيطرت الفكر الواقعي التقليدي على مفاهيم الأمن وأبعاده بشكل كبير.

المطلب الثالث: مهددات الأمن القومي.

أولا: مفهوم التهديدات الأمنية:

إن العلاقة بين مفهومي "الامن" و "التهديد" علاقة تأثير متبادل، وأي محاولة لتفسير الأمن لابد أن تبدأ بتحديد مصادر التهديد، ولقد ركزت الدراسات الأمنية في السابق على خطر الغزو العسكري، باعتباره أهم مصادر تهديد الأمن، بيد أن الدراسات الحديثة ذهبت إلى وجود مصادر أخرى للتهديد، تتمثل في التهديدات السياسية والاقتصادية والاجتماعية والبيئة ببعديها الداخلي والخارجي.

"التهديد" في مفهومه الاستراتيجي هو بلوغ تعارض المصالح والغايات القومية مرحلة يتعذر معها إيجاد حل سلمي يوفر للدول الحد الأدنى من امنها السياسي والاقتصادي والاجتماعي والعسكري، مقابل قصور قدراتها لموازنة الضغوط الخارجية، الأمر الذي قد يضطر الأطراف المتنازعة إلى اللجوء إلى استخدام القوة العسكرية، معرضة الأمن القومي لأطراف أخرى للخطر[1].

ثانيا : تصنيفات التهديدات الأمنية :

وتعتبر عملية تصنيف مهددات الأمن القومي أمرا مهما، إذ هناك ثلاث مفاهيم متداخلة عند تحديد ما يعانيه الأمن القومي من مشاكل وهي : التحديات، المخاطر والتهديدات.

- **التحديات** : وهي المشاكل والصعوبات التي تواجه الدولة وتحد أو تعوق من تقدمها، وتشكل حجرة عثرةأمام تحقيق أمنها واستقرارها ومصالحها الحيوية الذاتية المشتركة ويصعب تجنبها أو تجاهلها"[2].
- **المخاطر** :يرى **ألريش بيك Ulrich Beck** في كتابه "**مجتمع الأخطار**" أن " الخطر عبارة عن ضرر يهدد أمن الأفراد والبيئة والجماعات البشرية، لكنه يوشك أن يحدث أو حدث فعلاً ويمكن احتواءه إن لم يتفاقم"[3].
- **التهديد** :عرفه **باري بوزان** على أنه: "تهديد لمؤسسات الدولة باستخدام الإيديولوجيا أو استخدام مكونات القدرة لدولة ضد دولة أخرى، حيث يمكن أن يكون إقليم الدولة مهدداً بضرر أو غزو أو احتلال، ويمكن أن تأتي التهديدات من الخارج أو من الداخل"[4].

---

[1] أحمد عبد الحليم، **أمن الخليج: إلى أين؟** ، اوراق الشرق الاوسط، 1992، ص 28-29.

[2] عبد الله الحربي ، **مرجع سابق**، ص 28.

[3] LivierNay , **Lexique de Science politique vie et Institutions politiques** ,Europe Media Duplication SAS, Toulouse, 2008 , P 482 .

[4] تيري ديبيل، **استراتيجية الشؤون الخارجية...منطق الحكم الأمريكي**، ترجمة: وليد شحادة ، دار الكتاب العربيومؤسسة محمد بن آل راشد آل مكتوم، بيروت، 2009، ص 258-261.

كما توجد عدة معايير لتصنيف التهديدات الأمنية يعتمدها الباحثون، إذ يركز بعضهم على:

1. **معيار المجال:** ويشتمل على :

- **تهديدات سياسية:**غياب نظام سياسي مقبول، وغياب مؤشرات الديمقراطية...
- **تهديدات اقتصادية:** ضعف الناتج القومي والأداء الاقتصادي وعدم التوزيع العادل الثروة.
- **تهديدات إجتماعية وثقافية:** تفكك المجتمع وازمة الهوية.
- **تهديدات بيئية:** تهديد يمس محيط العيش، التلوث، الاحتباس الحراري ...إلخ.

2. **معيار درجة الخطورة** : تهديدات فعلية، محتملة، كامنة، متصورة.

3. **معيار التماثل والتأثير** : تهديدات تماثلية ، تهديدات لا تماثلية.

المبحث الثاني : الفضاء السيبراني والتحول في مفاهيم القوة والصراع.

كانت ثورة المعلومات وظهور الانترنيت إيذانا ببزوغ العصر السيبري، وخلق بيئة جديدة هي **الفضاء السيبراني (Cyber space)** – إضافة إلى الأرض والبحر والجو والفضاء– الذي أصبح يؤثر في النظام الدولي، خاصة مع بروز شكل جديد من القوة هو**القوة السيبرانية (Cyberpower)**، التي توزعت وانتشرت بين عدد أكبر من الفاعلين على المستوى الدولي والمحلي، ما جعل الفضاء السيبراني مجالا جديدا للصراع بين الدول.

المطلب الأول : الفضاء السيبراني وتحولات القوة.

أولا : مفهوم الفضاء السيبراني :

الفضاء السيبراني مجال افتراضي من صنع الإنسان يعتمد على نظم الكمبيوتر وشبكات الانترنيت وكم هائل من البيانات والمعلومات والأجهزة.

هناك من عرف الفضاء السيبراني بوصفه الذراع الرابعة للجيوش الحديثة[1]، وهناك من يرى أنه البعد الخامس للحرب، وهذا التعريف يحصر الفضاء السيبراني في المجال العسكري فقط دون التطرق للمجالات الأخرى.

وعرفته **الوكالة الفرنسية لأمن أنظمة الإعلام** (ANSSI)، وهي وكالة حكومية مكلفة بالدفاع السيبراني الفرنسي على أنه: " فضاء التواصل المشكل من خلال الربط البيني العالمي لمعدات المعالجة الآلية للمعطيات الرقمية"[2].

[1] عباس بدران، **الحروب الالكترونية: الاشتباك في عالم متغير**، مركز دراسات الحكومة الالكترونية، بيروت،2010،ص 4.

[2] Olivier KEMPF**, Introduction à la Cyberstratégie**, Paris, Economica, 2012, P 9.

وهذا التعريف يركز على الجانب التقني كما يغفل العامل البشري، والذي يعد جزءا أساسيا في فهم الفضاء السيبراني.

كما جاء تعريف **الاتحاد الدولي للاتصالات** للفضاء السيبراني بأنه " المجال المادي وغير المادي الذي يتكون وينتج عن عناصر هي: أجهزة الكمبيوتر، الشبكات، البرمجيات، حوسبة المعلومات، المحتوى، معطيات النقل والتحكم، ومستخدمو كل هذه العناصر"[1].

وعليه يمكننا القول بأن: "الفضاء السيبراني هو بيئة تفاعلية حديثة، تشمل عناصر مادية وغير مادية، مكون من مجموعة من الأجهزة الرقمية، وأنظمة الشبكات والبرمجيات، والمستخدمين سواء مشغلين أو مستعملين".

وتجدر الإشارة إلى أن مسألة تحديد مفهوم "الفضاء السيبراني"، هي مسألة نسبية تتوقف على طبيعة إدراك وفهم كل من الدول والهيئات كل حسب رؤيته وإستراتيجيته وقدرته على استغلال المزايا المتاحة ومواجهة المخاطر الكامنة في هذا الفضاء.

ثانيا : تحولات القوة وظهور القوة السيبرانية:

أصبح الفضاء السيبراني احد العناصر الأساسية التي تؤثر في النظام الدولي، بما يتيحه من أدوات تكنولوجية مهمة لعمليات الحشد والتعبئة في العالم، فضلا عن التأثير في القيم السياسية، فسهولة الاستخدام ورخص التكلفة زادا من قدرته على التأثير في مختلف مجالات الحياة، سواء السياسية، الاقتصادية، العسكرية، الاجتماعية وحتى الايديولوجية، وبات جليا أن من يمتلك آليات توظيف البيئة السيبرانية يصبح أكثر قدرة على تحقيق أهدافه والتأثير في سلوك الفاعلين المستخدمين لهذه البيئة.

[1]The International Télécommunication Union, **ITU Toolkit for CybercrimeLégislation**, Geneva, 2010, P 12.

من الأمور المستقرة في العلاقات الدولية أن مصادر قوة الدولة وأشكالها تتغير، فإلى جانب القوة الصلبة ممثلة في القدرات العسكرية والاقتصادية، تزايد الاهتمام بالأبعاد غير المادية للقوة، ومن ثم بروز القوة الناعمة التي تعتمد على جاذبية النموذج والإقناع، ومع ثورة المعلومات ظهر شكل جديد من أشكال القوة هو القوة السيبرانية (Cyber power)، التي لها تأثير كبير على المستوى الدولي والمحلي، فمن ناحية أدت إلى توزيع وانتشار القوة بين عدد أكبر من الفاعلين مما جعل قدرة الدولة على السيطرة موضع شك، ومن ناحية أخرى منحت الفاعلين الأصغر قدرة أكبر على ممارسة كل من القوة الصلبة والقوة الناعمة عبر الفضاء السيبراني، وهو ما يعني تغيرا في علاقات القوى في السياسة الدولية.

يعد **جوزيف.س ناي** (Joseph S.Nye) من أبرز المهتمين بالقوة السيبرانية، حيث يعرفها بأنها :" القدرة على الحصول على النتائج المرجوة من خلال استخدام مصادر المعلومات المرتبطة بالفضاء السيبراني، أي أنها القدرة على استخدام الفضاء السيبراني لإيجاد مزايا للدولة، والتأثير على الأحداث المتعلقة بالبيئات التشغيلية الأخرى وذلك عبر أدوات سيبرانية"[1]، كما يوضح **جوزيف.س ناي** أن مفهوم القوة السيبرانية يشير إلى "مجموعة الموارد المتعلقة بالتحكم والسيطرة على أجهزة الحاسبات والمعلومات والشبكات الالكترونية والبنية التحتية المعلوماتية والمهارات البشرية المدربة للتعامل مع هذه الوسائل"[2].

ويتناول مفهوم القوة السيبرانية مجمل القضايا التي تتعلق بالتفاعلات الدولية العسكرية والاقتصادية والسياسية والثقافية والإعلامية وغيرها.

[1]Joseph S.Nye JR , **Cyber Power**, Harvard Kennedy School, 2010, P 03 .
[2]**Ibid** , P 04 .

وحتى تتمكن الدولة من ممارسة النفوذ داخليا أو خارجيا عبر القوة السيبرانية يجب أن تتوفر على مجموعة عناصر أهمها:

- **وجود بنية تحتية سيبرانية** : تشمل أجهزة الكمبيوتر، وشبكات الاتصالات، والبرمجيات، وقواعد البيانات لمختلف الأنظمة والقطاعات.
- **بنية مؤسسية** : تتولى مهمة ممارسة القوة السيبرانية وتحقيق الأمن السيبراني للدولة.
- **بنية تشريعية** : تكون ضامنة ومحددة لاستعمال القوة السيبرانية.
- **إستراتيجية بأهداف واضحة:** تحدد طرق العمل والأهداف المرجوة.

وحتى تكتمل عناصر القوة السيبرانية لابد للدولة من القيام بتطوير أسلحة في مجال الحرب السيبرانية لاستعمالها سواء في العمليات الهجومية أو من أجل الردع.

المطلب الثاني : الفواعل في مجال القوة السيبرانية.

يحدد **جوزيف.س ناي** ثلاثة أنواع من الفاعلين الذين يمتلكون القوة السيبرانية[1]:

- **الدول** : والتي لديها قدرة كبيرة على تنفيذ هجمات سيبرانية وتطوير البنية التحتية وممارسة السلطات داخل حدودها.
- **الفاعلون من غير الدول** : ويستخدم هؤلاء الفاعلون القوة السيبرانية لأغراض هجومية بالأساس، إلا أن قدرتهم على تنفيذ أي هجوم سيبراني مؤثر تتطلب مشاركة ومساعدة أجهزة استخباراتية متطورة، ولكن يمكنهم اختراق المواقع الالكترونية واستهداف الانظمة الدفاعية.
- **الأفراد (القراصنة)**:الذين يمتلكون معرفة تكنولوجية عالية والقدرة على توظيفها، وعادة ما تكون هناك صعوبة في الكشف عن هوياتهم، ومن الصعب ملاحقتهم.

[1]Joseph S.Nye JR , **Ibid**, P 10 .

كما يمكننا التفصيل أكثر بخصوص الفاعلين من غير الدول كالتالي[1]:

- **الشركات متعددة الجنسيات :**

تمتلك بعض شركات التكنولوجيا موارد للقوة تفوق قدرة بعض الدول، ولا تنقصها سوى شرعية ممارسة القوة التي مازالت حكرا على الدول، فخوادم شركات مثل: **جوجل**Google **وفيسبوك**Facebook **وميكروسوفت** Microsoft، تسمح لها بامتلاك قواعد البيانات العملاقة التي من خلالها تستكشف وتستغل الأسواق، وتؤثر في اقتصاديات الدول وفي ثقافة المجتمعات وتوجهاتها، وهذا ما حدث في الأزمة بين شركة جوجل والصين حول المحتوى، أو فضيحة تسريب بيانات مستخدمي فايسبوك لصالح شركة "**كامبردج أناليتيكا**" التي تم الاستعانة بها لصالح حملة المرشح الجمهوري **ترامب**.

- **المنظمات الإجرامية :**

تقوم هذه المنظمات الإجرامية بعمليات القرصنة السيبرانية، وسرقة المعلومات واختراق الحسابات البنكية وتحويل الأموال، كما توجد سوق سوداء على الانترنيت المظلم Dark internet لتجارة المخدرات والأسلحة والبشر، حيث تكلف هذه الجرائم السيبرانية مليارات الدولارات سنويا.

- **الجماعات الإرهابية :**

تعد من أبرز الفواعل الدولية، خاصة بعد أحداث 11 سبتمبر، حيث تستغل الفضاء السيبراني في عمليات التجنيد والتعبئة والدعاية وجمع الأموال والمتطوعين، كما تحاول جمع المعلومات حول الأهداف العسكرية، وكيفية التعامل مع الأسلحة وتدريب المجندين الجدد عن بعد، رغم أنها لم تصل بعد إلى مرحلة القيام بهجوم سيبراني حقيقي على منشآت البنية التحتية للدول.

[1] ايهاب خليفة،**القوة الالكترونية وأبعاد التحول في خصائص القوة**، مكتبة الاسكندرية،مصر، 2014، ص 33-42.

- **الأفراد :**

أصبح الفرد بفضل الفضاء السيبراني فاعلا مؤثرا في العلاقات الدولية، ومن أبرز النماذج ظاهرة **الويكيليكس** "Wikileaks" الذي نجح في نشر ملايين الوثائق السرية للإدارة الأمريكية وقنصلياتها، مما خلق مشاكل دبلوماسية بين الولايات المتحدةالأمريكية وحلفائها.

المطلب الثالث : الصراع السيبراني.

اختصر الفضاء السيبراني حاجز الزمان والمكان، وخلق مساحات للتفاعلات الداخلية والدولية في الواقع الافتراضي، ومن ثم، برزت فضاءات جديدة للصراع بأدوات مختلفة، وأنماط جديدة تختلف عن الصراعات التقليدية، بعد أحداث 11 سبتمبر 2001 كان الفضاء السيبراني ساحة الصراع والقتال بين تنظيم القاعدة و الولايات المتحدة، وفي عام 2007 جرت العمليات العدائية بين استونيا وروسيا، وهو ما حدث أيضا في 2008 في الحرب بين روسيا و جورجيا، وجاء الهجوم السيبراني بفيروس "**ستاكسنت**" على برنامج إيران النووي عام 2012، ليبرز قوة الأسلحة السيبرانية في الصراعات الدولية.

ولعل أبرز ما يعزز انتشار الأنشطة غير السلمية في الفضاء السيبراني[1]:

1. ارتباط العالم المتزايد بالفضاء السيبراني وزيادة خطر تعرض البنية التحية الكونية للمعلومات لهجمات سيبرانية.
2. استخدام الفاعلين من غير الدول للفضاء السيبراني لتحقيق أهدافهم وتأثير ذلك على سيادة الدولة.
3. انسحاب الدولة من قطاعات إستراتيجية لصالح القطاع الخاص.

[1] عادل عبد الصادق، **أسلحة الفضاء الالكتروني في ضوء القانون الدولي**، سلسلة أوراق، العدد 23، مكتبة الاسكندرية، مصر، 2016، ص 17-18.

4. إشكالية تعاملالدول مع الشركات التكنولوجية متعدية الجنسيات، والتي أصبحت تفوق قدراتها، مثل مواقع التواصل الاجتماعي كالفيسبوك وتويتر واليويتوب الذين أصبحوا فاعلين دوليين بامتياز.

وبالتالي أصبح الفضاء السيبراني ساحة جديدة للصراع بشكله التقليدي ولكنه ذو طابع سيبرانييعكس النزاعات التي تخوضها الدول أو الفاعلين من غير الدول على خلفيات دينية أو عرقية أوإيديولوجية أواقتصادية أو سياسية، ويتمدد الصراع السيبراني بداخل شبكات الاتصال والمعلومات متجاوزا الحدود التقليدية وسيادة الدول.

وكشف استخدام الفضاء السيبراني عن حالة التعارض الحقيقي للاحتياجات والقيم والمصالح بين العديد من الفاعلين، وساعد ذلك على ظهور أساليب جديدة للصراع الدولي، تباينت بين الطابع التقني والتجاري والاقتصادي والعسكري، إلى جانب ظهور طرق بديلة عن الحرب المباشرة بين الدول عبر شبكات الاتصال والمعلومات.

فهناك صراع سيبرانيتحركه دوافع سياسية، ويأخذ شكلا عسكريا، ويتم فيه استخدام قدرات هجومية ودفاعية عبر الفضاء السيبراني.

ويوجد صراع سيبراني ذو طبيعة ناعمة، حول الحصول على المعلومات والتأثير في المشاعر والأفكار وشن حرب نفسية وإعلامية.

كما يأخذ الصراع السيبراني طابعا تنافسيا حول الاستحواذ على سبق التقدم التكنولوجي وسرقة الأسرار الاقتصادية والعلمية، والتحكم بالمعلومات، والعمل على اختراق الأمن القوميللدول، كهجمات قراصنة الكمبيوتر والتجسس بما يكون له من تأثير على تدمير الاقتصاد والبنية التحتية بنفس القوة التي قد يسببها تفجير تقليدي مدمر.

ويمكن أن يستخدم الفضاء السيبراني كوسيلة من وسائل الصراع داخل الدولة، بين مكوناتها، على أساس طائفي أو اقتصادي أو ديني.

المبحث الثالث : مفهوم الأمن السيبراني والتهديدات السيبرانية.

إن اعتماد عالم اليوم على المعلومة حقيقة ثابتة، وهي تفرض اعتمادا أكثر على الأنظمة الالكترونية التي تعالجها، والحديث عن الأمن يستدعي تعريف الخطر، أي التهديد الذي يتعرض له النظام، إضافة إلى نقاط الضعف والثغرات، ومن ثم الإجراءات المفروض اتخاذها، لدفع الخطر، ونتيجة زيادة التهديدات والمخاطر في الفضاء السيبراني التي تواجه الدول ظهر مفهوم الأمن السيبراني.

المطلب الأول : مفهوم الأمن السيبراني وأبعاده.

أولا : تعريف الأمن السيبراني.

يعرف الأمن السيبراني بأنه امن الشبكات والأنظمة المعلوماتية، والبيانات، والمعلومات، والأجهزة المتصلة بالانترنيت، وعليه فهو المجال الذي يتعلق بإجراءات، ومقاييس، ومعايير الحماية المفروض اتخاذها، أو الالتزام بها، لمواجهة التهديدات، ومنع التعديات، او على الأقل الحد من آثارها[1].

