الصفحة الرئيسية للمجلة: www.asjp.cerist.dz/en/PresentationRevue/796 PISSN : 2477-9970 - EISSN : 2822-1540

نموذج الولايات المتحدة الأمريكية في مجال الأمن السيبراني: بين ضرورة الهجوم وإمكانات الدفاع

The cybersecurity model of the United States of America : between the necessities of attack and the capabilities of defense

أ. مهوب وسام *

جامعة 20 أوت سكيكدة. الجزائر

w.mihoub@univ-skikda.dz

ملخص:

أضحى الفضاء السيبراني ساحة هامة لمختلف التفاعلات الدولية ومع تصاعد الهجمات السيبرانية بين الدول تأثر الأمن القومي لهذه الأخيرة فسعت الدول بصورة فردية أو جماعية إلى انتهاج سياسات من أجل تطوير قدراتها وسلوك إجراءات وقائية كافية لضمان صد كافة الهجمات السيبرانية فعلية كانت أم محتملة واتجهت إلى صياغة استراتيجيات تستجيب لتحديات الانترنت، سياسيا: إنشاء هيئات وطنية للأمن السيبراني، عسكريا: تشكيل جيوش وقوى سيبرانية تهتم بعمليات الدفاع والحماية وحتى الهجوم، قانونيا، قانونيا: تطوير منظومة قانونية وطنيا وإقليميا ودوليا تتلاءم مع التهديدات السيبرانية الجديدة وتراعي خصوصية الفضاء السيبراني

الكلمات المفتاحية : الأمن السيبراني؛ الحروب السيبرانية؛ الهجمات السيبرانية.

***

Abstract:

Cyberspace has become an important arena for various international interactions, and with the escalation of cyber-attacks between countries, the national security of the latter has been affected. Countries, individually or collectively, have sought to adopt policies in order to develop their capabilities and take sufficient preventive measures to ensure repelling all cyber-attacks, whether actual or potential, and have tended to formulate responsive strategies. To the challenges of the Internet, politically: establishing national bodies for cyber security, militarily: forming armies and cyber forces concerned with defense and protection operations and even attack, legally, legally: developing a national, regional and international legal system that is compatible with new cyber threats and takes into account the privacy of cyberspace

Keywords: *Cyber space ; Cyber wars ; cyber-attacks.*

* المؤلف المرسل: أ. مهوب وسام

المقدمة:

ترتب عن التطور الهائل في تكنولوجيا المعلومات والاتصالات ثورة حقيقة كانت شاملة للمشهد العام للحياة اليومية على كافة الأصعدة: اجتماعيا، اقتصاديا وحتى سياسيا وأمنيا. وفي المقابل من ذلك عرفت المخاطر السيبرانية استزادة ملحوظة لم تنحصر تداعياتها في الفضاء الافتراضي أو الرقمي فحسب ليصبح بذلك تحدي الأمن السيبراني أعلى درجات التحديات التي تواجهها الدولة الوطنية الحديثة (بمفهومها الوستفالي)، خصوصا مع ما يميز الهجمات السيبرانية؛ تأثيراتها سريعة وفجائية وفعالة إلى جانب انتفاء البعد الجغرافي عدا عن التكلفة العالية لاستخدام النظام الآلي.

تتمثل **أهمية** تناول الموضوع بالدراسة في كون الولايات المتحدة الامريكية دولة رائدة في مجال الفضاء السيبراني؛ إذ أدت التقنيات الرقمية المتطورة إلى زيادة التشابك في البنى العسكرية والسياسية والإقتصادية والاجتماعية لتصبح أكثر حساسية وأشد سرعة في تفاعلها مع البيئة الخارجية، ومع ما شهدته الولايات المتحدة الأمريكية من هجمات سيبرانية تمس البنى السياسية والاقتصادية على غرار الشركات الاقتصادية والتجارية بالاعتماد على فيروسات إلكترونية خطيرة جدا ومعقدة مقارنة بالبرامج الإلكترونية الخبيثة، فإنها لجأت إلى المحافظة على ميزة تفوق الجيش الأمريكي داخل الفضاء السيبراني بغرض تعزيز ردع الهجمات في وقتي السلم والحرب معا، والتوجه نحو بناء وتطوير رأس مال تكنولوجي وبشري بإمكانه تقوية تنافسية الولايات المتحدة الأمريكية في الفضاء السيبراني.