فـ**ريتشارد كمرر Richard A.Kemmerer** يعرف الأمن السيبراني بأنه :" عبارة عن وسائل دفاعية من شأنها كشف وإحباط المحاولات التي يقوم بها القراصنة"[2].

بينما عرفه **إدوارد أمورسو AmorsoEdward** على أنه :" وسائل من شأنها الحد من خطر الهجوم على البرمجيات أو أجهزة الحاسوب أو الشبكات، وتشمل تلك الوسائل الأدوات المستخدمة في مواجهة القرصنة وكشف الفيروسات ووقفها،.. إلخ"[3].

[1] منى الأشقر جبور، **مرجع سابق**، ص 25.
[2]Richard A. Kemmerer**, Cyber security**, University of California Santa Barbara, Department of Computer Science, 2003, P.3
[3]Edward Amoroso**, Cyber Security**, SiliconPress, 2007 , P01.

وبحسب تعريف **الإتحاد الدولي للاتصالات** في تقريره حول **(اتجاهات الاصلاح في الاتصالات للعام 2010-2011)**، هو " مجموعة من المهمات، مثل تجميع وسائل، وسياسات، وإجراءات أمنية، ومبادئ توجيهية، ومقاربات لإدارة المخاطر، وتدريبات، وممارسات فضلى، وتقنيات، يمكن استخدامها لحماية البيئة السيبرانية، وموجودات المؤسسات والمستخدمين"[1].

وتهدف الحماية إلى جعل المعتدين يحجمون عن خططهم، أو منعهم من تحقيقها، وإلى ضمان حد مقبول من الأخطار، وذلك عبر وضع خطة تتلائم والمحيط التقني، البشري، التنظيمي، والقانوني.

ثانيا : أبعاد الأمن السيبراني.

يطال الأمن السيبراني جميع المسائل العسكرية، الاقتصادية، والاجتماعية، والسياسية، والإنسانية، بهدف تحقيق منظومة أمن متكاملة تعمل على الحفاظ على الأمن القومي للدولة من كل التهديدات السيبرانية، وعليه لابد من توضيح أبعاد الأمن السيبراني، التي نوردها كالآتي[2] :

- **البعد العسكري** : يكمن في الحفاظ على قدرة الوحدات العسكرية على التواصل عبر الشبكات العسكرية، مما يسمح بتبادل المعلومات والأوامر وتدفقها (هي الفكرة التي خلقت وطورت من أجلها الشبكات ومن بعدها الانترنيت)، وإصابة الأهداف عن بعد، إلا أنها تمثل كذلك نقطة ضعف، خاصة إذا لم تكن مؤمنة جيدا من الاختراق، الذي قد يؤدي إلى تدمير قواعد البيانات العسكرية، أو قطع الاتصال بين القيادة والوحدات العسكرية، فضلا عن إمكانية التحكم في بعض الأسلحة وخروجها عن السيطرة (طائرات بدون طيار، صواريخ موجهة، أقمار صناعية.... إلخ)، ويعتبر فيروس

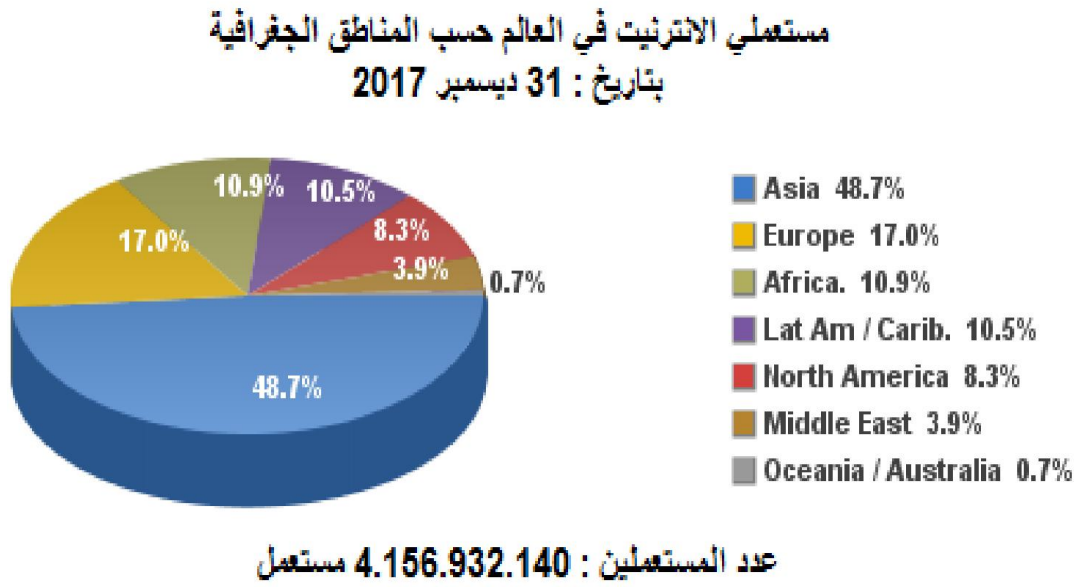
[1] ITU, **Cyber security**, Geneva: International Telecommunication Union (ITU),2008.

[2] محمد مختار،**"الأمن السيبراني"** ، مفاهيم المستقبل، اتجاهات الأحداث ، العدد 6 ، 2015، ص 6.

ستاكسنتStuxnet بداية لاستعمال القوة السيبرانية لتدمير البنية المادية (هاجم حواسيب أجهزة الطرد المركزي الإيرانية).

- **البعد الاقتصادي** : أصبح الانترنيت أساسا للمعاملات التجارية والمالية والاقتصادية، كما تستعمل الحواسيب في تسيير وتطوير الصناعات وتحريك الاقتصاد، وأصبح الكل مترابطا عبر شبكات الكمبيوتر، مما يستدعي الحديث عن أهمية تحقيق الأمن السيبراني في المجال الاقتصادي.
- **البعد الاجتماعي** :

الشكل 1 : مستعملي الانترنيت حول العالم



المصدر : Internet world statsعلى الموقع www.internetworldstats.com

يفوق مستخدمي الانترنيت 4 مليارات شخص في العالم، منهم اكثر من 2.6 مليار يستخدمون مواقع التواصل الاجتماعي، مما يجعلها أكبر تجمع للتفاعل البشري، ويفتح الباب واسعا لتبادل الأفكار والخبرات الجيدة، لكن في المقابل يعرض أخلاقيات المجتمع للخطر، نظرا لصعوبة مراقبة محتوى الانترنيت، كما يعرض الهويات لعمليات

اختراق خارجي قد تتسبب في تهديد السلم الاجتماعي للدولة، وعليه فلابد من العمل على توعية المواطن بهذه المخاطر لتحقيق الأمن السيبراني في بعده الاجتماعي.

- **البعد السياسي** : يعد التدخل الروسي السيبراني في الانتخابات الأمريكية أبرز دليل على ضرورة وأهمية الأمن السيبراني في بعده السياسي، إضافة إلى التسريبات للوثائق الحساسة والاختراقات التي غالبا ما تؤدي إلى أزمات دبلوماسية بين الدول، كما أن الفضاء السيبراني أصبح بيئة خصبة للحملات الانتخابية والدعاية لمختلف الفاعلين الدوليين.
- **البعد القانوني** : إن التطورات التكنولوجية المتسارعة، تفرض مواكبة التشريعات القانونية لها، من خلال وضع أطر وتشريعات للأعمال القانونية وغير القانونية في الفضاء السيبراني، فالملاحظ أن الجريمة السيبرانية تفتقد في معظم الحالات والبلدان أطرا قانونية صارمة للتعامل معها، إضافة إلى ضرورة تفعيل التعاون الدولي المشترك لمكافحتها.

المطلب الثاني : أنماط التهديدات السيبرانية.

تقسم التهديدات السيبرانية التي تواجهها الدول والأفراد إلى أربعة أنماط رئيسية هي[1] :

1. **هجمات الحرمان من الخدمة:** حيث يتمإطلاق حزمة كبيرة من الطلبات والمهمات على خوادم الضحية بصورة تفوق قدرة الخادم أو الجهاز على معالجتها والاستجابة لها، مما يؤدي إلى توقفه بصورة جزئية أو كلية أو إبطاء عمله، وهذا ما يسبب ضرر للمستخدم النهائي، وهي تستعمل كثيرا ضد مواقع الانترنيت أو البنوك أو المؤسسات من أجل التأثير عليها أو لدفع فدية مالية.

[1] محمد مختار، **"هل يمكن للدول أن تتجنب مخاطر الهجمات الالكترونية؟"**، مفاهيم المستقبل، العدد 6، مركز المستقبل للأبحاث والتطوير، 2015، ص 5-6.

2. **إتلاف المعلومات أو تعديلها** : ويقصد به الوصول إلى معلومات الضحية عبر شبكة الانترنيت أو الشبكات الخاصة، والقيام بعملية تعديل البيانات الهامة دون أن يكتشف الضحية ذلك، فالبيانات تبقى موجودة لكنها مضللة قد تؤدي إلى نتائج كارثية خاصة إذا كانت خطط عسكرية أو مواعيد آو خرائط سرية.
3. **التجسس على الشبكات** : ويقصد به الدخول غير المصرح والتجسس على شبكات الخصم، دون تدمير آو تغيير في البيانات، والهدف منه الحصول معلومات قد تكون خطط عسكرية أو أسرار حربية، اقتصادية ، مالية ، أو سياسية، مما يؤثر سلبا على مهام الخصم.
4. **تدمير المعلومات:** ويتم في هذه الحالة مسح وتدمير كامل للأصول والمعلومات والبيانات الموجودة على الشبكة، يصطلح عليه " تهديد لسلامة المحتوى" ويعني بها إحداث تغيير في البيانات سواء بالحذف أو التدمير من قبل أشخاص غير مخولين.

وهناك من يميز بين عدة أنواع لمخاطر التهديدات السيبرانية نذكر منها[1] :

- التعرض لسرية الاتصالات التي تطال البريد الالكتروني، والدخول إلى الأنظمة والملفات دون إذن، وهذا يعتبر اعتداءا على الحريات والحقوق الشخصية.
- التلاعب بالمعلومات الموجودة في نظام معين، وتشويهها او إتلافها، سواء عبر الاختراق أو نشر الفيروسات.
- الجرائم العادية التي تستخدم الانترنيت، كالسرقة والغش وسرقة الهويات، والاعتداء على الملكية الفكرية وغيرها.
- الجرائم التي تندرج في إطار الجريمة المنظمة، والتي تهدد امن الأفراد والدول، كتبييض الأموال والإرهاب...إلخ.

[1] منى الأشقر جبور،**مرجع سابق** ، ص 35-36.

خلاصة الفصل الأول :

في نهاية الفصل الأول، نخلص الى ان مفهوم الأمن القومي قد طرأ عليه الكثير من التعديل والتغيير، على مستوى التهديدات، الفاعلين، والقطاعات، فبعد أن كان محصورا عند الواقعيين في الدولة والقوة العسكرية، توسع في مفهومه الشامل، ليعم جميع مجالات الحياة، وتوجه تركيزهعلى أمن الأفراد والمجتمعات، هذه الاخيرة التي دخلت العصر الرقمي بفضل ثورة المعلومات والاتصالات، فالكل مرتبط بالشبكة، مما خلق فضاءا جديدا للتفاعل، هو الفضاء السيبراني، الذي بدوره أحدث تغييرا في مفاهيم العلاقات الدولية، كمفهوم القوة والصراع والحرب، حيث انتشرت القوة وتوزعت بين الفاعلين، وتحول الصراع من المادي الى الافتراضي، واصبحت الحروب تخاض بالأصفار والآحاد، وبدا واضحا أن الدول تتجه نحو عسكرة الفضاء السيبراني، مما نتج عنه ظهور تهديدات جديدة تتزايد في الحجم والشدة، وتشكل تهديدا خطيرا للأمن القومي.

فكلما زاد التشابك، زادت التهديدات السيبرانية، وأثر ذلك على الأمن القومي، مما عجل بظهور مفهوم جديد هو الامن السيبراني، بأبعاده المختلفة، والذي تحاول الدول من خلاله الحد من المخاطر والتهديدات في الفضاء السيبراني.

الفصل الثاني:

مظاهر تأثير التهديدات السيبرانية على الأمن القومي وآليات مواجهتها

الفصل الثاني:

مظاهر تأثير التهديدات السيبرانية على الأمن القومي وآليات مواجهتها

يتناول هذا الفصل البحث في العلاقة بين الأمن السيبراني والأمن القومي، الذي تغير مفهومه بدخول رافد جديد هو الأمن السيبراني، الذي يعالج سبل مكافحة التهديدات والأخطار في الفضاء السيبراني، التي تتطور من الجريمة السيبرانية، إلى الإرهاب السيبراني، لتنتهي عند الحروب السيبرانية كأعلى درجات الصراع، ثم نتناول بالدراسة جهود الدول والمنظمات لمواجهة هذه التهديدات والسعي لإقامة فضاء سيبراني سلمي.

وفي هذا الإطار يقسم الفصل إلى ثلاثة مباحث كالتالي :

المبحث الأول : علاقة الأمن السيبراني بالأمن القومي.

المبحث الثاني :أبرز التهديدات السيبرانية.

المبحث الثالث : جهود الدول لمواجهة التهديدات السيبرانية.

المبحث الأول :علاقة الأمن السيبراني بالأمن القومي.

يعالج هذا المبحث العلاقة الترابطية بين الأمن السيبراني والأمن القومي، وكيف تحولت العقيدة الأمنية للدول وتغيرت استراتجياتها،سعيا منها للحفاظ على أمنها القومي.

المطلب الأول:الأمن السيبراني رافد جديد للأمن القومي.

تزايدت العلاقة بين الأمن والتكنولوجيا، ومعها تزايدت امكانية تعرض المصالح الاستراتيجية للدولة للتهديدات السيبرانية، وهددت بتحول الفضاء السيبراني لوسيط ومصدر لأدوات جديدة للصراع الدولي المتعدد الاطراف.

بعد أحداث 11 سبتمبر بدأ التركيز على الفضاء السيبراني كتهديد أمني جديد، خاصة مع استخدام تنظيم القاعدة له كساحة قتال ضد الولايات المتحدة الامريكية، وفي 2007 و2008 على التوالي، كان الأمن القومي لكل من استونيا وجورجيا مهددا من طرف روسيا، حيث استعملت هجمات الحرمان من الخدمة لتقويض العمل في الإدارات والمؤسسات الحكومية لكلا الدولتين، وجاء الهجوم السيبراني بفيروس "**ستاكسنت**" على أجهزة الطرد المركزي الايرانية،من أجل تعطيل برنامج ايران النووي، ليمثل نقلة نوعية مهمة في تطوير واستخدام الأسلحة السيبرانية[1].

هذا، إضافة الى الدور الكبير الذي لعبته شبكات التواصل الاجتماعي في حالة الثورات العربية في بداية 2011، حيث مثلت نقطة هامة في زيادة الاهتمام الدولي بأمن الفضاء السيبراني، وبرزت محاولات للسيطرة عليه بعد تصاعد الاحتجاجات حتى في الدول الاكثر ديموقراطية كبريطانيا والولايات المتحدة الامريكية.

[1] عادل عبد الصادق، **القوة الالكترونية: اسلحة الانتشار الشامل في عصر الفضاء الالكتروني**، مجلة السياسة الدولية، العدد 188، مؤسسة الأهرام، مصر، 2012، ص 32.

وإذا كان الأمن القومي يعنى بالحماية وغياب التهديد لقيم المجتمع الأساسية، وغياب الخوف من خطر تعرض هذه القيم للهجوم، فإن الفضاء السيبراني قد فرض إعادة التفكير في مفهوم الأمن، والذي يتعلق بدرجة تمكن الدولة من أن تصبح في مأمن من خطر التعرض للهجوم، وإجراءات الحماية ضد تعرض المنشآت الحيوية للبنية التحتية للتهديد، من خلال الاستخدام السيئ لتكنولوجيا الاتصال والمعلومات.

إن العلاقة بين الأمن السيبراني والأمن القومي تزداد كلما زاد نقل المحتوى المعلوماتي والعسكري والامني والفكري والسياسي والاجتماعي والاقتصادي والخدمي والعلمي والبحثي إلى الفضاء السيبراني، خاصة مع التسارع في تبني الحكومات الالكترونية والمدن الذكية في العديد من الدول، واتساع نطاق وعدد مستخدمي الانترنيت في العالم، والثورة الكبرى في انترنيت الأشياء، حيث أصبحت قواعد البيانات القومية في حالة انكشاف خارجي، اضافة الى حملات الدعاية والمعلومات المضللة ونشر الشائعات أو الدعوة لأعمال تحريضية أو دعم المعارضة أو الاقليات، مما يساهم في تلاشي سيادة الدولة ويشكك في قدرتها على الحفاظ على أمنها القومي[1].

وعليه فلم يقتصر اهتمام الدول بالأمنالسيبراني على البعد التقني وحسب، بل تجاوزه إلى أبعاد أخرى مثل الإبعاد الثقافية والاجتماعية والاقتصادية والعسكرية وغيرها،وهو ما عمل على دعم حقيقة ان الاستخدام غير السلمي للفضاء السيبراني يؤثر على الرخاء الاقتصادي والاستقرار الاجتماعي لجميع الدول التي أصبحت تعتمد على البنية التحتية الكونية لمعلومات.

اضافة الى ان تصاعد دور الفاعلين من غير الدول في العلاقات الدولية قد اثر بدوره على سيادة الدول، وبخاصة مع بروز دور الشركات التكنولوجية العابرة للحدود، وبروز أخطار القرصنة والجريمة السيبرانية والجماعات الإرهابية.

[1] ايهاب خليفة، **القوة الالكترونية: كيف يمكن ان تدير الدول شؤونها في عصر الانترنيت**، دار العربي، 2017، ص 54.

لقد أصبحت المصالح القومية التي ترتبط بالبنية التحتية الحيوية عرضة لخطر الهجوم، حيث جعل الفضاء السيبراني تلك المصالح مرتبطة ببعضها البعض في بيئة عمل واحدة، ومن ثم فإن أي هجوم على إحدى تلك المصالح يكون سببا لحدوث عدم توازن استراتيجي، ومهددا خطيرا للأمن القومي، وهذا ما دفع العديد من الدول إلىإدخالالأمنالسيبراني ضمن استراتيجيتها للأمن القومي.

المطلب الثاني:العقيدة الأمنية الجديدة.

إن حالة انعدام الثقة واللايقين في العلاقات الدولية، هو ما يشجع تزايد النزاعات في العالم، إضافة إلى التطورات السريعة في الفضاء السيبراني، جعلت الدول تسارع إلى تبني تغييرات في العقيدة الامنية، وذلك بإدراج القوة السيبرانية كمحدد رئيس لمدى قوة الدولة، وقدرتها على حسم النزاعات لصالحها.

وكمثال على ذلك، نجد أن العقيدة الروسية الجديدة ، تكشف أنه تمت إضافة بند جديد يخص تهديدات الأمن السيبراني في المجالين العسكري والاقتصادي.

ووفقا للعقيدة الروسية الجديدة لأمن المعلومات، التي وقعها الرئيس الروسي فلاديمير بوتين، فإن إحدى التهديدات الرئيسية لروسيا تتمثل "بزيادة عدد الدول الأجنبية التي لديها تأثير على البنية التحتية لمعلومات الأغراض العسكرية في روسيا".

أحد الأهداف الرئيسية لواضعي هذه العقيدة الجديدة، هو "الردع الاستراتيجي والوقاية من النزاعات العسكرية، والتي يمكن أن تنجم عن استخدام تكنولوجيا المعلومات"[1].