تهدف الورقة البحثية إلى إبراز أهمية ضمان الأمن السيبراني للدول الوطنية بشكل عام والولايات المتحدة الأمريكية على وجه الخصوص، من خلال فهم التهديدات السيبرانية التي تواجهها الولايات المتحدة الأمريكية من مقاربة هجومية، وكذا الإحاطة بالأدوار الأمريكية في الفضاء السيبراني لدى تموضعها في موضع الدفاع وصولا إلى الجهود الوطنية في تحقيق الأمن السيبراني وطنيا إقليميا وحتى دوليا وهذا من خلال الاعتماد على **مقاربة منهجية** متعددة الأبعاد (تاريخية ونسقية) **لمعالجة الإشكالية** التالية: **كيف تستجيب الولايات المتحدة الأمريكية لمختلف التهديدات التي تمس أمنها الوطني في الفضاء السيبراني؟**

للإجابة عن هذه الإشكالية تركز الورقة البحثية على تحليل العناصر التالية:

أولا: إمكانات الولايات المتحدة الأمريكية في تبني الطرح الدفاعي في الفضاء السيبراني

ثانيا: المقاربة الهجومية في الاستراتيجية الأمريكية لمواجهة التهديدات السيبرانية

ثالثا: تقييم التجربة الأمريكية في مجال الأمن السيبراني

أولا: إمكانات الولايات المتحدة الأمريكية في تبني الطرح الدفاعي في الفضاء السيبراني

يعتبر جوزيف ناي من أبرز الباحثين المهتمين بالقوة السيبرانية حيث يعرفها أنها: "القدرة على الحصول على النتائج المرجوة من خلال استخدام مصادر المعلومات المرتبطة بالفضاء السيبراني، أي أنها القدرة على استخدام الفضاء السيبراني لإيجاد مزايا الدولة والتأثير على الاحداث المتعلقة الأخرى وذلك عبر أدوات سيبرانية[1]".

كما يوضح بأن مفهوم القوة السيبرانية يشير إلى "مجموعة الموارد المتلقة بالتحكم والسيطرة على أجهزة الحاسبات والمعلومات والشبكات الإلكترونية والبنية التحتية المعلوماتية والمهارات البشرية المدربة للتعامل مع هذه المسائل" هذا ويشترط ناي توفر عدة عناصر من أجل ممارستها نفوذها داخليا وخارجيا عبر القوة السيبرانية:

- بنية مؤسساتية تتولى مهمة ممارسة القوة السيبرانية وتحقيق الأمن السيبراني للدولة.
- بنية تشريعية تكون ضامنة ومحددة لاستعمال القوة السيبرانية.
- بنية تحتية سيبرانية تشمل أجهزة الكمبيوتر بمختلف الأنظمة والقطاعات.
- استراتيجية بأهداف واضحة تحدد طرق العمل والأهداف المرجوة [2]

يعتقد جوزيف ناي أن الأمن السيبراني للولايات المتحدة الأمريكية يواجه أربعة أصناف من التهديدات؛ إذ أن كلا من الحروب السيبرانية والتجسس الاقتصادي ترتبط أساسا بالفواعل الدولتية فيما ترتبط الجريمة والإرهاب السيبرانيين بالفواعل غير الدولتية.