يقول أوليغ ديميدوف، وهو خبير في الأمن السيبراني، من مؤسسة الرأي الروسية **بي آي آر**: "العقيدة في شكلها الحالي هي العقيدة الأفضل بما يخص التهديدات الموجهة

[1] **ما الجديد في عقيدة الأمن السيبراني الروسي؟**، مركز دراساتكاتيخون ، على الموقع : http://katehon.com/ar/article/m-ljdyd-fy-qyd-lmn-lsybrny-lrwsy تاريخ الاطلاع: 22-04-2018.

للأمن العسكري والتكنولوجي في روسيا"،فهي تعمل على الحماية منالعمليات السيبرانية من قبل الأجهزة الخاصة الأجنبية، فضلا عن مكافحة النشاط الاستطلاعي الأجنبي في روسيا، ويشير الخبير إلى أن الحكومة الروسية أولت اهتماما خاصا لمواجهة "ثورات التويتر" الجديدة، كتلك التي حدثت في الشرق الأوسط في بداية العقد الحالي.

ارتبط تصاعد الصراع بين روسيا والدول الغربية بقيادة الولايات المتحدة، خلال السنوات الماضية، باستدعاءمتنام لحرب المعلومات كأحد المداخل الهامة للتأثير في مسارات الصراع.

وكما يعتقد **ديفيد سميث David J. Smith** في دراسة له بعنوان "كيف تستخدم روسيا الحرب السيبرانية؟"، أن روسيا "تعتمد على مفهوم واسع للحرب المعلوماتية، يشمل: الاستخبارات، والتجسس المضاد، والخداع، والتضليل، والحرب السيبرانية، وتدمير الاتصالات وأنظمة دعم الملاحة، والضغوط النفسية، بالإضافة إلى الدعاية وإلحاق الضرر بنظم المعلومات"[1].

ويفترض "**بافل أنتونوفيتش**" **Pavel Antonovich** أن "ترسيم الخطوط الفاصلة بين الحرب والسلام يمكن أن يتآكل بسهولة في الفضاء السيبراني، فيمكن أن يتم إلحاق أضرار، مهما كانت طبيعتها، بالخصم، وذلك دون تجاوز الخط الفاصل بين الحرب والسلام بشكل رسمي"[2].

[1]David Smith, **How RussiaHarnesses Cyber Warfare**,Defense Dossier, American Foreign Policy Council (August 2012: Issue 4), 9. Accessedat : http://www.afpc.org/files/august2012.pdf.

[2]محمد بسيوني، **دوافع الاستراتيجية الروسية لحرب المعلومات ضد الدول الغربية**، جريدة الصباح الجديد ، على الرابط : http://newsabah.com/newspaper/138116 تاريخ الاطلاع : 30-03-2018.

وفي الجهة المقابلة، نجد أن منظمة "**حلف شمال الأطلسي NATO**" سعت بدورها إلى تحديث عقيدتها الأمنية، استجابة للتغيرات الحاصلة في طبيعة التهديدات، وطبيعة الحرب، حيث أقرت مجموعة من النقاط الأساسية من بينها[1]:

- ان الدفاع السيبراني يمثل جزءا اساسيا من الدفاع الجماعي للحلف.
- الفضاء السيبراني يمثل مجالا لعمليات الحلف.
- بناء قدرات سيبرانية تعد مهمة اساسية للحلف وحلفائه.

بالإضافة، نجد كلا من الصين، اسرائيل، بريطانيا، فرنسا، والولايات المتحدة الأمريكية، إيران، وكوريا الشمالية، قد طورت كل منها عقيدتها الأمنية، وأصبحت تعتبر الفضاء السيبراني مسرحا للعمليات العسكرية، كما أوجدت قيادة خاصة ومستقلة لقيادة العمليات السيبرانية.

[1]**Cyber defence**, North Atlantic TreatyOnganisation, , At : https://www.nato.int/cps/en/natohq/topics_78170.htmseen: 19-03-2018

المبحث الثاني :أبرز التهديدات السيبرانية.

يتم فيه التطرق إلى أبرز التهديدات السيبرانية، وتم ترتيبها حسب درجة الخطورة، بداية بالجريمة السيبرانية، الارهاب السيبراني، وأخيرا الحرب السيبرانية.

المطلب الأول:الجريمة السيبرانية.

خلق الفضاء السيبراني فرصا جديدة المجرمين، وانتج انواعا جديدة من الجريمة تسمى "الجريمة السيبرانية"، تشمل القرصنة والاحتيال والتخريب وغيرها.

أولا : مفهوم الجريمة السيبرانية :

تعرف الجريمة السيبرانية بالمعنى الضيق على انها "جريمة الكمبيوتر" وأي تصرف غير قانوني موجه ضد الجهاز، النظام، او المعلومات التي تحويه، اما بمعناها الواسع، فهي الجريمة المتصلة باستخدام الكمبيوتر، أي تصرف غير قانوني، يرتكب باستخدام تقنيات المعلومات والاتصالات، بما فيه حيازة مواد ممنوعة، او توزيعها، أو عرضها[1].

كما تعرف على أنها:" مجموعة الافعال والاعمال غير القانونية التي تتم عبر معدات أو أجهزة الكترونية أو شبكة الأنترنيت او تبث عبرها محتوياتها، وهي ذلك النوع من الجرائم التي تتطلب الإلمام الخاص بتقنيات الحاسب الآلي ونظم المعلومات لارتكابها أو التحقيق فيها ومقاضاة فاعليها"[2].

ثانيا : خصائص الجريمة السيبرانية :

إن ارتباط الجريمة السيبرانية بالانترنيت ميزها عن الجريمة التقليدية بعدة خصائص نذكر منها ما يلي :

- ترتكب عبر شبكة الانترنيت، فهي حلقة الوصل بين اطراف الجريمة.

[1] منى الأشقر جبور، **مرجع سابق**، ص 50.
[2] عبد الفتاح مراد، **شرح جرائم الكمبيوتر والانترنيت**، دار الكتب والوثائق المصرية، دط، دت، ص 38.

- جريمة عابرة للحدود، فهي تستفيد من خصائص الفضاء السيبراني.
- صعوبة اثبات الجريمة السيبرانية ، نظرا لإمكانية التخفي وتزوير الهوية وصعوبة تتبع مصدر الجريمة.
- ارتفاع حجم الخسائر الناتج عن الجرائم السيبرانية ، خاصة إذا تعلق الامر بالجرائم المالية.
- المجرمون على درجة كبيرة من الذكاء والتطور التكنولوجي.
- قلة عدد التبليغات عن الجرائم السيبرانية ، بسبب الخوف من التشهير وفقدان السمعة، او لعدم القدرة على اكتشاف الجريمة إلا بعد وقت طويل من حدوثها.

ثالثا : المجرمون السيبرانيون :

يملك المجرمون السيبرانيون في أغلب الحالات معلومات وتكنولوجيا أكثر تقدما من ضحاياهم، مما يعطي أفضلية للمهاجم اكثر من المدافع عن انظمة الكمبيوتر.

ويقوم المهاجم باستغلال نقاط الضعف، او الثغرات الامنية، في اي نظام معلوماتي، من اجل الاعتداء على أمن الشبكة والانترنيت.

ويختلف نوع المجرمين السيبرانيين، بناء على الأهداف والدوافع، حيث نجد الباحث عن التسلية، والباحث عن المعرفة، وعن استكشاف كيفية عمل الأنظمة، والخدمات والوظائف التي تقوم بها، ومنهم من يرغب بإثبات قدرته الفكرية والتقنية، او إثبات وجهة نظره، كما يوجد من يبحث عن الانتقام وعن وسيلة لانزال الضرر بالغير، أو المجرم الذي يسعى إلى الابتزاز والسرقة، والاعتداء على الأنظمة الاقتصادية والسياسية والاجتماعية[1].

[1] منى الأشقر جبور، **مرجع سابق**، ص 52.

رابعا : أهم الجرائم السيبرانية :

يمكن اعتبار العمل الجرمي المحدد قانونا جريمة سيبرانية عندما يستهدف الهجوم[1] :

- أمن المعلومات، أي مصداقيتها، وتوافرها، وصحتها، وتندرج في هذا الاطار، عمليات اختراق الانظمة، عبر سرقة كلمة السر، أو التصيد، أو التضليل والاحتيال، كما عمليات تدمير البيانات وسرقتها.
- سلامة الاشخاص، كما هو حال التربص والترصد للأطفال، بغية الاعتداء عليهم، واستدراجهم، بهدف استغلالهم جنسيا، كما تندرج هما عمليات استدراج الاشخاص، في اطار عمليات الاتجار بالرقيق، او تجارة الاعضاء البشرية، أو انتاج المواد الاباحية، او تقديمها.
- الأموال، من خلال عمليات الغش، والاحتيال، التزوير، الابتزاز، تبييض الاموال ...الخ.
- المحتوى، كتوزيع مواد اباحية عن الاطفال، بث الكراهية، التمييز العنصري، عرض خدمات المرتزقة، الترويج للإرهاب.
- أمن الدولة، وسيادتها، مثل التجسس، وافشاء معلومات سرية.
- الملكية الفكرية، والتي يدخل فيها سرقة البرامج والقرصنة، والاستعمال غير الشرعي لإنتاج محمي بالملكية الفكرية.

[1] منى الأشقر جبور، **مرجع سابق**، ص 50.

المطلب الثاني: الارهاب السيبراني.

ظهر مفهوم الإرهاب السيبراني كتهديد أمني جديد عابر للحدود، للدول والمجتمعات، حيث يقوم على استخدام التقنيات الحديثة لشن هجومات إرهابية بهدف نشر الخوف والرعب.

أولا : تعريف الإرهاب السيبراني:

لابد من الإشارة إلى أن الإرهاب والإنترنت مرتبطان بطريقتين هما:

- ممارسة الأعمال التخريبية عبر شبكات الحاسوب والإنترنت.
- أن الإنترنت أصبحت منبرا للجماعات والأفراد لنشر رسائل الكراهية والعنف، وللاتصال ببعضهم البعض وبمؤيديهم والمتعاطفين معهم.

عرف **جيمس لويس James Lewiss** الارهاب السيبرانيعلى أنه :"استخدام أدوات شبكات الحاسوب في تدمير أو تعطيل البني التحتية الوطنية المهمة مثل :الطاقة والنقل،أو بهدف ترهيب الحكومة والمدنيين[1]".

ثانيا : وسائل الإرهاب السيبراني:

البريد الإلكتروني: يعد من أبرز وسائل الإرهاب السيبراني، حيث يستخدم البريد الإلكتروني في التواصل بين الإرهابيين وتبادل المعلومات بينهم.

إنشاء مواقع الانترنت: سهلت على المنظمات الإرهابية توسيع أنشطتهم من خلال تبادل الآراء والأفكار والمعلومات.

اختراق وتدمير المواقع : تتم عملية الاختراق السيبراني عن طريق تسريب البيانات الرئيسة والرموز الخاصة ببرامج شبكة الإنترنت، و تدمير المواقع هو الدخول غير المشروع بهدف تخريب الموقع أو نشر رسائل تشيد بالإرهاب[1].

[1] Alix Desforges**, Cyberterrorisme : quel périmètre ?,** Fiche de l'Irsem n° 11, 2011, P 03.

ثالثا : استخدام الجماعات الإرهابية للفضاء السيبراني:

تعمل الجماعات الإرهابية على استخدام التكنولوجيا المتطورة لنشر مبادئها وتصوراتها ، والقيام بعدة أعمال تخريبية، وذلك من خلال ما يلي:[2]

الاتصال : تستخدم الجماعات الإرهابية الانترنت للاتصال بين أعضائها وتمويل عملياتهم، والحصول على المعلومات الحساسة.

نشر الأفكار المتطرفة: تعمل الجماعات الإرهابية على نشر التطرف من خلال مواقع التواصل الاجتماعي وغرف الدردشة خاصة فئة الشباب لاستغلالهم في العمليات الإرهابية.

فمثلا، تكشف عدة تقارير أن التنظيم الإرهابي "داعش" لديه 90 ألف صفحة باللغة العربية على موقع التواصل الاجتماعي الفايسبوك و40 ألف بلغات أخرى ، إضافة إلى موقع الكترونيللتجنيد بسبعة لغات[3].

التخطيط والتنسيق : تستخدم الجماعات الإرهابية الانترنت للتخطيط والتنسيق فيما بينها وتدبير الهجمات الإرهابية، فقد تم التخطيط لهجمات 11 سبتمبر عبر الرسائل الالكترونية وغرف الدردشة، كما نجحت داعش في التخطيط والتنسيق لعملياتها الإرهابية الكبرى في أوروباعبر الفضاء السيبراني، وخاصة في فرنسا وبلجيكا، وفشلت أجهزة المخابرات الأوروبية في رصد العمليات قبل وقوعها[4].

---

[1] عبد الرحمن بن عبد الله السند ،**وسائل الإرهاب الإلكتروني وحكمها في الإسلام وطرق مكافحتها** من الموقع :http://shamela.ws/browse.php/book-1244/page-20تاريخ الاطلاع :21-04-2018.

[2]عبدالله بن عبدالعزيز بن فهد العجلان،**الإرهابالإلكترونيفي عصر المعلومات**،بحث مقدم إلى المؤتمر الدولي الأول حول "حماية أمن المعلومات والخصوصية في قانون الإنترنت"، القاهرة، 2008.

[3]إيهاب شوقي، **الارهاب الالكتروني وجرائمه**، شبكة الاخبار العربية، على الموقع : https://www.assakina.com/awareness-net/rebounds/81251.html تاريخ الاطلاع: 2018/04/11.

[4]أيمن حسين ،**الإرهاب الالكتروني أخطر معارك حروب الفضاء**، من الموقع : http://alwatan.com/details/166324تاريخ النشر :2017/01/14، تاريخ الاطلاع:20-04-2018 .

التلقين الالكتروني: تسعى الجماعات الإرهابية من خلال الوسائل الالكترونية إلى تقديم إرشادات وطرق صنع القنابل اليدوية والأسلحة الكيماوية الفتاكة وأساليب التفخيخ والتفجير.

التمويل الالكتروني: تحظى الجماعات الإرهابية بتمويل إلكتروني، وتنظم حملات لجمعالتبرعات المالية، خاصة مع انتشار العملات الالكترونية (مثل : البيتكوين).

رابعا : مظاهر تهديد الإرهاب السيبراني لأمن الدول:

تستطيع الجماعات والمنظمات الإرهابية تدمير البنية المعلوماتية للمؤسسات الحكومية، وغيرها من الكيانات التي تعتمد على شبكة الانترنت، والذي يؤدي بدوره إلى إحداث خلل في عمل الدولة والإضرار بمواطنيها وأمنها القومي، ومن تداعيات الإرهاب السيبراني ما يلي :

تهديد أمني سياسي: تعمل المنظمات الإرهابية على إلحاق الشلل بأنظمة القيادة والسيطرة والاتصالات، أو تعطيل أنظمة الدفاع الجوي، إضافة لاختراق البريد الإلكتروني لرؤساء الدول وكبار الشخصيات السياسية، واختراق المواقع الالكترونية لنشر رسائل مضللة.

ففي عام 2010 قام "**ويكيليكس**" بتسريب وثائق تحوي معلومات سرية مُتداولة بين الإدارة الأمريكية وقنصلياتها الخارجية بدول العالم[1]، وفي مارس 2014 هاجمت مجموعة "**سايبربيركوت**" الأوكرانية المواقع الإلكترونية لحلف الناتو، ما أدى إلى تعطيل مواقع الحلف لعدة ساعات". وأقر مفتش وحدة الجرائم السيبرانية الأمريكي في أوت 2014، بأن قراصنة أجانب تمكنوا من اختراق حاسبات تابعة للهيئة الأمريكية لتنظيم الأنشطة النووية مرتين على الأقل خلال السنوات الثلاث الماضية، ومؤخراً أكدت صحيفة نيويورك تايمز في تقرير لها في 26 إبريل 2015 أن قراصنة روسيين اطلعوا على رسائل إلكترونية للرئيس الأمريكي

[1] شيريهان نشأت المنيري، "**مخاطر جرائم الانترنت على استقرار النظام الدولي**"،مجلة السياسة الدولية،من الموقع: http://www.siyassa.org.eg/NewsQ/2450.aspx تاريخ الاطلاع :20-04-2018.

باراك أوباما العام الماضي، بعدما تمكنوا من اختراق الشبكة الإلكترونية غير السرية للبيت الأبيض، واطلعوا على أرشيف الرسائل الإلكترونية لموظفين في البيت الأبيض يتواصلون يومياً مع أوباما، ومن خلال هذا الأرشيف تمكن القراصنة من قراءة رسائل تلقاها أوباما[1] وهذا يعد تهديدا خطيرا للأمن القومي الأمريكي.

أما أمنيا تعمل الجماعات الإرهابية على التسلل الإلكتروني إلى الأنظمة الأمنية في دولة ما وشلها، وفك الشفرات السرية للتحكم بتشغيل منصات إطلاق الصواريخ الإستراتيجية، والأسلحة الفتاكة، وتعطيل مراكز القيادة والسيطرة العسكرية ووسائل الاتصال للجيوش بهدف عزلها عن قواتها، والنفاذ إلى النظم العسكرية واستخدامها لتوجيه الجنود إلى نقطة غير آمنة قبل قصفها أو تفجيرها[2].

تهديد اقتصادي: اختراق النظام المصرفي وإلحاق الضرر بأعمال البنوك وأسواق المال ، وتعطيل عمليات التحويل المالي، وإلحاق الأذى بالاقتصاد الوطني، ومن أمثلتها قيام الإرهابيين بتحويل ملايين الدولارات من بعض الحسابات الشخصية لكبار العملاء بعد إختراق نظام التحويلات الدولي بين البنوك، وقيام بعض الهاكرز المحترفين بسرقة بيانات بطاقات الإئتمان من بعض أكبر مراكز التسوق الإلكتروني الدولية وخصم ملايين الدولارات من أصحاب تلك البطاقاتلتوفير تمويل لأعمالها الإرهابية في الدول التي تم بيع السندات فيها[3].

---

[1] هاجر حسونة، **الإرهاب الالكتروني ...هل يتحول إلى مصدر التهديد الأول في العالم**، من الموقع : http://alkhaleejonline.net/articles/1430728333185670700/ تاريخ النشر: 2015/05/04 تم الاطلاع :21-04-2018.

[2] عبدالله بن عبدالعزيز بن فهد العجلان، **مرجع سابق**،ص22.

[3] أيمن حسين ، مرجع سابق.

أكدت شركة "**كاسبرسكي**" الرائدة في مجال الأمن المعلوماتي أن مجموعة من "الهاكرز" تمكنوا من السيطرة على حسابات في مصارف عالمية، وسرقة نحو مليار دولار[1].

تهديد اجتماعي : توجه المنظمات الإرهابية رسائلها للإعلام والجمهور الخاص بالمجتمعات التي تقوم بترويعها وإرهابها، وذلك بهدف شن حملات نفسية ضد الدول، فهي تعرض أفلاما مرعبة للرهائن والأسرى أثناء إعدامهم، مما يؤثر على المدنيين.

المطلب الثالث : الحروب السيبرانية.

تكمن خطورة الحروب السيبرانية في كون العالم أصبح يعتمد أكثر فأكثر على الفضاء السيبراني،لا سيما في البنى التحتية المعلوماتية، ولا شك أن ازدياد الهجمات السيبرانية يعني إمكانية تطورها لتصبح سلاحا حاسما في النزاعات بين الدول في المستقبل.

أولا : مفهوم الحرب السيبرانية :

لا يوجد إجماع على تعريف محدد ودقيق لمفهوم الحرب السيبرانية،فيعرفها كل من "**ريتشارك كلارك**" و"**روبرت كناكي**" على أنها "أعمال تقوم بها دولة تحاول من خلالها اختراق أجهزة الكمبيوتر والشبكات التابعة لدولة أخرى بهدف تحقيق أضرار بالغة أو تعطيلها[2]".