الجرائم السيبرانية: بالعودة إلى التقرير الرسمي عن مركز الدراسات الإستراتيجية في واشنطن (**CSIS**) بمعية شركة ماكافي لبرنامج الأمن المعلوماتي (**McAfee**) والذي تم نشره مطلع سنة 2018 فإنه يبدو جليا النمو المتسارع في خسائر الجرائم السيبرانية لتنتقل من 45 مليار دولار عام 2014 نحو 600 مليار دولار عام 2017 وهو الرقم المرشح نحو الإرتفاع تباعا حيث يعود هذا التزايد إلى الاستخدام المتطور للأساليب التكنولوجية في تنفيذ الجرائم السيبرانية إلى جانب تسهيل حركة وتبادل العملات الرقمية[3]

التجسس السيبراني: يُعنى بجمع المعلومات مع مقابل مادي وبما أنه يهدد قطاعات هامة منها العسكرية الأمنية السياسية والصناعية فإن له آثار استراتيجية جد خطيرة، تلقت أنظمة الحاسوب التابعة للجيش الأمريكي سنة 2008 أخطر الهجمات بفعل التجسس السيبراني إذ تم نقل الآلاف من البيانات والمعلومات الإلكترونية السرية إلى خوادم خارجية جديدة وتم استهداف أكثر من 72 شركة تم إحصاء 13 منها كانت تابعة لمقاولي وزارة الدفاع الأمريكي حيث كان الهدف تحصيل معلومات تدور حول استراتيجيات وهياكل عسكرية وأمنية هذا وقد شهدت المواقع الإلكترونية التابعة لشركة لوكهيد مارتن (**Lockheed Martin**) الأمريكية هجمات سيبرانية[4]

التحريض الإلكتروني: أين يكون الفضاء السيبراني هو المجال الحيوي الذي يمارس فيه التخويف والتضليل والتأثير لغايات سياسية أو حتى آيديولوجية، فعلى سبيل المثال فإن تنظيم أنونيموس (**Anonymous**) أجرى العديد من الهجمات السيبرانية التي تعد رفيعة المستوى وكان ذلك ردا على اعتقال مؤسس موقع ويكيليكس (**Wikileaks**) جوليان أسانج (**Julian Paul Assange**) حيث تسببت تسريبات هذا الموقع بزرع الإرتباك ونشر عدم الثقة في المؤسسات الحكومية الرسمية الأمريكية بل وأدت إلى زيادة التوترات السياسية والأمنية بينها وبين حلفائها خصوصا وأنها كشفت الكثير من الحقائق التي تدور حول مسؤولين سامين في الدولة[5]

الحروب السيبرانية: مثل التدخل الروسي في الانتخابات الرئاسية الأمريكية سنة 2016 عهدا جديدا في الحروب السيبرانية خصوصا مع سعي الطرف الروسي لدعم المترشح للرئاسة آنذاك دونالد ترامب (**Donald Trump**) وبهذا انتقلت الحروب السيبرانية من الساحة العسكرية والاستخباراتية إلى الساحة االديمقراطية.

هذا وقد وجهت وزارة العدل الأمريكية اتهامات جنائية وفرضت عقوبات على شركة إيرانية وتسعة أفراد إيرانيين ناشطين في مجموعة مابنا الإيرانية (**Mapna Group**) حيث قاموا بالاتجاه نحو اختراق أنظمة حساسة لمئات الجامعات والشركات وحتى الأشخاص بهدف الإستحواذ على البيانات العلمية والاستيلاء على البحوث الأكاديمية.

تسعى الولايات المتحدة الأمريكية إلى تحقيق عدة غايات وأهداف من أجل ضمان أمنها في الفضاء السيبراني:

حفظ الأمن: الذي يتحقق عن طريق ردع الهجمات السيبرانية واعتماد هندسة مناسبة للنظم والشبكات مع استحداث نظم دفاعية متينة، هذا ولابد كذلك من مراعاة المعايير العالمية في بناء

سلوكات الفواعل الحكومية وحماية المدنيين من خلال ضمان الإستخدام السليم للقوى السيبرانية خدمة للصالح الأمريكي.

فرض الهيمنة: بالحفظ على تفوق الجيش الأمريكي في الفضاء السيبراني بغرض تعزيز ردع الهجمات وقت السلم والحرب معا، تطوير رأس مال تكنولوجي وبشري وحماية المعلومات والبيانات الفكرية والتجارية.

الحفاظ على الاتصالات: من خلال ضمان مصادر أنترنت آمنة ومفتوحة وهو ما ينعكس إيجابا على الأبعاد الاقتصادية والاجتماعية، زيادة الإبتكار والتقدم العلمي، رفع مستوى التفاعل الاجتماعي والثقافي، صد الجريمة السيبرانية بالحفاظ على موثوقية الأنترنت وهو ما يحمي المصالح الوطنية للولايات المتحدة الأمريكية.

كما تواجه الامن القومي الأمريكي جملة من التحديات الحقيقة في مجال الأمن السيبراني:

انتفاء البعد الجغرافي مع الزيادة في سرعة نقل المعلومات ولذلك لا يتوفر الفضاء السيبراني على ميزة الإنذار المبكر للهجوم وافتقاد القدرة على تحديد المواقع الجغرافية غرض الرد عليها، إذ أن الهجمات السيبرانية تكون مفاجئة مباغتة وسريعة جدا وبالتالي لا تكون مرهونة بالبعد الجغرافي وتظل الأهداف عرضة للهجوم دون معرفة الفاعل مع عدم إمكانية وجود الوقت الكافي للرد أو حتى الصد.

سهولة وإتاحة الإتصال عن طريق الانترنت وبذلك فإن الدخول إلى الانترنت يفتقد للحواجز التي تعيق الإتصال به لذلك فإن ذلك يتيح للمهاجمين تحقيق غايات ضخمة مقارنة بتكلفة أقل في الوقت الذي تحتاج فيه الهجمات المتطورة إلى قدرات عالية.

تزايد حجم وكثافة الهجمات السيبرانية ضد الولايات المتحدة الأمريكية وهو ما يزيد من خطر استهداف مواقع أمنية عسكرية وسياسة واقتصادية وحتى اجتماعية خصوصا وأن الهجوم على البنى التحتية بإمكانه إلحاق أضرار هائلة ليصبح بذلك مجرد التهديد بالهجوم لوحده أسلوب للردع.

ضبابية معايير السلوك فهي غالبا ما تكون غير واضحة أو غير مقبولة في الفضاء السيبراني لعدم وجود قواعد متفق حولها خصوصا وأن الفضاء السيبراني بإمكانه أن يوفر للمهاجمين ما يكفي من أجل التمكين من ممارسة كافة أشكال وأنماط الهجمات السيبرانية[6].

ثانيا: المقاربة الهجومية في الاستراتيجية الأمريكية لمواجهة التهديدات السيبرانية

حسب الوكالة الروسية للاستشارات الأمنية (زيكوريون- **Zecurion**) فإن الولايات المتحدة الأمريكية تتجه إلى الإنفاق بشكل كبير على أمن الفضاء السيبراني مقارنة ببقية الدول في العالم حيث تصل الميزانية السنوية للولايات المتحدة الأمريكية في هذا الشأن إلى 7 مليار دولار أمريكي، فيما يصل تعداد الموظفين إلى حوالي 9000 موظف فيما تنفق بالموازاة مع ذلك كل من الصين 1,5 مليار دولار والمملكة المتحدة 450 مليون دولار، هذا وتخصص كوريا الشمالية ما مقداره 20 بالمئة من الميزانية العسكرية لصالح الأمن السيبراني.

1- الحروب السيبرانية ممثلة وفقا للثنائية (دولة_دولة): (إيران-أمريكا)

في سنة 2010 تعرض البرنامج النووي الإيراني لهجوم إلكتروني مدمر كان غرضه إيقاف أنشطة إيران النووية، ووجهت أصابع الاتهام لكل من أمريكا، بريطانيا، فرنسا، ألمانيا وحتى إسرائيل ولكن أبرزها الولايات المتحدة الأمريكية وإسرائيل وهذا راجع لعدم جدوى العقوبات الاقتصادية المفروضة على إيران[7].