ويعرفها "**بولو شاكريان**" Paulo Shakarianبأنها :" امتداد للسياسة من خلال الإجراءات المتخذة في الفضاء السيبراني من قبل دول أو فاعلين غير دوليين، حيث تشكل تهديدا خطيرا للأمن القومي[3]".

---

[1] هاجر حسونة، **مرجع سابق**.

[2] Richard A. Clarke & Robert knake,**Cyber War: The NextThreat to National Security and What to Do About It**, HarperCollins, 2010, p:6.

[3] Paulo & Jana Shakarian, Andrew Ruef, **Introduction to Cyber warfare, A multidisciplinaryApproach**, Elsevier, 2013, P 02.

يقترح آخرون أن يتم التركيز بدلا من ذلك على أنواع وأشكال النزاع التي تحصل في الفضاء السيبراني، ويحددون مستوياتها كالتالي :

- **القرصنة السيبرانية: وتقع في المستوى الأول**،ومن أمثلته القيام بعمليات قرصنة المواقع الإلكترونية أو بتعطيل الحواسيب الخادمة (Servers) من خلال إغراقها بالبيانات.

- **الجريمة السيبرانية والتجسس السيبراني:** ويقعان في المستوى الثاني والثالث وغالبا ما يستهدفان الشركات والمؤسسات وفي حالات نادرة بعض المؤسسات الحكومية.

- **الإرهاب السيبراني: ويقع في المستوى الرابع**،ويعبر عن الهجمات غير الشرعية التي ينفذها فاعلون غير حكوميون ضد أجهزة الكمبيوتر والشبكات والمعلومات المخزّنة.

- **الحرب السيبرانية:** وهي المستوى الأخطر للنزاع في الفضاء السيبراني،وتهدف إلى التأثير على الإرادةالسياسيةللطرف المستهدف وقدرته في عملية صنع القرار، وكذلك التأثير فيما يتعلق بالقيادة العسكرية و/أو توجهات المدنيين في مسرح العمليات الإلكتروني.

ثانيا : خصائص الحروب السيبرانية.

من المتوقع أن تصبح الحرب السيبرانية نموذجا تسعى إليه العديد من الجهات نظرا للخصائص العديدة التي تنطوي عليها، ومنها:

- **حروب لا تناظرية (Asymmetric)** [1]: فالتكلفة المتدنية نسبيا للأدوات اللازمة لشن هكذا حروب يعني أنّه ليس هناك حاجة لدولة معينة او منظمة ما،لقدرات ضخمة لتشكل تهديدا خطيرا وحقيقيا على دولة مثل الولايات المتّحدة الأمريكية.

[1] **المجال الخامس.. الحروب الإلكترونية في القرن الـ21**، مركز الجزيرة للدراسات، على الموقع : http://studies.aljazeera.net/ar/issues/2010/20117212274346868.html ، تاريخ الاطلاع : 15-03-2018

- **تمتع المهاجم بأفضلية واضحة**[1]: فهذه الحروب تتميز بالسرعة والمرونة والمراوغة. وفي بيئة مماثلة يتمتّع المهاجم بأفضلية، ومن الصعوبةنجاح عمليات الدفاع.

- **المخاطر تتعدى استهداف المواقع العسكرية**[2]: هناك جهود متزايدة لاستهداف البنى التحتية المدنية والحسّاسة كاستهداف شبكات الكهرباء والطاقة وشبكات النقل والنظام المالي والمنشآت الحساسة النفطية أو المائية أو الصناعية بواسطة فيروس يمكنه إحداث أضرار مادّية حقيقية تؤدي الى دمار هائل.

ثالثا : تداعيات الحروب السيبرانية على الامن القومي.

سببت الحروب السيبرانية جملة من المخاطر والتداعيات على تفاعلات السياسة الدولية، يمكن طرح أبرزها على النحو الآتي[3]:

1. **تصاعد المخاطر السيبرانية**، خاصة مع قابلية المنشآت الحيوية (مدنية وعسكرية) في الدول للهجوم، الأمر الذي يؤثر في وظائف تلك المنشآت. وبالتالي، فإن التحكم في تنفيذ هذا الهجوم يعد أداة سيطرة استراتيجية .
2. **تعزيز القوة وانتشارها**، عمل الفضاء السيبراني على إعادة تشكيل قدرة الأطراف المؤثرة، وأدى الى عملية انتشار القوة بين فاعلين متعددين.
3. **عسكرة الفضاء السيبراني**، حيث برز في هذا الإطار عدة اتجاهات، مثل التطور في مجال سياسات الدفاع والأمن السيبراني، وتصاعد القدرات في سباق التسلح السيبراني، وتبني سياسات دفاعية سيبرانية لدي الأجهزة المعنية بالدفاع والأمن في الدول، وتزايد الاستثمار في مجال تطوير أدوات الحرب السيبرانية داخل الجيوش الحديثة.

---

[1] **المجال الخامس.. الحروب الإلكترونية في القرن الـ21، مرجع سابق.**
[2] **المجال الخامس.. الحروب الإلكترونية في القرن الـ21، مرجع سابق.**
[3] عادل عبد الصادق، **الحروب السيبرانية : تصاعد القدرات والتحديات للأمن العالمي**، المركز العربي لأبحاث الفضاء الالكتروني. على الموقع :http://accronline.com/article_detail.aspx?id=28395 ، تاريخ الاطلاع : 15-02-2018.

4. **إدماج الفضاء السيبراني ضمن الأمن القومي للدول**، وذلك عبر تحديث الجيوش، وتشكيل وحدات متخصصة في الحروب السيبرانية، وإقامة هيئات وطنية للأمن والدفاع السيبراني، والقيام بالتدريب، وإجراء المناورات لتعزيز الدفاعات السيبرانية.
5. **الاستعداد لحروب المستقبل**، حيث تتبنى العديد من الدول استراتيجية حرب المعلومات باعتبارها حربا للمستقبل، وترى الدول الكبرى أن من يحدد مصير تلك المعركة المستقبلية ليس من يملك القوة فقط، وإنما القادر على شل القوة، والتشويش على المعلومة.

المبحث الثالث :جهود الدول لمواجهة التهديدات السيبرانية.

قام الباحث في هذا المبحث، بالتطرق إلى مختلف الجهود الوطنية والدولية من أجل مواجهة التهديدات السيبرانية، سواء في الجانب التقني أو الجانب القانوني,

المطلب الأول: الجهود الوطنية لتأمين الفضاء السيبراني.

أولا : بناء الجيوش السيبرانية :

كان للتطور السريع للتكنولوجيا، خاصة الحرب السيبرانية تحديا لمفاهيم الأمن القومي، حيث أصبحت قضية الدفاع عن البنية القومية للمعلومات ذات أهمية قصوى، وعليه سعت معظم الدول إلى تشكيل جيوش سيبرانية ورصدت ميزانيات ضخمة للتطوير في مجال الهجوم والدفاع والحماية.

وحسب الوكالة الروسية للاستشارات الأمنية **زيكوريون** فإن الولايات المتحدة تنفق أكثر على أمن الفضاء السيبراني أكثر من أي بلد آخر، فوزارة الدفاع لديها ميزانية سنوية تبلغ 07 مليارات دولار للأمن السيبراني، وعدد الموظفين القراصنة يبلغ أكثر من 9000

موظف، وتنفق كل من الصين والمملكة المتحدة سنويا 1.5 مليار دولار و 450 مليون دولار، على التوالي.

وخصصت كوريا الشمالية نحو 20% من الميزانية العسكرية للأمن السيبراني. ويحتل الجيش السيبراني الروسي المرتبة الخامسة في العالم، حيث تظهر التقارير أن قوات الأمن السيبراني الروسية وصلت إلى 1000 موظف، وتنفق وزارة الدفاع الروسية حوالي 300 مليون دولار سنويا على مثل هذه الأنشطة[1].

ثانيا : تشكيل هيئات وطنية للأمن السيبراني: بما أن التهديدات السيبرانية لا تفرق بين مدني وعسكري، سعت الدول إلى تشكيل هيئات متخصصة في الأمن السيبراني، تكون مهمتها:

- ✓ إعداد الإستراتيجية الوطنية للأمن السيبراني، والإشراف على تنفيذها.
- ✓ وضع السياسات وآليات الحوكمة والإرشادات المتعلقة بالأمن السيبراني وتعميمه.
- ✓ وضع أطر إدارة المخاطر المتعلقة بالأمن السيبراني.
- ✓ وضع أطر الاستجابة للحوادث والاختراقات.
- ✓ وضع السياسات والمعايير الوطنية للتشفير.
- ✓ رفع مستوى الوعي بالأمن السيبراني.

كما يحدد الإتحاد الدولي للاتصالاتITU خمسة معايير لتصنيف مستوى الأمن السيبراني للدول وهي كالتالي : معاير تشريعية، تقنية، تنظيمية، بناء القدرات، ومعيار التعاون[2].

[1] **أفضل خمسة جيوش الكترونية في العالم** ، مركز الدراسات كاتيخون ، على الموقع: http://katehon.com/ar/article/mhy-fdl-khms-jywsh-lktrwny-fy-llm-wm-trtyb-ljysh-lsybrny-lrwsy تاريخ النشر : 2017/01/13 ، تاريخ الاطلاع : 2018/04/22

[2] **مؤشر الأمن السيبراني العالمي**، الاتحاد الدولي للاتصالات، 2017، ص 17. على الموقع : https://www.itu.int/pub/D-STR-GCI.01-2017

جدول رقم 01 : ترتيب الدول الأكثر أمنا في الفضاء السيبراني حسب الاتحاد الدولي للاتصالات

Country	GCI Score	Legal	Technical	Organizational	Capacity Building	Cooperation
Singapore	0.92	0.95	0.96	0.88	0.97	0.87
United States	0.91	1	0.96	0.92	1	0.73
Malaysia	0.89	0.87	0.96	0.77	1	0.87
Oman	0.87	0.98	0.82	0.85	0.95	0.75
Estonia	0.84	0.99	0.82	0.85	0.94	0.64
Mauritius	0.82	0.85	0.96	0.74	0.91	0.70
Australia	0.82	0.94	0.96	0.86	0.94	0.44
Georgia	0.81	0.91	0.77	0.82	0.90	0.70
France	0.81	0.94	0.96	0.60	1	0.61
Canada	0.81	0.94	0.93	0.71	0.82	0.70

المصدر: مؤشر الأمن السيبراني العالمي 2017، الاتحاد الدولي للاتصالات

ثالثا : التشريعات الوطنية للأمن السيبراني.

سن العديدمن 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[1].

وتعتبر المبادرات التشريعية الأمريكية، حول الأمن السيبراني، من أهم المبادرات في العالم التي تعالج مشكلة التهديدات، ذلك أنها ارتبطت مباشرة بمحاربة الإرهاب.

هذا إضافة إلى أن معظم الدول الأوروبية والآسيوية، والعربية، وغيرها من دول العالم التي أضافت إلى قانونها الجزائي ملحقا خاصا لمكافحة الجريمة السيبرانية (مثل الجزائر)، وهناك ثلاث دول عربية فقط سنت قوانين مستقلة لمكافحة الجرائم السيبرانية، هي السعودية

[1] حسن بن أحمد الشهري،**"الإرهاب الالكتروني – حرب الشبكات-"** ،المجلة العربية الدولية للمعلوماتية، 2015، ص 19.

وعمان والإمارات العربية المتحدة، هذه الأخيرة التي تعتبر رائدة في المنطقة العربية في إصدار تشريعات الأمن السيبراني، حيث صدر **قانون مكافحة الجرائم السيبرانية** عام 2012، ثم تم تعديله في 2016، وقد دعم بمجموعة من السياسات التنظيمية والمعايير التقنية لتمكين مستخدمي الفضاء السيبراني ومقدمي الخدمات من الحصول على الظروف الأمنية اللازمة لحماية النظم الحساسة والبنية التحتية والبيانات، فضلا عن حماية المستخدمين[1].

المطلب الثاني: الجهود الدولية– من أجل فضاء سيبراني سلمي –

أولا : الحد من سباق التسلح السيبراني.

يلعب 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[2]، لقد بدأ سباق تسلح خطير لتطوير الأسلحة السيبرانية، كانت بداية ظهوره (يعتبر المختصون هذه الاسلحة السيبرانية بدائية) في الصراع الروسي– الاستوني، والروسي– الجورجي، والتطور البارز مع فيروس "ستاكسنت" الموجه ضد البرنامج النووي الإيراني والذي يتهم بتطويره كل من اسرائيل والولايات المتحدة.

[1] فاروق حاتم، **الإمارات تتقدم دول المنطقة في إصدار تشريعات الأمن السيبراني**، جريدة الاتحاد، على الرابط : http://www.alittihad.ae/details.php?id=66522&y=2017&article=full تاريخ النشر : 2017/11/08 تاريخ الاطلاع : 2018/04/21

[2] عادل عبد الصادق، **أسلحةالفضاء الالكتروني في ضوء القانون الدولي**، سلسلة أوراق، العدد 23، مكتبة الاسكندرية،2016، ص 64.

واتجهت الدول لتعزيز قدراتها السيبرانية سواء في مجال الدفاع والردع أو الهجوم، بالإضافة الى حماية بنيتها القومية للمعلومات، وذلك من خلال السعي إلى امتلاك التكنولوجيا وأنظمة الحماية، والعمل على تحقيق التفوق التقني.

وعليه، فإن المشكلة في سباق التسلح السيبراني تكمن في تحديد ماهية تلك الأسلحة، ومن ثم لا يصبح لدى المجتمع الدولي القدرة على التدخل لاحتواء التقدم في مجال تلك الأسلحة.

وحسب **جوزيف.س ناي** أنه يمكننا أن نتعلم من تاريخ العصر النووي. وفي حين أن التكنولوجيات السيبرانية والنووية تختلف اختلافًا كبيراً، فإن العملية التي يتعلم المجتمع من خلالها التعامل مع تكنولوجيا شديدة التعطيل، وفى المجال السيبرانى اقترحت روسيا في عام 1999، معاهدة للأمم المتحدة لحظر الأسلحة الإلكترونية والمعلوماتية (بما في ذلك الدعاية).

قاومت الولايات المتحدة ما اعتبرته محاولة للحد من القدرات الأمريكية، ولا تزال تعتبر هذه المعاهدة عامة مضللة لا يمكن التحقق منها، وبدلاً من ذلك اتفقت الولايات المتحدة وروسيا و13 دولة أخرى على أن يعين الأمين العام للأمم المتحدة مجموعة من الخبراء الحكوميين التي اجتمعت أولاً في عام 2004.

وقد أسفرت تلك المجموعة في البداية عن نتائج هزيلة، ولكن بحلول جوان 2015، أصدرت تقريراً أقرته مجموعة العشرين، يقضي بوضع معايير مقترحة لبناء الثقة[1].

[1] جوزيف.س ناي، **التحكم في الصراع السيبراني**، مدونات الجزيرة، على الرابط :

http://blogs.aljazeera.net/blogs/2017/8/، تاريخ النشر : 8-9-2017، تاريخ الاطلاع : 28-03-2018

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، يجب أن يعمل على منع نشر الأسلحة السيبرانية في وقت السلم، والسماح بالجهود الجماعية للدول أو المنظمات لتجنب التأثير على الاستخدام المدني للفضاء السيبراني.

ثانيا : قانون تالين.

نظرا لصعوبة الحد من سباق التسلح السيبراني، من جهة، وقصور القانون الدولي في هذا المجال، نتيجة عدم وجود أي أساس قانوني ينظم اللجوء إلى الحروب السيبرانية، من جهة اخرى، تم ابرام صك قانوني عام 2013 يدعى "دليل تالين"Tallin manaul، الذي أعدته مجموعة من خبراء القانون الدولي بدعوة من حلف شمال الأطلسيNATO، قصد دراسة مدى إمكانية تطبيق قواعد القانون الدولي الإنساني على الحروب السيبرانية، وذلك إثر الهجوم السيبراني الشامل الذي شنته روسيا ضد إستونيا عام2007[1].

ويحتوي دليل "تالين" على 95 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[2].

[1] سعيد درويش،**"ماهية الحرب الالكترونية في ضوء قواعد القانون الدولي"**، حوليات جامعة الجزائر 1، العدد29، ص 119.

[2] اللجنة الدولية للصليب الأحمر، **ما هي القيود التي يفرضها قانون الحرب على الهجمات السيبرانية؟**، على الرابط: https://www.icrc.org/ara/resources/documents/faq/130628-cyber-warfare-q-and-a-eng.htm تاريخ النشر : 28-03-2013، تاريخ الاطلاع : 24-04-2018.

ويجيب دليل "تالين" على أهم النقاط الحساسة ذات الصلة بالحروب والهجمات السيبرانية التي تنفذها الدول، أو تلك التي تقوم بها جهات فاعلة من دون الدول، كمفهوم النزاع المسلح في اطار الحرب السيبرانية، وكذا مفهوم الجيوش السيبرانية وكيفية ادارة الحرب السيبرانية من خلال قواعد الاشتباك السيبراني، وصفة المقاتل السيبراني، إضافة الى امكانية مراعاة القانون الدولي الانساني المعروفة كمبدأ التمييز، ومدى شرعية استهداف المقاتل السيبراني بالوسائل العسكرية المادية كالطائرات العسكرية بدون طيار.

ويقصر دليل "تالين" الهجوم السيبراني على أنه "عملية إلكترونية سواء هجومية أو دفاعية يتوقع أن تتسبب في إصابة أو قتل أشخاص أو الإضرار بأعيان أو تدميرها"، لكن لم يتفق الخبراء حول "الضرر"، فهو يتوقف على كل بلد أن يقرر حجم الضرر الكافي لتبرير خوض الحرب، وهذا ما يعرف بنظرية اللجوء إلى الحرب (Jus ad bellum)، بحيث يشترط أن تكون مبررة وعادلة، لكي يمكن إضفاء صفة المشروعية عليها[1].

ثالثا: الاتفاقيات الإقليمية والدولية لأمن الفضاء السيبراني.

تنسجم الاتفاقيات الإقليمية مع متطلبات مواكبة سرعة تطور التهديدات السيبرانية، ويسجل في هذا المجال، عدد من المبادرات نذكر منها[2] :

- في عام 2002، وضعت مجموعة بلدان الكومنولث قانونا نموذجيا لمكافحة الجريمة السيبرانية، إضافة إلى قانون الإثبات الرقمي.
- في عام 2009، بادرت المجموعة الاقتصادية لغرب إفريقيا، إلى إقرار توصية لمكافحة الجريمة السيبرانية، تشكل الإطار القانوني لعمل الدول الأعضاء.
- جاءت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات عام 2011، لتعزيز التعاون بين الدول العربية لمكافحة الجرائم السيبرانية والحفاظ على أمنها وسلامة مجتمعاتها.

[1] سعيد درويش، مرجع سابق، ص 133.
[2] منى الأشقر جبور، **السيبرانية هاجس العصر**، مرجع سابق، ص 103-104.

- وتعتبر اتفاقية **بودابست** 2001 (الاتفاقية الأوروبية لمكافحة الجريمة السيبرانية)، خطوة رائدة على مستوى التعاون بين الدول، وهي الوحيدة من حيث المدى وحجم الدول المنضمة إليها، دخلت حيز التنفيذ عام 2004، 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.

أما على المستوى الدولي، فقد لعبت هيئة الأمم المتحدة عبر القرارات الصادرة عنها التي تدعم الأمن والسلامة في الفضاء السيبراني، وتوعية الوعي العالمي بالأمن السيبراني دورا في جذب انتباه الدول الأعضاء إلى أهمية التحديات السيبرانية.