وقد أدى هذا الفيروس إلى تعطيل معمل أصفهان لتبديل ثاني أكسيد اليورانيوم إلى اليورانيوم الطبيعي وذلك من خلال ضرب البرامج المعلوماتية، وهذا ما تسبب في تعطيل أكثر من 30 ألف حاسوب بمفاعل "نطنز" كما دمر أيضا حوالي 100 جهاز طرد مركزي في "نطنز"، ولم تتمكن إيران من افتتاح المفاعل في أوت 2010 كما كان مقررا من قبل بل تم افتتاحه في سبتمبر 2011، بعد مرور عام من تاريخ الهجوم أي بعد خسارة مليارات الدولارات في إصلاح ما أفسده فيروس "ستاكنست"[8]

لم يتوقف الهجوم السيبراني على إيران عند هذا الحد بل شهدت هجوما آخر لبرنامجها النووي سنة 2012 بواسطة فيروس آخر يدعى فيروس "فلايم" أو الشعلة (**http://www.umayya.org**) والغرض من هذا الفيروس هو التجسس وليس التدمير، وذلك من خلال سرقة البيانات والتسجيلات الصوتية بواسطة الميكروفونات الداخلية في الأجهزة، تسجيل حركات الضغط على لوحة المفاتيح **Keystrokes** وأخذ صور من الرسائل النصية على الجهاز.

هذا وقد تجددت على إيران الهجومات الإلكترونية في يونيو 2019، حيث قامت إدارة ترامب بشن هجوم إلكتروني على قاعدة بيانات الحرس الثوري المستخدمة لشن هجومات على ناقلات النفط، مما تسبب في مسح شاشات الحرس الثوري. كما عاودت الولايات المتحدة الأمريكية هجوما آخر في سبتمبر 2019،بعد أن أطلقت إيران طائرات دون طيار وصواريخ كروز على منشأتين نفطيتين، وفي مقابل تلك الهجمات قامت إيران هي الأخرى بتوجيه ضربات أو هجمات إلكترونية من أجل رد

الإعتبار ومن بين أبرز تلك الهجمات عملية أبابيل سبتمبر 2013/2012 والتي استهدفت المؤسسات المالية الأمريكية وتزامن وقوع هذه العملية مع الفترة التي كانت واشنطن تفرض فيها عقوبات على البنك المركزي الإيراني وتم استخدام هجمات موزعة للحرمان من الخدمات وذلك من أجل تعطيل وعرقلة برامج الخدمات المصرفية عبر الأنترنيت إضافة إلى توقيف بعض الوظائف التجارية لإحدى الركائز الحساسة في الاقتصاد الأمريكي مما تسبب في خسائر وأضرار بلغت عشرات ملايين الدولارات، وبالرغم من أن هذه الهجومات تنسب إلى المقاتلين الإلكترونين في كتائب عز الدين القسام لكن يرجح بأن الحكومة الإيرانية وراء ذلك [9]

وفي27 سبتمبر 2013 عاودت إيران الكرة وذلك حين قام قراصنة إيرانيون باختراق أجهزة الكمبيوتر التابعة للبحرية الأمريكية، ولم تكتف إيران بهذا بل قامت أيضا في السنة الموالية أي عام 2014 باستهداف شركة "لاس فيغاس ساندر كلوب" ونتج عن هذا الهجوم غلق أنظمة الاتصالات ومسح محركات الأقراص الصلبة.