ومن أهم القرارات الصادرة عن الهيئة :

- قرار صادر سنة 1990، حول قانون جرائم المعلوماتية.
- قرار صادر سنة 1991، حول مكافحة الاستخدام الجرمي لتقنيات المعلومات والاتصالات.
- عام 2001، إنشاء "مجموعة الخبراء الحكومية GGE"، بدأت عملها في 2004، لمناقشة الأخطار القائمة والمحتملة في مجال أمن المعلومات، والإجراءات الممكنة لوضع الأسس الدولية التي تهدف إلى تقوية أمن نظم الاتصالات والمعلومات العالمية.
- في العام 2003، صدر قرار خاص حول الأمن السيبراني، ركز على القدرة على مكافحة الجريمة السيبرانية[1].
- في العام 2010، صدر قرار حول الأمن السيبراني، وملحق حول ضرورة أن تلجأ الدول، لمعرفة مدى تناسب أطرها التشريعية وقدرتها على مكافحة الجريمة السيبرانية.

[1] عادل عبد الصادق، **الإرهاب الالكتروني والقوة في العلاقات الدولية: نمط جديد وتحديات مختلفة**، مركز الدراسات السياسية والاستراتيجية، القاهرة، 2009، ص 334.

كما بذلت جهود عدة، من قبل مجموعات عمل متخصصة، بدعم من الاتحاد الدولي للاتصالات، لإقرار مجموعة من المعايير والقواعد، التي تضمن الاستخدام السلمي للمجال السيبراني.

لكن تبقى هذه الجهود، والمقررات والتوصيات، بالرغم من قيمتها على المستوى الدولي، غير كافية ولا فاعلة، نظرا لعدم الزاميتها القانونية، ولعدم إتاحتها إمكانية العقاب، هذا عدا عن الهوة الرقمية بين الدول، التي تزرع الشك بدل الثقة، خاصة مع سيطرة الولايات المتحدة الأمريكية على الانترنيت.

خلاصة الفصل الثاني:

بعد نهاية الفصل الثاني، نخلص الى أن الأمن السيبراني أصبح قضية بالغة الاهمية من قضايا الأمن القومي، حيث قامت معظم الدول بتطوير عقيدتها الأمنية لتتلائم مع المتغير الجديد، وهذا في محاولة لمواجهة التهديدات السيبرانية التي تزداد وتتطور بسرعة، فالجريمة والارهابوالحرب في الفضاء السيبراني تعد من بين التحديات الأمنية الجديدة أمام الدول.

لذلك، فالدول تسعى لحماية امنها القومي ومواجهة التهديدات السيبرانية، من خلال العمل على مسارين، الأول تقني، عبر تطوير الجيوش السيبرانية، وانشاء هيئات الأمن السيبراني، والثاني قانوني، من خلال سن تشريعات وطنية، إقليمية، دولية لمكافحة الجريمة والارهاب السيبراني، والعمل على الحد من سباق التسلح وعسكرة الفضاء السيبراني.

الفصل الثالث:

الولايات المتحدة الأمريكية بين الدفاع والهجوم السيبراني

الفصل الثالث:

الولايات المتحدة الأمريكية بين الدفاع والهجوم السيبراني

يبحث هذا الفصل البحث في انعكاسات التهديدات السيبرانية بمختلف انواعها على الامن القومي الأمريكي، وما أفرزته من صراعات بين الولايات المتحدة والدول الكبرى المنافسة، ثم يفصل في السياسات والاستراتيجيات المتبعة لمواجهة المخاطر السيبرانية، من أجل تحقيق الاهداف والمصالح القومية، وبما أن التطورات التكنولوجية تتسارع بشدة، كان لابد من التطرق إلى التهديدات المستقبلية والرؤية الأمريكية لدور الولايات المتحدة في الفضاء السيبراني.

وفي هذا الإطار يقسم الفصل إلى ثلاثة مباحث كالتالي :

المبحث الأول : انعكاسات التهديدات السيبرانية على الأمن القومي الأمريكي.

المبحث الثاني :السياسة السيبرانية الأمريكية واستراتيجيات المواجهة.

المبحث الثالث :مستقبل الفضاء الالكتروني الأمريكي.

المبحث الأول : انعكاسات التهديدات السيبرانية على الأمن القومي الأمريكي.

يعالج هذا المبحث أهم التهديدات السيبرانية على الأمن القومي الأمريكي، ويوضح أهداف الإدارة الأمريكية وأبرز التحديات التي تواجهها في الفضاء السيبراني، ويعطي أمثلة عن الصراعات السيبرانية خاصة مع الصين وروسيا.

المطلب الأول: التهديدات السيبرانية للأمن القومي الأمريكي.

يؤكد **جوزيف.س ناي** أن هناك أربع فئات رئيسية من التهديدات السيبرانية للأمن القومي الامريكي، تختلف في المدى الزمني ومن حيث المبدأ،فالحرب السيبرانية والتجسس الاقتصاديترتبط بالدول، والجريمة السيبرانيةوالإرهاب السيبراني ترتبط بفاعلين من غير الدول، وبالنسبة للولايات المتحدة، فيالوقت الحاضر، تأتي أعلى الخسائر من التجسسوالجريمة، ولكن على مدى العقد المقبل ،قد تصبح الحرب والإرهاب على رأس التهديدات[1].

أولا: الجريمة السيبرانية[2]:

بحسب تقرير صادر عن مركز الدراسات الاستراتيجية في واشنطن بالتعاون مع شركة "**مكافي**" لبرامج الأمن المعلوماتي، الذي نُشر في مطلع فبراير 2018، يظهر نمواً متسارعاً في خسائر الجرائم السيبرانية،حيث انتقلت من 445 مليار دولار في العام 2014 إلى 600 مليار في 2017، مرجعاً ذلك لاستخدام منفّذي الجرائم السيبرانية أساليب تكنولوجية حديثة، إضافة إلى تسهيل نشاط العملات الرقمية لأعمالهم وتحويل الأموال.

ووفق دراسة صدرت العام الماضي عن مؤسسة "**أوبن ثينكينغ**" (مختصة بالتدريب)، فإنه من المتوقع أن تتسبب الهجمات السيبرانية بخسارة الاقتصاد العالمي نحو 3 تريليونات

[1]Joseph S.Nye,jr, **Power and national Security in cyberspace, America's Cyber Future**, Center for a new America Security, V2, 2011, P 16.

[2]**الحروب الالكترونية، معارك العالم الافتراضي تنتقل إلى الميدان**، تقرير للخليج أونلاين، 2018، على الموقع: http://alkhaleejonline.net/articles/1521891769458091700/ تاريخ الاطلاع: 24-04-2018.

دولار بحلول عام 2020، تتكبد الولايات المتحدة الجزء الأكبر منها، إذا لم تتخذ الحكومات التدابير اللازمة لمواجهتها.

ثانيا: التجسس السيبراني:

يستخدم التجسس السيبراني لجمع المعلومات، وعادة ما تكون الدوافع مالية، ويمكن أن يكون لها آثار استراتيجية خطيرة، حيث تهدد قطاعات واسعة، منها العسكرية، السياسية أو الصناعية أو التكنولوجية.

في عام 2008 كانت أخطر الهجمات ضد أنظمة حواسب الجيش، حيث تم نقل آلاف الملفات من البيانات إلى خوادم خارجية، كما تم استهداف أكثر من 72 شركة من بينها 13 من مقاولي وزارة الدفاع بهدف سرقة معلومات حول الخطط والمباني العسكرية، كما قام قراصنة إلكترونيون صينيون بشن هجمات على المواقع الإلكترونية لشركة "**لوكهيد مارتين**" الأمريكية وسرقوا معلومات عن تكنولوجيا تصنيع مقاتلة "أف– 35" التي استخدمتها الصين فيما بعد، في تصميم وتصنيع مقاتلة "تي 20" الصينية[1].

ثالثا: المحرضون:

يستخدم المحرضون الفضاء السيبراني من أجل التأثير أو التخويف أو تضليل الخصم والرأي العام، بدوافع لسياسية أو ايديولوجية، فمنظمة مثل "**انونيموس**" أجرت العديد من الهجمات السيبرانية عالية المستوى، ردا على سجن مؤسس ويكيليكس "**جوليان أسانج**".

يحاول المحرضون زرع الارتباك و تقويض الثقة في فعالية المؤسسات الرسمية الأمريكية مثل الحكومة، أو المؤسسات المالية، حيث أن تسريبات "ويكيليكس"، أو" سنودن"

[1] إيهاب خليفة، **التطبيقات الأمنية لقوة الفضاء الالكتروني**، على الرابط : https://futureuae.com/ar/Mainpage/Item/851/cyber-power تاريخ الاطلاع : 23-04-2018.

زادت من التوتر بين الولايات المتحدة وحلفائها، ودمرت سمعة بعض المسؤولين في الحكومة[1].

رابعا: الحرب السيبرانية[2]:

لا شك أن التدخل الروسي في الانتخابات الرئاسية الأمريكية 2016؛ بهدف التأثير فيها لمصلحة الرئيس **دونالد ترامب** شكلت عهداً جديداً في الحرب السيبرانية، فللمرة الأولى تنتقل الحرب السيبرانية بين الدول إلى الساحة الديمقراطية، بعد أن كانت تقتصر على استهداف المنشآت العسكرية والاستخبارية.

وأكد تقرير لوكالة الاستخبارات الأمريكية في يناير 2017، أن الروس حاولوا "تقويض إيمان المواطنين بالعملية الأمريكية الديمقراطية، وتشويه سمعة الوزيرة هيلاري كلينتون، والتأثير في حظوظها الانتخابية."

لكن واشنطن نفسها لم تكن بمأمن من الحرب السيبرانية، ففي يوم الجمعة 23 مارس 2018 وجهت وزارة العدل الأمريكية اتهامات جنائية، وفرضت عقوبات على شركة إيرانية وعلى 9 إيرانيين ناشطين في معهد "مبنا" الإيراني، لاختراقهم أنظمة مئات الجامعات والشركات وضحايا آخرين، بغية سرقة البحوث والبيانات الأكاديمية والملكية الفكرية.

وفي العام 2014 كشفت صحيفة نيويورك تايمز أن وحدة المحاربين السايبريين في الجيش الصيني هي المسؤولة عن غالبية الهجمات التي تعرَضت لها الشركات الأمريكية، وحتى الوزارات.

وفي نفس السنة، قامت مجموعات تابعة لكوريا الشمالية بقرصنة شركة "**سوني بيكتشرز إنترتينمنت**"، وقطعت واشنطن عنها الإنترنت لمدة 3 أيام، وعزلتها عن العالم طيلة تلك الفترة، كإجراء انتقامي وردعي.

---

[1] Kristin M.lord&Travis Sharp, **America's Cyber Future**,Center for a new America Security, V1, 2011, P 18 .

[2] **الحروب الالكترونية، معارك العالم الافتراضي تنتقل إلى الميدان**، مرجع سابق.

المطلب الثاني : أهداف وتحديات الولايات المتحدة الأمريكية في الفضاء السيبراني.

أولا: الأهداف[1] :

- **ضمان الاتصال:** ويعني الحفاظ على الإنترنت مفتوح وآمن، وذلك لتسهيل عملية النمو الاقتصادي، والقدرة على الابتكار والتقدم العلمي ، وزيادة التفاعل الاجتماعي والثقافي، هذا، بالإضافة إلى مكافحة الجريمة السيبرانية من أجل الحفاظ موثوقية الانترنت خاصة في المعاملات المالية والاقتصادية بما يخدم استمراريةالمصالح الوطنية للولايات المتحدة.
- **ضمان الأمن:** ويكون بردع الهجمات السيبرانية، وزيادةمرونة النظم والشبكات من خلال الهندسة المناسبة، وإنشاء نظام الدفاع بالطبقات"الدفاع في العمق"، إضافة إلى بناء وتطبيق المعايير العالميةفيما يتعلق بالسلوك المقبوللجهات الفاعلة الحكومية وغير الحكومية،وحماية المدنيين، لضمان الاستخدام السليم للقوة السيبرانية كوسيلة لخدمة المصالح القومية للولايات المتحدة.
- **ضمان الهيمنة (القوة):** الحفاظ على ميزة تفوق الجيش الأمريكي الفضاء السيبراني من أجل تعزيز ردع الهجمات خلال وقت السلم والحرب، وحماية المعلومات والأسرار التجارية والملكية الفكرية من التدمير، سواء عبر الجريمة السيبرانية أوالتجسس السيبراني، اللذان يضعفان القدرة التنافسية للولايات المتحدة في الاقتصاد العالمي، إضافة إلى السعي لبناء وتطوير رأس المال التكنولوجي والبشري من أجل تعزيز تنافسية أمريكا في الفضاء السيبراني.

[1]Kristin M.lord&Travis Sharp, **America's Cyber Future**,Center for a new America Security, V1, 2011, P 15.

ثانيا: التحديات:

- **سرعة نقل المعلومات وعدم أهمية الجغرافيا**[1]:تفقد الولايات المتحدةفي الفضاء السيبراني ميزتي الانذار المبكر للهجوم، والقدرة على تحديد الموقع الجغرافي للرد، فالهجوم يتم بسرعة الضوء، والهجمات السيبرانية غير مقيدة بالموقع الجغرافي، فيمكن لأي شخص أن يطلق هجوما من أي مكان في العالم، وعليه فالأهداف سوف تبقى عرضة للهجمات وقد لا يكتشف الفاعل، ولا يتوافر وقت للدفاع، إضافة إلى ان المهاجم يمكن أن يهرب بسرعة شديدة، عبر إعادة التوجيه.
- **حجم وكثافة الهجومات السيبرانية**[2]: تتعرض الولايات المتحدة لهجوم مستمر في الفضاء السيبراني، كما تنمو هذه الهجمات في الحجم والكثافة، مما يزيد خطر وقوع حادث كارثي قد يسبب آثارا اجتماعية كبيرة.

إن عواقب الهجمات السيبرانية المتطورة ضدنظاممالي يعتمد بشكل متزايد على النظام الآلي،تعتبر عالية التكلفة،وتمثل أدوات مثالية للإكراه،كما أن الهجوم على البنية التحتية الحيوية يمكن أن يلحق أضرارا هائلة، ويصبح مجرد التهديد بالهجوم، يمكن أن يجبر الآخرين على تغيير سلوكهم.

- **سهولة الدخول للأنترنيت:** حواجز الدخول إلى الفضاء السيبراني منخفضة جدا، فلإطلاق هجوم على الإنترنت، تحتاج فقط جهاز كمبيوتر واتصال بالإنترنت، ونتيجة لذلك، فإن الفضاء السيبراني يتيح إمكانات وأهداف كبيرة للمهاجمين بتكلفة أقل، على الرغم من أن الهجمات المتطورة التي تشنها الدول تحتاج إلى قدرات عالية[3].

تتزايد احترافية الجرائم السيبرانية، حيث يمكن لأي كان أن يحصل على سلاح سيبراني (فيروس) شديد التأثير في السوق السوداء، عبر البحث في **الانترنيت المظلم Dark Internet**، حيث توجد مزادات لبيع الأسلحة السيبرانية، كما يمكن طلب صناعة فيروس حسب مواصفات معينة، أو طلب القيام بالهجوم على موقع معين من طرف محترفين في القرصنة.

---

[1]Idem, P 24-25.
[2]Idem, P 25.
[3]Idem, P 26-27.

- **عدم وضوح قواعد السلوك:** غالبًا ما تكون معايير السلوك المقبولة غير واضحة في الفضاء السيبراني، لعدم وجود معايير متفق عليها، فالفضاء السيبراني يوفر للمهاجمين ما يكفي من الغموض لتمكينهم من ممارسة الجريمة،التجسس والتحريض والحرب[1].

أحد الجوانب الأكثر تحديًا للأمن السيبرانيهو أن المهاجمين يمكن أن يتسببوا في ضرر كبير، دون تجاوز عتبة النزاع المسلح، أو إثارة استجابة قوية، مثال ذلك فيروس**Stuxnet**، التي دمر أجهزة الطرد المركزي الايرانية، وأخر البرنامج النووي ثمانية سنوات، دون استخدام القوة المادية التي من المحتمل أن تثير ردا أقوى من إيران.

المطلب الثالث : الصراعات السيبرانية للولايات المتحدة الامريكية.

أولا: الصراع الأمريكي–الصيني:

يقول أحد المسؤولين العسكريين الأمريكيين: "هذا الاختراق يعني توفير ملايين من الدولارات كانت ستصرفها الصين لتأمين تفوق وأفضلية عسكرية في حال نشوب حرب.... لقد وفر الصينيون على أنفسهم –جهد ووقت– 25 سنة من البحث والتطوير! إنها معضلة كبرى!"[2].

اتسمت العلاقة بين الولايات المتحدة والصين بقدر كبير من الصراع والتحدي والريبة، وزاد التوتر بينهما في السنوات الأخيرة، خاصة السخط المتبادل حول سلوك كل منهما في الفضاء السيبراني.

فمن وجهة نظر الولايات المتحدة، ثمة ثلاث قضايا رئيسية، تتمثل الشكوى الأساسية في اختراقات الصين المتعددة والمتكررة لشبكات الشركات، بغرض سرقة الملكية الفكرية ومعلومات الملكية التجارية، وكان المصدر الثاني للقلق استخدام الفضاء السيبراني

[1] Idem, P 27-28.

[2] نبيل نايلي، **غنيمة حرب الصين السيبيرية**، على الموقع : http://www.mepanorama.net/295564/ تاريخ الاطلاع : 25-04-2018.

لأغراض تجسسية تقليدية تتعلق بالأمن، ويتمثل المصدر الثالث للقلق في احتمال ان تكون الصين على أهبة الاستعداد لشن هجوم سيبراني بهدف تدمير البنية التحتية الاساسية الأمريكية في حال حدوث ازمة[1].

ومن جانب الصين، فأنها تشجب اتهامات الولايات المتحدة لها بالقرصنة، ويشكو المسؤولون الصينيون من القيود المفروضة على دخول شركات الاتصالات الصينية (**Huawei – ZTE**) إلى الأسواق الامريكية، وتدين الصين "الهيمنة" الامريكية على الانترنيت[2].

شرعت الولايات المتحدة والصين في مباحثات ثنائية رسمية بخصوص الفضاء السيبراني عام 2013، إلا أن الصين أوقفت هذه المباحثات في 2014، بعد إدانة الولايات المتحدة لخمسة ضباط في جيش التحرير الشعبي، لتجسسهم السيبراني على أهداف تابعة للولايات المتحدة.

ثانيا: الصراع الأمريكي–الروسي:

ربما يرغب كلا من الطرفين روسيا، والولايات المتحدة في الحفاظ وتعزيز الاستقرار الاستراتيجي، لكن طبيعة التهديد السيبراني تحمل توجها تصعيديا، فصعوبة التنبؤ بتوقيت ومكان الهجوم ومنفذيه، وعدم امكانية التحكمفي حجم الاضرار التي قد يسببها، تزيد من حالة عدم اليقين والشك، وقد تؤدي عملية خاطئة في توجيه التهم الى جهة فاعلة معينة إلى تصعيد خطير، قد يؤدي إلى انتقام عنيف باستعمال قدرات تقليدية، فاعتماد روسيا على مجموعة من المرتزقة السيبرانيين قد يصعب التحكم بهم، قد يؤدي الى تصعيد الصراع[3].

[1] سكوت وارين هارولد وآخرون، **التوصل إلى اتفاق مع الصين بشان الفضاء الالكتروني**، مؤسسة راند، 2016، ص 8.
[2] نفس المرجع، ص 9.
[3] كريستوفر س.تشسفيس، وآخرون، **تعزيز الاستقرار الاستراتيجي مع روسيا**، مؤسسة راند، 2017، ص 7.