ولم تكتف إيران بهذا القدر من الهجومات السيبرانية على الولايات المتحدة الأمريكية بل واصلت أعمالها الهجومية والمقرصنة وأبرز مثال على ذلك فيروس شمعون بحملاته الثلاث، وآخرها كان في سنة 2016 بعدها عرفت العلاقات الإيرانية الأمريكية نوعا ما فترة من الهدنة أو الاستقرار لتعود للواجهة مرة أخرى، حيث تزامن ذلك مع انسحاب إدارة دونالد ترامب من الصفقة النووية لسنة 2018 حيث حذرت شركة كروويد ستريك للأمن السيبراني عملائها بأن تزايدت بشكل ملحوظ عمليات الاختراق والتصيد من قبل إيران وفي سنة 2019 ادعت شركة مايكروسفت بأن هناك محاولة اختراق لحسابات البريد الالكتروني التي تتعلق بمسؤولين وصحفيين للحكومة الأمريكية والحملة الرئاسية بصفة عامة وهذه الاختراقات قام بها مجموعة من الهاكرز وكما يطلق عليها باسم "الفوسفور "التابعين للحكومة الإيرانية.

وفي مطلع سنة 2020 شهدت إيران حادثة إغتيال قاسم سليمان وهو قائد فيلق القدس التابع للحرس الثوري وهو ما أسهم في تأجيج الصراع بين الطرفين (إيران والولايات المتحدة الأمريكية) وزاد من معدل الهجمات السيبرانية الإيرانية. حيث أنه في اليوم الموالي أي بعد وقوع الحادثة بيوم قامت إيران بعملية إختراق الموقع الالكتروني لبرنامج مكتبة الإيداع الفيدرالية الأمريكية هذا ما زاد من احتمال حدوث تصعيد التوتر بين الطرفين مع إمكانية حدوث حرب إلكترونية حقيقية خاصة بعد إعلان إيران عن نيتها في الانتقام وشن هجمات جديدة تمس البنوك، المرافق والقطاعات الحيوية

(**Siboni, p 18**).... وبالرغم من أن إيران ليست لديها نفس درجة التقدم والخبرة التي تمتلكها الولايات المتحدة الأمريكية في مجال الأمن السيبراني خاصة وأن هذه الأخيرة (الولايات المتحدة الأمريكية) لديها ترسانة دفاعية سيبرانية تمكنها من صد أي هجوم الكتروني لكن كل هذا لا يمنع إيران من تطوير أنظمتها الإلكترونية التي تؤهلها للقيام بالهجمات السيبرانية مستقبلا. كما نستخلص أيضا بأن هذه الحرب بين الدولتين ليست مرهونة بزمن معين أو محدد فهي مازالت مستمرة ومازالت ردود الانتقام متواصلة من قبل الطرفين لكن يبقى هناك احتمال العدول وعدم تصعيد الأزمة والتي يمكن من خلالها حدوث التصادم المباشر فكل هذه الاحتمالات مرهونة بالأوضاع السياسية والاقتصادية الدولية في السنوات القادمة.

الحروب السيبرانية ممثلة وفقا للثنائية (دولة-شركة دولية): (الصين-شركة غوغل)

شهدت العلاقات الأمريكية الصينية على مر العصور توترات وصلت إلى حد الصراع في جميع المجالات فبعدما كان صراعا عسكريا، جيوبوليتكيا أصبح تجاريا، إقتصاديا سيبرانيا يخص مجال الفضاء الالكتروني ومع مبدأ انعدام الثقة في الطرف الاخر حسب ما تؤمن به المقاربة الواقعية، بأن الطرفين أصبحا يشككان في نوايا بعضهم البعض وأي محاولة يقوم بها الطرف (أ) هي بمثابة عملية تجسس ومحاولة إختراق للطرف (ب)، خصوصا بعد استثمار كلا الدولتين في الأنظمة الشبكية أو كما يسميها **xinxibia** أو.**informatization** مارستا الدولتان التجسس الالكتروني ضد بعضهما البعض ولأسباب عديدة ومن أشهر الهجمات السيبرانية اللاتماثلية التي حدثت في العقود الأخيرة هي الهجوم أو النزاع السيبراني بين الصين وشركة غوغل الأمريكية.[10]