ومن أهم الأمثلة، ماحدث في أكتوبر 2016، حيث نشر موقع "**ويكيليكس**" آلاف الرسائل الإلكترونية المسربة من بريد الحزب الديمقراطي، واتهمت حينها الصحف الأمريكية والمراكز المتخصصة في الأمن السيبراني، روسيا، بوقوفها وراء اختراق البريد الإلكتروني، وبالفعل أكدت الاستخبارات الأمريكية في تقرير سري لها تلك الاتهامات، وقالت إن "النظام الروسي شن حملة إلكترونية بأوامر من الرئيس **فلاديمير بوتين**، هدفت إلى التأثير على مسار الانتخابات الرئاسية الأمريكية، عبر الإضرار بسمعة هيلاري كلينتون، وترجيح كفة المرشح الجمهوري **ترامب**.

وبدأت الولايات المتحدة الأمريكية تأخذ الأمر على محمل الجد في خطورة الحرب السيبرانية التي تشنها موسكو بنوايا تخريبية، إذ قررت واشنطن مؤخرا إغلاق ثلاث منشآت دبلوماسية روسية في بلادها، وتعريضها للتفتيش، ومنع استعمال برنامج مكافحة الفيروسات الروسي "**كاسبرسكي**" في الإدارات الحكومية، الخطوة التي اعتبرتها موسكو "عملًا عدائيًا"، وردّت عليه بتخفيض عدد الدبلوماسيين الأمريكيين في الأراضي الروسية إلى النصف.

في هذا السياق، صدر تقرير أمريكي جديدفي سبتمبر 2017، يقول إن الهجمات السيبرانية الروسية، هي امتداد لتكتيكات الحرب الباردة، وأنه يجب على الولايات المتحدة أن تعاملها كصفحة جديدة في هذا الصراع، منبها إلى أن موسكو تستغل الشبكات الاجتماعية لـ"نشر دعاية مغرضة لصالحها"، من خلال إغراق هذه المواقع التواصلية التي يستعملها مئات الملايين بمعلومات مضللة[1].

[1] خالد بن الشريف، **الفضاء السيبراني امتداد حرب باردة بين واشنطن وموسكو**، على الموقع : https://www.ultrasawt.com/ تاريخ الاطلاع : 25-04-2018.

المبحث الثاني :السياسة السيبرانية الأمريكية واستراتيجية المواجهة.

يركز هذا المبحث على أهمية الفضاء السيبراني في استراتيجية الامن القومي، ويفصل أهم محاور السياسة السيبرانية، وصولا إلى سبل وطرق مواجهة الولايات المتحدة للتهديدات السيبرانية.

المطلب الأول: أهمية الأمن السيبراني في استراتيجية الأمن القومي الأمريكي.

تعتبر استراتيجية الأمن القومي الأمريكي معيارا يكشف عن القضايا الأمنية التي يعتزم رئيس الولايات المتحدة التركيز عليها، وعلى اختلاف طبعاتها، تقوم على أربع أركان رئيسية هي :

- حماية المواطنين الامريكيين، الأرض، طريقة العيش الأمريكية.
- تعزيز الازدهار الأمريكي (خاصة الجانب الاقتصادي).
- الحفاظ على السلام العالمي.
- تعزيز النفوذ الامريكي في العالم.

ولمعرفة مدى اهتمام صانع القرار الأمريكي بالأمن السيبراني، قام "**دايفيد بايسون David Bisson**" بدراسة موجزة سنة 2015، حول تقارير استراتيجيات الأمن القومي السابقة، وسعى إلى تقييم استخدام هذه الوثائق لمصطلح "cyber" ، كما ونوعا[1].

وكانت النتائج من الناحية الكمية، زيادة ورود كلمة "Cyber" زيادة مضطردة، حيث تكررت الكلمة اكبر عدد من المرات(41 مرة) في تقرير **ترمب** لسنة 2017، يليه **أوباما** بـ 41مرة في تقريرين 2006، و2010، ولم يستعمل **بوش** الكلمة إلا مرة واحدة (بسبب الاهتمام بالحرب على الارهاب)، كما استعمل **كلينتون** كلمة "cyber" 22 مرة.

[1]David Bisson, **A "Cyber" Study of the U.S. National Security Strategy Reports** , accessedat : https://www.tripwire.com/state-of-security/government/a-cyber-study-of-the-u-s-national-security-strategy-reports/seen : 25-04-2018.

الجدول02: دراسة حول ورود كلمة "Cyber" في تقارير استراتيجية الأمن القومي الأمريكي.

عنوان الوثيقة	السنة	الرئيس	عدد مرات ورود كلمة "Cyber"	سياق ورود الكلمة
استراتيجية الامن القومي للقرن الجديد	1998	كلينتون	04	حماية المنشآت الحيوية، الجريمة، التعاون الدولي
استراتيجية الامن القومي للقرن الجديد	2000	كلينتون	10	حماية المنشآت الحيوية، الجريمة، التعاون الدولي، تبادل المعلومات، تحديد التهديدات
استراتيجية الامن القومي للعصر العالمي	2001	كلينتون	08	التهديدات الدولية، الحروب اللاتماثلية، المعلومات، المرونة السيبرانية
استراتيجية الامن القوميللو.م.أ	2002	بوش الابن	00	لا شيء
استراتيجية الامن القوميللو.م.أ	2006	بوش الابن	01	عسكرة الفضاء السيبراني
استراتيجية الامن القومي	2010	اوباما	22	الدعم العسكري، الأولوية العالمية، الشراكة، الإرهاب،الوعي
استراتيجية الامن القومي	2015	اوباما	19	التجسس السيبري، القواعد، المنشآت القاعدية، تنامي التهديدات، عسكرة الفضاء السيبراني، الوعي ،الشراكة
استراتيجية الامن القومي	2017	ترمب	41*	الفواعل ،الفضاء السيبري، التحديات والفرص، العصر السيبراني، الجريمة، الهجوم، المنشآت القاعدية، القدرات، الأمن السيبراني

المصدر: https://www.tripwire.com/state-of-security/government/

أما من الناحية النوعية، بدأت واشنطن في تصور مفهوم كلمة "Cyber" في عام 1998، وتعلق على العموم، بتهديدات سيبرانية،وحماية البنية التحتية الحيوية، وبعد العام 2000 ، بدأنا نرى عسكرة الفضاء السيبراني ووضع خطة شاملة لمواجهة مخاطر الإنترنت[1].

[1]David Bisson, Ibid.

* الباحث أكمل معلومات الجدول الخاصة بعام 2017.

بعد انتخاب أوباما تنوع استخدام مصطلح "السيبرانية" في تقارير استراتيجية الأمن القومي، وفي عام 2010، انشات قيادة للحرب السيبرانية الامريكية ، وأصبحت "الإنترنت" تعتبر بأنها "واحدة من أخطر التحديات الأمنية الوطنية، والسلامة العامة، والتحديات الاقتصادية للولايات المتحدة".

يعكس عام 2015 العديد من المخاوف، فهو يركز بشكل خاص على التجسس السيبراني ، والمعايير الدولية، والحاجة إلى الحفاظ على "الفضاء السيبراني" العالمي المشترك[1].

في عهد ترمب، تنوعت المفاهيم، حيث أولت الوثيقة اهتماما كبيرا بالعصر السيبراني، والامن السيبراني، وتحديد الفاعلين، وماهي التحديات التي يفرضها الفضاء السيبراني والفرص التي يخلقها، هذا إضافة إلى محاربة الجريمة السيبرانية ومواجهة التهديدات، وبناء القدرات السيبرانية.

نظرًا لدورها المركزي في إنشاء الانترنيت (الفضاء السيبراني)، ظلت الولايات المتحدة رائدة فيما يتعلق بقدرتها على تفسير التهديدات الإلكترونية الجديدة والناشئة، وهو ما يظهر جليا في استراتيجيات الأمن القومي.

[1]David Bisson, Ibid.

المطلب الثاني: الاستراتيجية السيبرانية للولايات المتحدة الأمريكية.

من أجل بناء فضاء سيبراني مفتوح وآمن وموثوق في الداخل والخارج، تعتمد الولايات المتحدة استراتيجية دولية للفضاء السيبراني، تتكون من سبعة أولويات[1]:

1. في مجال الاقتصاد: تعزيز المعايير الدولية والابتكار والأسواق الحرة.

وذلك بالمحافظة على بيئة للتجارة الحرة التي تشجع الابتكار التكنولوجي، وعلى امكانية الوصول الى الشبكات العالمية، حماية الملكية الفكرية، و الأسرار التجارية، ضمان أولوية المعايير الفنية الآمنة التي يحددها خبراء التقنية.

2. في مجال حماية الشبكات: تعزيز الأمن والموثوقية والمرونة.

تعزيز التعاون السيبراني، لا سيما بشأن قواعد السلوك الدولي والأمن السيبراني، ومحاربة الاختراقات والتداخل بين الشبكات الداخلية الذي يهدد ويقوض الأمن القومي، اضافة الى ضمان إدارة قوية للحوادث، والمرونة، وبناء قدرات الاستعادة للبنية التحتية للمعلومات، مع توفير الأجهزة والبرمجيات الموثوق بها، لضمان سلامة البنية التحتية للشبكات والمعلومات الحيوية.

3. في مجال تطبيق القانون: توسيع التعاون الدولي وسيادة القانون.

المشاركة في تطوير سياسة مكافحة جرائم الإنترنت، ومناقشة كيفية تطوير المعايير والتدابير الدولية المتعلقة بالجرائم السيبرانية على المستوى الثنائي والمتعدد الأطراف، من أجل مواءمة قوانين الجريمة السيبرانية على الصعيد الدولي، خاصة حرمان الإرهابيين والمجرمين من القدرة على استغلال الإنترنت.

كما يجب مواجهة السلوك الإجرامي في الفضاء السيبراني بتطبيق فعال للقوانين، وليس سياسات تقيد الوصول المشروع إلى الإنترنت أو المحتوى على الإنترنت.

[1] **International Strategy for Cyberspace**, The white house, Washington,2011. P 17-23.

4. في المجال العسكري: التحضير للتحديات الأمنية للقرن 21.

التكيف مع الحاجة العسكرية المتزايدة لشبكات موثوقة وآمنة، والعمل على ضمان جاهزية الجيش الأمريكي للعمل في بيئة قد يسعى بعض الفاعلين إلى تعطيل أنظمتها أو تدمير البنية التحتية الأخرى الحيوية للدفاع الوطني.

اضافة الى بناء وتعزيز التحالفات العسكرية القائمة، لمواجهة التهديدات المحتملة في الفضاء السيبراني، نظرا للحاجة إلى مستويات أعلى من التعاون الدولي، وذلك بتوسيع التعاون عبر الفضاء السيبراني مع الحلفاء والشركاء لتحقيق الأمن الجماعي.

5. في مجال حوكمة الإنترنت: تعزيز الهياكل الفعالة والشاملة.

إعطاء الأولوية للانفتاح والابتكار على الإنترنت، لأن القدرة على توزيع المعلوماتبكفاءة في الفضاء السيبراني، هي جوهر النشاط الاستهلاكي والتجاري والسياسي والعلمي والتعليمي الحديث، إضافة إلى السعي للحفاظ على أمن واستقرار الشبكة العالمية، وتثمين النقاش بين الفاعلين في إدارة الإنترنت.

6. في مجال التنمية الدولية: بناء القدرات وتحقيق الأمن والازدهار.

وذلك بتوفير المعرفة الضرورية، والتدريب، والموارد الأخرى، للبلدان التي تسعى إلى بناء القدرات التقنية وتحقيق الأمن السيبراني، عبر تطوير العلاقات مع صانعي السياسات لتعزيز بناء القدرات التقنية، وتوفير الاتصال المنتظم والمستمر بالخبراء.

7. في مجال حرية الإنترنت: دعم الحريات الأساسية والخصوصية.

دعم الجهات الفاعلة في المجتمع المدني لتحقيق منصات موثوقة وآمنة لحرية التعبير، وتكوين الجمعيات، وتشجيع التعاون الدولي من أجل حماية خصوصية البيانات.

هذه الاستراتيجية عبارة عن خريطة طريق تسمح للفاعلين في الفضاء السيبراني بتعريف وتنسيق دورهم بشكل أفضل في هذا الفضاء، أنها دعوة للدول والشعوب للمشاركة في تحقيق هذه الرؤية لتحقيق الرخاء والأمن والانفتاح في عالمنا الشبكي.

وفي 2017 حددت إدارة الرئيس **ترمب** استراتيجية تتضمن توجيهات يمكن اتخاذها للمساعدة في الحفاظ على أمن أمريكا من التهديدات السيبرانية ومنها: تحديد أولويات المخاطر، بناء شبكات حكومية يمكن الدفاع عنها، ردع وتعطيل الفواعل السيبرانية الاجرامية، تحسين تبادل المعلومات والاستشعار[1].

المطلب الثالث: مواجهة الولايات المتحدة للتهديدات السيبرانية.

أولا : الهيئات الحكومية للأمن السيبراني.

قال الرئيس أوباما عن الأمن السيبراني في العام 2009، "نحن لسنا مستعدين كما يجب، كحكومة و كدولة"،إن الأمن السيبراني مسألة معقدة بحيث لا يمكن إدارته من خلال وكالة أو منظمةواحدة ، وعليه يجب التنسيق بين كل الفاعلين، ومن ابرزهم[2] :

- **وزارة الدفاع (DoD)**: رفعت وزارة الدفاع الفضاء السيبرانيليكون المجال الخامس للحرب، جنبا إلى جنب معالأرض والبحر والجو والفضاء الخارجي، حيث قامت بإنشاءقيادة فرعية باسم القيادة الإلكترونية الأمريكية،لحماية الشبكات العسكرية الأمريكية.

- **وكالة الأمن القومي (NSA)**: هي هيئة مخابرات تابعة لحكومة الولايات المتحدة، مسؤولة عن مراقبة وجمع ومعالجة المعلومات والبيانات لأغراض المخابرات والمخابرات

[1]Mark Pomerleau**, WhatTrump's National Security Strategysays on Cyber ?**, accessedat : https://www.fifthdomain.com/civilian/2017/12/18/what-trumps-national-security-strategy-says-on-cyber/seen : 25-04-2018.

[2]Kristin M.lord&Travis Sharp, **America's Cyber Future**,Center for a new America Security, V1, 2011, P 31-37.

المضادة، لديها قدرات سيبرانية عالية، واقترحت لقيادة جهود الأمن السيبراني في الولايات المتحدة.

-**وزارة الأمن الداخلي (DHS)**: مسؤوليتها حماية الأراضي الأمريكية من أي هجمات، وتبذل جهودا لتأمين الهيئات الحكومية المدنية، والشبكات غير السرية، وهي تعتبر الأمن السيبراني واحد من خمس مجالات أساسية في الوزارة.

هذا إضافة الى وكالة الاستخبارات الأمريكية(**CIA**)، ومكتب التحقيقات الفدرالي (**FBI**)، والكنغرس، والبيت الأبيض.

وفي 2017 وعد الرئيس الأمريكي **ترمب** برفع القيادة السيبرانية في البنتاجون إلى وضع قيادة مقاتلة موحدة، وقال **ترمب** :"إن قرار إنشاء قيادة سيبرانية منفصلة يظهر عزمنا المتزايد على مواجهة التهديدات السيبرانية وسيساعد في طمأنة حلفائنا وشركائنا وردع خصومنا"[1].

ثانيا: القدرات الأمريكية في الدفاع والهجوم السيبراني.

إن حجم القدرات السيبرانية الأميركية يرتفع باطراد، وستتمكن قريبا من إرسال مقاتلين سيبرانيين في مهمات قتالية لمساندة القوات على الأرض، ويلاحظ ذلك في زيادة موازنة الأمن السيبراني الهجومي والدفاعي.

وتعتبر وكالة الأمن القومي، من أبرز الفاعلين في الفضاء السيبراني، وتركز انشطتهاعلى المراقبة في الخارج، ويضع القانون الأمريكي القليل من القيود على عملها، لكن كشفت وثائق **سنودن** أن الوكالة تجسست بشكل متزايد على الأمريكيين الذين يعيشون فوق الأراضي الأمريكية، في حين سمح برنامج PRISM، للوكالة بالحصول على معلومات

[1]W.J. Hennigan , **Trumpannounces plan to elevate U.S. military command thatoversees cyber operations**, Los Angles times , accessedat : http://www.latimes.com/politics/washington/la-na-essential-washington-updates-trump-announces-plan-to-elevate-u-s-1503078609-htmlstory.html, seen : 25-04-2018

خاصة عن عملاء في الشركات الرائدة في مجال الإنترنت، بما في ذلك جوجل، فيس بوك، وآبل، ومايكروسوفت، بالإضافة إلى التجسس على العديد من رؤساء العالم بما فيهم رؤساء الدول الصديقة والحليفة[1].

جدير بالذكر أن الرئيس أوباما أعلن في 2014 قراره التوقف عن عمليات التجسس على رؤساء الدول الصديقة، بيد أن الإدارة سمحت للوكالة باستهداف كبار مستشاري القادة وبعض الزعماء وفقاً لما يراه كبار المسؤولين مناسباً.

كما تّتهم الوكالة بعدم التبليغ واستعمال ثغرات في نظام التشغيل**ويندوز**، ويرجح ان قراصنة تمكنوا من اختراق الوكالة، وقاموا بتسريب برمجيات حساسة تستعمل للقرصنة، منها ما استعمل في فيروس الفدية "**واناكراي**" الذي أصاب آلاف الأجهزة في العالم.

ورداً على البيئة التنافسية الدولية، أسس البنتاجون وحدة خاصة بالقوة السيبرانية القتالية وقيادة الأمن السيبراني، هدفت إلى تنسيق الجهود اللامركزية للأمن السيبراني، وتوفير قيادة موحدة لكل من العمليات الدفاعية والهجومية، فعلى الجانب الدفاعي، تعد القيادة السيبرانية مسؤولة عن الإجراءات الهادفة إلى حماية واكتشاف والاستجابة للنشاط الخفي في إطار نظم المعلومات وشبكات الإنترنت للبنتاجون، كذلك، تنطوي العمليات السيبرانية الهجومية على تعطيل ومنع وتدمير المعلومات، والهجوم الإلكتروني بهدف تدمير البنية التحتية العسكرية أو المدنية للخصم[2].

[1] **الكشف عن تجسس واشنطن على نتانياهو**، الجزيرة، على الرابط : http://www.aljazeera.net/news/presstour/2015/12/30/ تاريخ الاطلاع : 25-04-2018.

[2] مروة صبحي، **تسليح تكنولوجي: تنافس غير تقليدي في مجال التكنولوجيا العسكرية**، مركز المستقبل للأبحاث والدراسات المستقبلية، على الرابط : **http://rawabetcenter.com/archives/6591** تاريخ الاطلاع : 26-04-2018

المبحث الثالث : مستقبل الأمن السيبراني الأمريكي.

يناقش هذا المبحث المخاطر المستقبلية على الأمن القومي الأمريكي في الفضاء السيبراني، والدور الذي تريد أن تلعبه الولايات المتحدة في هذا الفضاء.

المطلب الأول: التهديدات السيبرانية المستقبلية للولايات المتحدة الأمريكية.

بما أن الفضاء السيبراني ينمو ويتطور بسرعة، فالتهديدات السيبرانية تتطور بسرعة أيضا، وعليه، فاستراتيجية الأمن السيبراني الامريكية الحالية إذا لم يتم تطويرها، ستجعل الولايات المتحدة عرضة للهجمات في المستقبل،ومن بين التهديدات السيبرانية المستقبلية المحتملة نذكر:

1. مخاطر الحوسبة السحابية:

وهي تكنولوجيا تعتمد على نقل المعالجة ومساحة التخزين الخاصة بالحاسوب إلى ما يسمى السحابة، وهي عبارة عن أجهزة خوادم يتم الوصول إليها عن طريق الانترنت، وهذا ما يجعل البيانات عرضة لمخاطر وتهديدات كبيرة، هذا هو الاتجاه الناشئ الأكثر أهمية الذييؤثر في الأمن السيبراني[1].

فمن جهة، فتجميع البياناتعلى خوادم كبيرة في مكان واحد، يعطي دافعا للقراصنة لاختراقها، ومن جهة أخرى، ستصبح البيانات في يد جهات مركزية تملك دفاعات سيبرانية هائلة، ربما سيؤثر على حرية الانترنيت وخصوصية المستخدمين .

[1]NirKshetri, **The Quest to Cyber Superiority**, Springer, 2016 , P 04.

2. تهديدات تقنيات الذكاء الاصطناعي[1]:

توجد العديد من التهديدات المترتبة على تصاعد الاعتماد على تقنيات الذكاء الاصطناعي، وتنقسم إلى:

- **تهديدات أمنية:** أحد التداعيات الخطرة هو تهديد هذه التقنيات حق البشر في الحياة، ويتضح ذلك في حالة الأنظمة القتالية المستقلة مثل **الدرون** التي تحمل أسلحة، أو الروبوتات المقاتلة، حيث تكمن الخطورة في اختراقها، نتيجة لقصور أو خطأ بشري في إجراءات التأمين والتلاعب بالخوارزميات التي تتحكم فيها.
- **تداعيات اجتماعية:** تؤدي زيادة الاحتكاك مع الآلات إلى انفصال البشر تدريجياً عن محيطهم الاجتماعي البشري، وهو ما يُفقد العلاقات الإنسانية مرونتها التقليدية.

3. مخاطر الهواتف الذكية وانترنيت الأشياء:

تشير التوقعات إلى وصول الأجهزة المتوافقة مع تقنية انترنت الأشياء إلى 20 مليار جهاز بحلول العام 2020، وستكون الهواتف الذكية إحدى أهم الوسائل التي ستسمح لنا بالتحكم بجميع هذه الاجهزة،ينطوي هذا التحول على مخاطر عديدة أهمها القرصنة السيبرانية، ستكون الاخطار الناجمة عن اختراق هذه الهواتف أكثر وذات تأثير أكبر، خاصة بعد ازدياد هجمات الفدية[2]، إضافة إلى مشكلة الخصوصية، التي تتفاقم مع الأجهزة المحمولة، حيث أن هذه الاجهزة تحتوي على معلومات حساسة عن المستخدم واماكن تواجده، وتصرفاته وحتى حالته النفسية، فالأجهزة المحمولة تدمر الخصوصية.

---

[1] إيهاب خليفة،**تهديدات ذكية، مخاطر خروج الذكاء الاصطناعي عن السيطرة البشرية**، مجلة لغة العصر الالكترونية، على الرابط : http://aitmag.ahram.org.eg/News/82161.aspx تاريخ الاطلاع : 26-04-2018.

[2] **رياض يسمينة، مخاطر الهواتف الذكية بعد انتشار انترنيت الاشياء**، على الرابط : http://ar.itp.net/mobile/614057-% تاريخ الاطلاع: 27-04-2018.

4. مشكلة هيكلية الانترنيت :

إن البنية الهيكلية الحاليةللإنترنت تلعب دورا في تحفيز وانتشار التهديدات السيبرانية، ويقترح الخبراء إدخال تغييرات في بنية الانترنيت على مرحلتين:

1. إعادة هندسة الإنترنت لجعل الفضاء السيبراني أكثر أمنا، حيث يتم التركيز على مزيد من تحديد الهوية ، والأمن ، مع المحافظة على الخصوصية .

2.وضع شبكات جديدة على الإنترنت لتقديم الخدمات للجهات التي تتطلب المجهولية والخصوصية الصارمة (مثل المعاملات المالية أو الاتصالات العسكرية).

5. صعوبة المحافظة على الريادة الأمريكية[1]:

خاصة مع التطور الكبير الذي تعرفه دول العالم في بناء القدرات السيبرانية، والانكماش في الانفاق الحكومي الامريكي في هذا المجال، مما يقلل من قدرتها على التأثير الدولي.

المطلب الثاني: الدور المستقبلي للولايات المتحدة الأمريكية في الفضاء السيبراني.

تعمل الولايات المتحدة على المستوى المحلي والدولي من أجل تعزيز بنية تحتية للمعلومات والاتصالات مفتوحة وآمنة وموثوقة، من خلال ثلاث محاور رئيسية، هي، الدبلوماسية والدفاع والتنمية، وذلك لتعزيز الرخاء والأمن والانفتاح، حتى يمكن للجميع الاستفادة من الفضاء السيبراني.

[1]NirKshetri, **The Quest to Cyber Superiority**, Springer, 2016 , P 06.

1. الدبلوماسية وتعزيز الشراكات[1]:

إن توسيع مبادئ السلام والأمن في الفضاء السيبراني، يتطلب تعزيز الشراكة والمبادرات الموسعة، لذلك تسعى الولايات المتحدة الى اشراك المجتمع الدولي في حوار صريح وبناء، من أجل بناء توافق حول مبادئ وقواعد السلوك المسؤول في الفضاء السيبراني.

في مجال الشراكة، تسعى الولايات المتحدة إلى اقناع أكبر عدد من الفاعلين برؤيتها للفضاء السيبراني، وذلك لحماية مصالحها الاقتصادية والاجتماعية والسياسية والأمنية، وستدعم هذه الجهود بالتعاون مع القطاع الخاص في الداخل والخارج.

اضافة الى الشراكات الثنائية والمتعددة الأطراف، والمشاركة في الحوارات الثنائية، على جميع المستويات، من اجل المضي قدمًا في العمل المشترك بشأن التحديات الناشئة في عالم الإنترنت .

كما تعتبر المنظمات الإقليمية فعالة في معالجة مشاكل الأمن السيبراني، لذلك فسوف تلعب دوراً مهما في تطوير وتطبيق قواعد السلوك،الى جانب المنظمات الدولية خاصة في مجال حوكمة الإنترنت.

كما ستعمل الو.م.أ بشكل وثيق مع مالكي البنية التحتية والمشغلين –المسؤولون عن وظائف الشبكة – لتوسيع المبادرات لتأمين نظام الشبكة وتسعى أيضًا إلى مشاركة القطاع الخاص في إدارة الإنترنت.

2. الدفاع: حماية الشبكات والردع.

ستدافع الولايات المتحدة عن شبكاتها، سواء كان التهديد من الإرهابيين أو مجرمي الإنترنت أو الدول ووكلائها، كما تسعى لتشجيع الجهات الفاعلة ذات السلوك الجيد، وردع أولئك الذين يهددون السلام والاستقرار من خلال الأعمال التخريبية في الفضاء السيبراني.

[1] **International Strategy For Cyberspace**, The white house, 2001, P 11-12.

- **حماية الشبكات** : تتطلب حماية الشبكات الحساسة قدرات دفاعية عالية، ستواصل الولايات المتحدة تعزيز دفاعاتها على الشبكة وقدرتها على الصمود والتعافي من الهجمات، بالنسبة لتلك الهجمات الأكثر تطوراً التي تسبب أضراراً، يجب تطوير خطط استجابة حديثة للحد من التأثيرات على الشبكة.
- **تعزيز القوة داخليا:** يتطلب ضمان مرونة الشبكات والأنظمة، إجراءات وطنية جماعية متضافرة تمتد لتشمل الحكومة بأكملها، بالتعاون مع القطاع الخاص، والأفراد.
- **تعزيز القوة خارجيا** : لدى الولايات المتحدة مصلحة مشتركة في مساعدة الدول الأقل نمواً لبناء قدرات في مجال الدفاع السيبراني، وذلك بزيادة الجهود المبذولة في هذا المجال، لأن هذا، سيعزز الأمن الجماعي في المجتمع الدولي.
- **الردع**[1]: عند الضرورة، سترد الولايات المتحدة على الأعمال العدائية في الفضاء السيبراني، فالولايات المتحدة تحتفظ بالحق في استخدام جميع الوسائل الضرورية – الدبلوماسية والإعلامية والعسكرية والاقتصادية – حسبما يتلاءم مع القانون الدولي المعمول به، من أجل الدفاع عن أمتنا وحلفائنا وشركائنا ومصالحنا.

3. التنمية: بناء الرخاء والأمن[2]:

في مجال التنمية تعمل الولايات المتحدة على تسهيل بناء قدرات الأمن السيبراني في الخارج، على المستوى الثنائي ومن خلال المنظمات الاقليمية والدولية، بحيث يكون لكل دولة الوسائل اللازمة لحماية بنيتها القومية للمعلومات، وتعزيز الشبكات العالمية، وبناء شراكات لتعزيز أمن الفضاء السيبراني.

وفي مجال بناء قدرات الأمن السيبراني، فإن الولايات المتحدة ملتزمة بالمساعدة في بناء قدرات الأمن السيبراني للدول،لأن تعزيز الأمن السيبراني للدول النامية له فوائد فورية

[1]Joseph S.Nye Jr, **Deterrence and dissuasion in Cyberspace**, Mit pressJournals, acceesat : https://www.mitpressjournals.org/doi/pdf/10.1162/ISEC_a_00266seen: 26-04-2018.
[2]**International Strategy For Cyberspace**, The white house, 2001, P 14-15.

وطويلة الأجل، حيث أن قدرة المزيد من الدول على مواجهة التهديدات السيبرانية يساهم في عملية بناء الثقة في الفضاء السيبراني.

وإذ أن الأمن السيبراني قضية عالمية يجب معالجتها بتضافر جهود جميع البلدان، وعليه فعلى الولايات المتحدة أن تعمل على زيادة الوعي، والتدريب القانوني والتقني، وتدعم تطوير السياسات السيبرانية للدول.

ينظر إلى مساعدة الولايات المتحدة في بناء القدرات كاستثمار، والتزام، وفرصة مهمة للحوار والشراكة، ومع تطور مساهمات الدول في قضايا الفضاء السيبراني، فإن الولايات المتحدة ترغب في أن تتطور الحوارات، من بناء القدرات، إلى التعاون الاقتصادي، والتقني، والتنفيذي، والأمني، والدبلوماسي النشط بشأن قضايا الفضاء السيبراني ذات الاهتمام المشترك.

خلاصة الفصل الثالث :

في ختام هذا الفصل نخلص الى أن الولاياتالمتحدة الأمريكية تعد دولة رائدة في الفضاء السيبراني، فمعظم بنيتها التحتية الحساسة، واقتصادها، وحتى مواطنوها، اصبحت أكثر تشابكا بفضل التقنيات الرقمية المتطورة، وهذا ما جعل تفاعلها مع العالم أسرع من قدرتها على فهم العواقب الامنية، وتخفيف المخاطر المحتملة، مما يفاقم هذه التطورات حالة الشك وعدم اليقين على المستوى الدولي، حيث تصاعدت حدة الصراع بينها وبين الصين وروسيا، هذا ما جعل الاهتمام بالأمن السيبراني يزداد عند صانع القرار الامريكي، جسده في ادخال الأمن السيبراني في استراتيجية الأمن القومي، بالإضافة الى اصدار استراتيجية خاصة بالفضاء السيبراني عام 2011.

ورغم تنوع وكثرة الهيئات الأمريكية الحكومية والخاصة المكلفة بالأمن السيبراني، والقدرات الكبيرة التي تملكها الولايات المتحدة في الدفاع والهجوم السيبراني، والترسانة القانونية التي تؤطر الفضاء السيبراني في الداخل الامريكي، إلا أنها تبقى عاجزة عن منع الاختراقات والتجسس على مؤسساتها، هذا إضافة إلى التهديدات المستقبلية المحتملة في بيئة تتطور بسرعة كبيرة، مما جعل الولايات المتحدة تضع خارطة طريق للدور المستقبلي الذي ستلعبه بالاشتراك مع باقي الفاعلين في العالم من أجل فضاء سيبراني سلمي وآمن.

الخاتمة

الخاتمة :

كان الأمن ولا يزال الهدف المنشود للإنسان، واعتبرته الدول هدفا أساسيا بعد تشكل الدولة القومية، حيث انبرت الدراسات الأمنية لتحليل وتفسير الظاهرة، اختلفت المفاهيم والتعريفات بين المدارس الفكرية، حيث انتقل مفهوم الامن من المفهوم المادي العسكري الدولاتي عند الواقعيين، إلى الامن المجتمعي الهوياتي الإنساني عند معارضيهم.

ومع تطور المجتمعات والثورة التكنولوجية الهائلة في المعلومات والاتصال، والتوجه نحو مجتمع المعلومات والمعرفة، تشكل فضاء جديد هو الفضاء السيبراني، هذا الفضاء الذي يستعمله الأفراد كما الدول، أحدث تغييرات جذرية في مفاهيم العلاقات الدولية كمفهوم القوة والصراع والحرب، حيث تغيرت القوة وانتشرت بين الفاعلين، وتحول الصراع إلى صراع سيبراني، وعليه دعت الحاجة إلى تطوير مفهوم الأمن لمواجهة التهديدات الجديدة، حيث جاء مفهوم الأمن السيبراني كرد فعل على هذه التهديدات، التي مست جميع مجالات الحياة، خاصة مع اتجاه الدول لإنشاء قواعد البيانات القومية، وتطوير شبكات الاتصال، والاعتماد على شبكة الانترنت كبيئة أساسية للعمل، ما يعني أن التعرض للمخاطر السيبرانية يعني تعريض الأمن القومي لمخاطر كبيرة قد تهدد استقرار الدولة وتماسكها.

في كل يوم، المزيد من المستخدمين يتشاركون المزيد من البيانات على المزيد من الأجهزة، هذا الترابط والتفاعلفي الفضاء السيبراني يتزايد يوما بعد يوم، وتتزايد معه المخاطر والتهديدات.

هذه التهديدات التي تنوعت في الاشكال، والخطورة، بدأت بجرائم سيبرانية يقوم بها أفراد ومنظمات اجرامية كالاختراق والتجسس وسرقة الاموال، وتطورت إلى تخويف وابتزاز المجتمعات وارهابهم عن طريق الأنترنيت، لتصل إلى أخطر أنواع الصراع بين الدول وتهديد

امنها القومي، حيث ظهر جليا عسكرة الفضاء السيبراني، واستعمال الاسلحة السيبرانية عالية التأثير في شن حروب سيبرانية مدمرة.

وحيث ان الفضاء السيبرانياصبح ساحة هامة للتفاعلات الدولية المختلفة، في ظل زيادة الهجمات السيبرانية بين الدول، بما يؤثر على أمنها القومي، سعت الدول فرادى ومجتمعة الى بذل الجهد من أجل تطوير قدراتها، واتخاذ الإجراءات الوقائية الكافية لحمايتها من أي هجمات سيبرانية محتملة، فقامت بتشكيل وحدات الاستجابة لطوارئ الانترنيت، والهيئات الوطنية للأمن السيبراني، كما شكلت جيوشا سيبرانية لتقوم بمهمات الدفاع والهجوم والحماية، هذا في الجانب التقني، أما في الجانب القانوني، فطورت من منظومتها القانونية لتتلائم مع التهديدات الجديدة، وبما أن الفضاء السيبراني، لا يعترف بالزمان والجغرافيا، بذلت الدول مساعي إقليميا، ودوليا، لوضع أطر قانونية واتفاقيات دولية للفضاء السيبراني، وجعله أكثر أمنا، لعل من أبرزها **دليل تالين**، الذي فسر العديد من المفاهيم الغامضة في الفضاء السيبراني.

وبما انه لم يتحقق الأمن المثالي في العالم المادي، فلن يتحققأمن مثالي في الفضاء السيبراني، لذلك فالهدف المرجو هو تقليل المخاطر إلى مستوى مقبول، يمكن معه الاستمرار في النمو والتقدم.

يقول **دانيال جير** :" إن التكنولوجيا التي وفرت لك كل شيء تريده، هي نفسها التكنولوجيا التي تريد أن تنزع منك كل شيء لديك".

وحيث أن الولايات المتحدة تعتبر مهد الانترنيت، التي بدأت كمشروع عسكري، ثم توسعت لتشكل ما نعرفه اليوم بالفضاء السيبراني، فإن اعتماد الولايات المتحدة الكبير على التكنولوجيا، في جميع القطاعات، قد خلق نقاط ضعف حرجة، يتم استغلالها من طرف

خصومها بشكل أسرع وأكبر من قدرتها على الاستجابة، ويضعها أمام تحديات كبيرة، وهذا ما يجعل مستقبل الولايات المتحدة على المحك.

إن مواجهة التهديدات السيبرانية الراهنة، أمر ضروري، لكن الخطر الحقيقي يكمن في التهديدات المستقبلية، لذلك فإن تجاهلها اليوم، سيعرض الأمن القومي للولايات المتحدة لخطر أكيد ودائم.

فالتحدي اليوم، هو الاستعداد لتهديد الغد، بتطوير استراتيجيات المواجهة، والعمل مع بقية دول العالم، من اجل تشارك قيم الأمن والاستقرار واحترام قواعد السلوك الجيد، من اجل فضاء سيبراني سلمي، يعزز الأمن والتقدم والازدهار للجميع.

النتائج والتوصيات :

أولا : النتائج :

- في عصرنا الرقمي، اصبح الفضاء السيبراني مجالا جديدا وهاما للتفاعلات الدولية، وقد احدث تغيرات في مفاهيم القوة والصراع والحرب، ظهر فاعلون جدد، وانتشرت القوة السيبرانية بينهم، وازداد الصراع في الشبكات، قد يتطور أحيانا ليصبح حروبا جديدة بأسلحة سيبرانية (العالم يعيش مرحلة الهوبزية السيبرانية).
- يتميز الفضاء السيبراني بالغموض، وشدة وتنوع التهديدات، التي تتزايد في الاحترافية والخطورة بسرعة كبيرة، مما يجعل الأمن السيبراني – كرافد جديد للأمن القومي– على رأس الأوليات في الاستراتيجية العسكرية والعقيدة الأمنية للدول.
- التهديدات السيبرانية لها طابعها التقني الخاص، اضافة الى انها تهديدات عابرة للحدود، تهدد سيادة الدول، وعليه، فالمواجهة تكون على مستويين، الاول تقني، بتحديث الجيوش، وهيئات الأمن السيبراني، والثاني قانوني، بوضع التشريعات

الوطنية، والتعاون الاقليمي والدولي من أجل فضاء سلمي وآمن (ربما يحتاج العالم إلى عقد إجتماعي سيبراني جديد).

- رغم أن الولايات المتحدة تعد أقوى دولة سيبرانية، فهي تواجه تهديدات سيبرانية حالية ومستقبلية، ومنافسة شديدة في الفضاء السيبراني خاصة من الصين روسيا، بما قد يهدد أمنها القومي ودورها في الأمن العالمي.
- تعمل الولايات المتحدة من خلال هيئات ووكالات مختلفة، ومجموعة من التشريعات الرائدة، على مواجهة تحديات الأمن السيبراني، من خلال التعاون الدولي وتوحيد الرؤية المستقبليةلفضاء سيبراني آمن يساعد على التقدم والنمو.

ثانيا: التوصيات :

- فهم وإدراك أن الأمن السيبراني عنصر رئيس في الامن القومي، وله علاقة وطيدة مع قضايا التنمية السياسية والاقتصادية والاجتماعية، وضرورة ادماجه في العقيدة الأمنية للدولة، ووضع استراتيجية سيبرانية واضحة.
- ضرورة وضع وتحديث التشريعات القانونية التي تنظم وتؤطر الفضاء الالكتروني، خاصة قوانين مكافحة الجريمة السيبرانية والارهاب السيبراني.
- أهمية خلق اطار مؤسسي للأمن السيبراني في الجانب المدني، وتحديث الجيوش، وخلق جيوش سيبرانية، في الجانب العسكري.
- فهم وادراك دور الافراد في بناء الأمن، من خلال التعليم والتوعية ونشر ثقافة الامن السيبراني.
- ضرورة التعاون الاقليمي والدولي، بين جميع الفاعلين، لترسيخ قواعد السلوك الجيد، ونشر قيم وثقافة الفضاء السيبراني السلمي والآمن.

فهرس المصادر والمراجع

أولا : باللغة العربية :

أ. الكتب :

1. الأشقر جبور منى ، **السيبرانية هاجس العصر**، المركز العربي للبحوث القانونية والقضائية، بيروت ، 2017.
2. بهلول نسيم ، **فهم الأمن القومي الجزائري من مدخلي الأمن الوطني والدفاع الوطني**، دار حامد للنشر والتوزيع، عمان، 2015.
3. بيتر بي سيل، **الكون الرقمي**، تر: ضياء وراد، هنداوي سي آي سي ، المملكة المتحدة، 2017.
4. جون بيليس، **الأمن الدولي في حقبة ما بعد الحرب الباردة**، في: جون بيليس، ستيف سميث، عولمة السياسة العالمية، مركز الخليج للأبحاث، الإمارات العربية المتحدة، 2004.
5. جوزيف إس.ناي (الابن)، **مستقبل القوة**، تر: أحمد عبد الحميد نافع، المركز القومي للترجمة، القاهرة، 2015.
6. داون نونسياتو، **الحرية الافتراضية**، تر: أنور الشامي، ط1، وزارة الثقافة والتراث، قطر، 2011.
7. هاري آر.يارغر، **الاستراتيجية ومحترفو الأمن القومي**، تر: راجح محرز علي، ط1، مركز الامارات للدراسات والبحوث الاستراتيجية، أبو ظبي، الامارات العربية المتحدة، 2011.
8. زيد المرهون عبد الجليل ، **أمن الخليج وقضية التسلح النووي**، المنامة: مركز البحرين للدراسات والبحوث، 2007.
9. عباس مراد علي ، **الأمن والأمن القومي مقاربات نظرية**، ابن النديم للنشر والتوزيع، الجزائر، 2017.
10. عبد الوهاب الكيالي وآخرون، **موسوعة السياسة**، الجزء الأول، ط3، المؤسسة العربية للدراسات والنشر،بيروت، 1990.
11. عبد الصادق عادل ، **الإرهاب الالكتروني والقوة في العلاقات الدولية: نمط جديد وتحديات مختلفة**، مركز الدراسات السياسية والاستراتيجية، القاهرة، 2009.
12. عبد الصادق عادل ، **أسلحة الفضاء الالكتروني في ضوء القانون الدولي**، سلسلة أوراق، العدد 23، مكتبة الاسكندرية، مصر، 2016.
13. لورنس لسيج، **الكود المنظم للفضاء الالكتروني**، هنداوي للتعليم والثقافة، مصر، 2013.

14. مظلوم جمال معين ، **الأمن غير التقليدي** ، جامعة نايف العربية للعلوم الأمنية، الرياض، 2012.

15. مراد عبد الفتاح ، **شرح جرائم الكمبيوتر والانترنيت**، دار الكتب والوثائق المصرية، دط. دسن.

16. مجموعة مؤلفين، **الحروب المستقبلية في القرن الحادي والعشرين**، مركز الامارات للدراسات والبحوث الاستراتيجية، 2014.

17. ساعاتي أمين ،**الأمن القومي العربي** ، المركز السعودي للدراسات الإستراتيجية،القاهرة،1993.

18. تيري ديبيل، **استراتيجية الشؤون الخارجية...منطق الحكم الأمريكي**، ترجمة: وليد شحادة ، دار الكتاب العربيومؤسسة محمد بن آل راشد آل مكتوم، بيروت، 2009.

19. خليفة ايهاب ،**القوة الالكترونية وأبعاد النحول في خصائص القوة** ، مكتبة الاسكندرية، مصر، 2014.

20. خليفة ايهاب ، **القوة الالكترونية: كيف يمكن ان تدير الدول شؤونها في عصر الانترنيت**، دار العربي، 2017.

ب.المقالات والدوريات :

1. بن أحمد الشهري حسن ، "**الإرهاب الالكتروني – حرب الشبكات**–"،المجلة العربية الدولية للمعلوماتية، 2015.

2. جوشوا بارون وآخرون، "**تداعيات العملة الافتراضية على الأمن القومي**"، مؤسسة راند، 2015.

3. درويش سعيد،" **ماهية الحرب الالكترونية في ضوء قواعد القانون الدولي**"، مجلة حوليات جامعة الجزائر1، العدد29، 2016.

4. كريستوفر س.تشسفيس، وآخرون، "**تعزيز الاستقرار الاستراتيجي مع روسيا**"، مؤسسة راند، 2017.

5. محمد يحي ربيع ، "**اسرائيل وخطوات الهيمنة على الفضاء السيبراني في الشرق الأوسط**"، مجلة رؤى استراتيجية، العدد 3، مركز الإمارات للدراسات والبحوث الاستراتيجية، 2013

6. مقرح الزهراني يحي ، "**الأبعاد الاستراتيجية والقانونية للحرب السيبرانية**"، مجلة البحوث والدراسات، العدد 23، الوادي، الجزائر، 2017.

7. مختار محمد ، "**هل يمكن للدول أن تتجنب مخاطر الهجمات الالكترونية؟**"، مفاهيم المستقبل، اتجاهات الأحداث ، العدد 6، مركز المستقبل للأبحاث والتطوير، 2015.

8. سكوت وارين هارولد وآخرون، "**التوصل إلى اتفاق مع الصين بشان الفضاء الالكتروني**"، مؤسسة راند، 2016.

9. عبدالله الحربي سليمان ، "**مفهوم الأمن: مستوياته وصيغه وتهديداته (دراسة نظرية في المفاهيم والأطر)**"،المجلة العربية للعلوم السياسية، العدد 19، 2008.

10. عبد الصادق عادل ، "**القوة الالكترونية: اسلحة الانتشار الشامل في عصر الفضاء الالكتروني**"، مجلة السياسة الدولية، العدد 188، مؤسسة الأهرام، مصر، 2012.

11. فريجة احمد ، فريجة لدمية ،"**الأمن والتهديدات الأمنية في عالم ما بعد الحرب الباردة**"، مجلة دفاتر السياسة والقانون، العدد 14، ورقلة، 2016.

ج. المداخلات العلمية :

1. عبدالله بن عبدالعزيز بن فهد العجلان، **الإرهاب الإلكتروني في عصر المعلومات**، بحث مقدم إلى المؤتمر الدولي الأول حول "حماية أمن المعلومات والخصوصية في قانون الإنترنت"، القاهرة، 2008.

د. المذكرات والرسائل الجامعية:

1. دحماني مولود، **أثر مخرجات العلاقة الارتباطية بين مسار الانتقال الديمقراطي ومحددات الامن القومي على قوة الدولة في مراحل التحول السياسي**، مذكرة ماجستير، جامعة مولود معمري، تيزي وزو، 2016.

2. علاء عبد الحفيظ، **العلاقة بين الأمن القومي والديمقراطية**، رسالة دكتوراه في الفلسفة ، قسم العلوم السياسية، جامعة القاهرة ، 2009.

3. غسان سعيد جلعود وليد، **دور الحرب الالكترونية في الصراع العربي الاسرائيلي**، مذكرة ماجستير، كلية الدراسات العليا، جامعة النجاح الوطنية، 2013.

هـ. المطبوعات :

1. رحموني فاتح النور ، **محاضرات الإستراتيجية والأمن الدولي**، ألقيت على طلبة الماستر، قسم العلوم السياسية، جامعة المسيلة ، 2017-2018.

و. مواقع الانترنيت :

1. الاتحاد الدولي للاتصالات، **مؤشر الأمن السيبراني العالمي**، 2017، على الرابط : https://www.itu.int/pub/D-STR-GCI.01-2017 تاريخ الاطلاع : 20-04-2018.

2. **الانترنيت المظلم أرض الخدمات المخفية**، مؤسسة إيكان، علنا لرابط : https://www.icann.org/news/blog/ar-421519a4-57e7-48d4-ab40-885920dc281a تاريخ الاطلاع : 28-04-2018.

3. اللجنة الدولية للصليب الأحمر، **ما هي القيود التي يفرضها قانون الحرب على الهجمات السيبرانية؟**، على الرابط:- https://www.icrc.org/ara/resources/documents/faq/130628-cyber-warfare-q-and-a-eng.htm تاريخ الاطلاع : 24-04-2018.

4. **الحروب الالكترونية، معارك العالم الافتراضي تنتقل إلى الميدان**، تقرير للخليج أونلاين، 2018، على الرابط:http://alkhaleejonline.net/articles/1521891769458091700/ تاريخ الاطلاع: 24-04-2018.

5. **الكشف عن تجسس واشنطن على نتانياهو**، الجزيرة، على الرابط :http://www.aljazeera.net/news/presstour/2015/12/30/ تاريخ الاطلاع : 25-04-2018.

6. **المجال الخامس.. الحروب الإلكترونية في القرن الـ21**، مركز الجزيرة للدراسات، على الرابط : http://studies.aljazeera.net/ar/issues/2010/20117212274346868.html

تاريخ الاطلاع : 25-04-2018.

7. **أنواع خوادم الشبكة**، على الموقع : http://www.networkset.net/2014/02/19 تاريخ الاطلاع : 2018/04/21.

8. **أنونيموس**، موسوعة الجزيرة، على الموقع :

http://www.aljazeera.net/encyclopedia/movementsandparties

تاريخ الاطلاع : 20-04-2018

9. **أفضل خمسة جيوش الكترونية في العالم** ، مركز الدراسات كاتيخون، على الرابط: http://katehon.com/ar/article/ تاريخ الاطلاع : 2018/04/22

10. بن الشريف خالد ، **الفضاء السيبراني امتداد حرب باردة بين واشنطن وموسكو**، على الرابط : https://www.ultrasawt.com/ تاريخ الاطلاع : 25-04-2018.

11. بسيوني محمد ، **دوافع الاستراتيجية الروسية لحرب المعلومات ضد الدول الغربية**، جريدة الصباح الجديد ، على الرابط :http://newsabah.com/newspaper/138116 تاريخ النشر : 30-10-2017، تاريخ الاطلاع : 26-04-2018.

12. جوزيف.س ناي، **التحكم في الصراع السيبراني**، مدونات الجزيرة، على الرابط : http://blogs.aljazeera.net/blogs/2017/8/ تاريخ الاطلاع : 24-04-2018.

13. جامعة الدول العربية، **الاتفاقية العربية لمكافحة جرائم تقنية المعلومات**، 2010، على الرابط: http://haqqi.info/ar/haqqi/legislation/arab-convention-cyber-%E2%80%8B%E2%80%8Bcrimes تاريخ الاطلاع : 20-04-2018.

14. حاتم فاروق ، **الإمارات تتقدم دول المنطقة في إصدار تشريعات الأمن السيبراني**، جريدة الاتحاد، على الرابط : http://www.alittihad.ae/details.php?id=66522&y=2017&article=full تاريخ النشر : 2017/11/08تاريخ الاطلاع : 2018/04/21

15. حسين أيمن ،**الإرهاب الالكتروني أخطر معارك حروب الفضاء**،على الرابط : http://alwatan.com/details/166324تاريخ النشر:2017/01/14، تاريخ الاطلاع : 23-04-2018.

16. حسونة هاجر ، **الإرهاب الالكتروني ...هل يتحول إلى مصدر التهديد الأول في العالم**، على الرابط : http://alkhaleejonline.net/articles/1430728333185670700/ تاريخ الاطلاع : 27-04-2018.

17. **ما الجديد في عقيدة الأمن السيبراني الروسي؟**، مركز دراسات كاتيخون، على الرابط : http://katehon.com/ar/article/m-ljdyd-fy-qyd-lmn-lsybrny-lrwsy تاريخ الاطلاع : 22-04-2018.

18. نشأت المنيري شيريهان ، **مخاطر جرائم الانترنت على استقرار النظام الدولي**، مجلة السياسة الدولية، على الرابط:http://www.siyassa.org.eg/NewsQ/2450.aspx تاريخ الاطلاع : 15-03-2018.

19. عبد الله السند عبد الرحمن ، **وسائل الإرهاب الإلكتروني وحكمها في الإسلام وطرق مكافحتها** من الرابط : http://shamela.ws/browse.php/book-1244/page-20 تاريخ الاطلاع : 10-04-2018.

20. عبد الصادق عادل ، **الحروب السيبرانية : تصاعد القدرات والتحديات للأمن العالمي**، المركز العربي لأبحاث الفضاء الالكتروني. على الرابط:http://accronline.com/article_detail.aspx?id=28395 ، تاريخ الاطلاع : 22-04-2018.

21. صبحي مروة ، **تسليح تكنولوجي: تنافس غير تقليدي في مجال التكنولوجيا العسكرية**، مركز المستقبل للأبحاث والدراسات المستقبلية، على الرابط : **http://rawabetcenter.com/archives/6591** تاريخ الاطلاع : 26-04-2018

22. شوقي إيهاب ، **الارهاب الالكتروني وجرائمه**، شبكة الاخبار العربية، على الرابط : https://www.assakina.com/awareness-net/rebounds/81251.html تاريخ الاطلاع : 26-04-2018.

23. خليفةايهاب ، **التطبيقات الأمنية لقوة الفضاء الالكتروني**، على الرابط : https://futureuae.com/ar/Mainpage/Item/851/cyber-power تاريخ الاطلاع : 23-04-2018.

24. نايلي نبيل ، **غنيمة حرب الصين السيبيرية**، على الرابط : http://www.mepanorama.net/295564/ تاريخ الاطلاع : 25-04-2018.

25. يسمينة رياض ، **مخاطر الهواتف الذكية بعد انتشار انترنيت الاشياء**، على الرابط : http://ar.itp.net/mobile/614057-%تاريخ الاطلاع: 27-04-2018.

ثانيا : باللغة الاجنبية :

A.Books :

1. Alix Desforges, **Cyberterrorisme : quel périmètre ?,** Fiche de l'Irsem n° 11, décembre 2011.

2. Edward Amoroso**, Cyber Security**, SiliconPress, 2007.

3. Joseph S.Nye JR , **Cyber Power**, Harvard Kennedy School, 2010.

4. Joseph S.Nye,JR, **Power and national Security in cyberspace, America's Cyber Future**, Center for a new America Security, V2, 2011.

5. Gabi Siboni, **Cyberspace and National Security**, Institute for Security Studies, Tel aviv, 2015.

6. Kenneth Geers**, Strategic Cyber Security**, CCDCOE,Tallinn, Estonia,2011.

7. Kristin M.lord&Travis Sharp, **America's Cyber Future**,Center for a new America Security, V1, 2011.

8. LivierNay , **Lexique de Science politique vie et Institutions politiques** ,Europe Media Duplication SAS, Toulouse, 2008 .

9. Marc Goodman, **Future Crimes**, Doubleday, Newyork, 2015.

10. NirKshetri, **The Quest to Cyber Superiority**, Springer, 2016 .

11. Olivier Kempf**, Introduction à la Cyberstratégie**, Paris, Economica, 2012.

12. Paulo & Jana Shakarian, Andrew Ruef, **Introduction to Cyber warfare, A multidisciplinaryApproach**, Elsevier, 2013.

13. Richard A. Kemmerer**, Cyber security**, University of California Santa Barbara, Department of Computer Science, 2003.

14. Richard A. Clarke & Robert knake,**Cyber War: The NextThreat to National Security and What to Do About It**, HarperCollins, 2010.

15. Shmueleven& David simanTov, **CybeWarfare**, Institute for Security Studies, Tel aviv, 2012.

B.Official documents:

1. **Tallinn Manual on the International Law applicable to Cyber Warfare**, Michael N.schmitt, Cambridge UniversityPress, 2013.

2. I**nternational Strategy for Cyberspace**, The white house, Washington,2011.

3. ITU, **Cyber security**, Geneva: International Telecommunication Union (ITU),2008.

4. The International Télécommunication Union, **ITU Toolkit for CybercrimeLégislation**, Geneva, 2010.

C.Reports :

1.**2016 US Governement Cybersecurity Report**, Security Scorecard R&D Departement, 2016.

2. Internet Security Threat report, Symantec, Volume 23, 2018. Accessed at : https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf seen : 02-04-2018

D.Reviews :

1.David Bisson, **A "Cyber" Study of the U.S. National Security Strategy Reports** , URL : **https://www.tripwire.com/state-of-security/government/a-cyber-study-of-the-u-s-national-security-strategy-reports**

2. Joseph S.Nye Jr, **Deterrence and dissuasion in Cyberspace**, Mit pressJournals, URL :https://www.mitpressjournals.org/doi/pdf/10.1162/ISEC_a_00266

3. W.J. Hennigan , **Trumpannounces plan to elevate U.S. military command thatoversees cyber operations**, Los Angles times , URL:**http://www.latimes.com/**

E. Web Sites :

1.**Cyber defence**, North Atlantic TreatyOnganisation, 19-02-2018, URL : https://www.nato.int/cps/en/natohq/topics_78170.htm, seen :24-04-2018.

2. David Smith, **How RussiaHarnesses Cyber Warfare**,Defense Dossier, American Foreign Policy Council ,August 2012.
URL :http://www.afpc.org/files/august2012.pdf, seen : 27-04-2018.3.

3. Mark Pomerleau**, WhatTrump's National Security Strategysays on Cyber ?**, URL :https://www.fifthdomain.com/civilian/2017/12/18/what-trumps-national-security-strategy-says-on-cyber,seen : 21-04-2018.

فهرس الأشكال والجداول

فهرس الأشكال والجداول :

فهرس المحتويات

فهرس المحتويات

ملخص الدراسة

ملخص الدراسة :

نعيش اليوم العصر الرقمي، بفضل الثورة الهائلة في تكنولوجيا المعلومات والاتصال، فزيادة التشابك في جميع المجالات، خلق بيئة جديدة للتفاعل بين الافراد والمجتمعات والدول، وهو ما اصطلح عليه بالفضاء السيبراني، هذا الفضاء الذي يتميز بالتطور السريع، والغموض الشديد، وخلق الاستخدامالسيء لهذا الفضاء، بيئة مليئة بالمخاطر والتهديدات، شكلت تهديدا خطيرا للأمن القومي للدول، حيث تغيرت مفاهيم القوة والصراع والحرب، وارتبطت طبيعتها بالفضاء السيبراني.

ومع بروز الأمن السيبراني كركيزة اساسية في بناء الأمن القومي، سارعت الدول وفي مقدمتها الولايات المتحدة الأمريكية، لتشكيل الهيئات والمؤسسات المدنية والعسكرية، وسن التشريعات القانونية، ووضع استراتيجية خاصة، لمواجهة التهديدات السيبرانية الحالية والمستقبلية، والدفاع عن أمنها، إضافة الى العمل على المستويين الإقليمي والدولي، من أجل فضاء سيبراني آمن وسلمي.

Abstract :

Today, We living the Cyber age, as a result of the ICT's revolution, the increase of the connectivity of all sectors, creating a new environment for interaction between individuals, communities and nations, which is called Cyberspace, which is characterized by rapid development, Full of dangers and threats, It posed a serious threat to the national security, where the concepts of power, conflict and war have changed, and their nature has been linked with Cyberspace.

Cyber-security as a key to building national security, States, primarily USA, have accelerated tocreate civil and military institutions, enacting legislations and developing a special strategy to fight current and future cyber threats, Also, they work at the regional and international levels, for a futur Cyberspace safe and peaceful.