فمنذ دخول شركة غوغل لسوق الصين في عام 2006، حدث إشتباك بين محرك البحث العملاق غوغل وحكومة جمهورية الصين بخصوص الرقابة وقضايا أخرى. وقد تطور محرك البحث **google** الصيني ليصبح بذلك ثاني أكبر خدمات جمع المعلومات استخداما في الصين بعد الشركة الصينية **Baidu** ،وكان أيضا أقل تعرضا للرقابة كما أن شركة غوغل حاولت الامتثال لسياسات الرقابة في جمهورية الصين الشعبية فحددت خدماتها فقط كمحرك بحثي، دون تقديم خدمات البريد الإلكتروني، كما أنها كانت تضع أو تقدم رسائل للمستخدمين الصينين تفيد بأن أحد المواقع المحجوبة أصبح غير متاح بسبب القوانين واللوائح والسياسات المحلية، مما يوحي للمستخدم الصيني بوجود معلومات، لكن الحكومة الصينية أغلقت الوصول إلى هذا الموقع .

وفي 2010 هددت غوغل **Google** بوقف تصفية محرك البحث الصيني الخاص بها أو الانسحاب من الصين، وأكدت الشركة أنه في ديسمبر 2009 هاجم قراصنة صينيون خدمة **Gmail** الخاصة بها وشاركوا في دمج الشبكة بالإضافة إلى أنظمة الكمبيوتر للعديد من الشركات الأمريكية الكبيرة الأخرى في الصين في ما أطلقت عليه الصحافة اسم "عملية فجر""**auroia opération**" والتي تم فيها إختراق الأجهزة الالكترونية التابعة للشركة وذلك من أجل سرقة المعلومات الموجودة فيها، كذلك اختراق حسابات **Gmail** لنشطاء حقوق الإنسان الصينين، ومسؤولين في الإدارة الأمريكية وبالرغم من أن **Google** أكدت في فبراير 2010 بأن الهجمات جاءت من الصين، إلا أن بكين نفت تورطها ودافعت عن سياسات الانترنت الخاصة بها. وذكرت وزارة الخارجية للصين أن الشركات الأجنبية بما في ذلك غوغل **Google** يجب أن تحترم القوانين واللوائح كما تحترم المصلحة العامة للشعب الصيني وثقافة وعادات الدولة الصينية. وردا على هذا قامت شركة غوغل بتحويل محركها البحثي للمستخدمين في الصين إلى آخر في هونغ كونغ غير خاضع لأي شكل من أشكال الرقابة ومن خلال هذا اعتبر الاعلام الصيني أن ما تقوم به شركة غوغل هو جزء من مؤامرة أمريكية على الصين[11].

وبالرغم من إدعاء الحكومة الصينية والإعلام الصيني بأن هناك مؤامرة تحاك من قبل الولايات المتحدة الأمريكية وإتهامها بالتجسس. لا يعتبر مبررا قويا لتلميع صورتها أمام الرأي العام العالمي، فهي متهمة أيضا من طرف عدة دول ليس فقط الولايات المتحدة الأمريكية بل أيضا ألمانيا، فرنسا، المملكة المتحدة وغيرها من الدول الأخرى.

ومن خلال هذا التنازع بين شركة غوغل والصين نستنتج بأن العلاقات بين الدول لا تتأثر فقط بالفواعل الدوليين، وإنما تتأثر وتتوتر حتى بين فواعل غير دولية أو فواعل غير متماثلة (دولة في مقابل شركة) ما يحدث علاقات على مستوى العلاقات بين الدول ويتعداه كذلك إلى مستويات ومجالات أخرى تؤثر في هيكلة النظام الدولي أو حتى في قضايا السياسة العالمية.

إضافة إلى هذين الهجومين عرفت البيئة الدولية هجومات سيبرانية عديدة نذكر منها:

_دولة إستونيا ففي عام 2007 تعرضت لهجوم إلكتروني مس المواقع الخاصة للبنوك، والجرائد والخدمات الحكومية الالكترونية ما أدى إلى تعطيل وإيقاف تلك المواقع على تقديم خدماتها وأيضا تعطيل كافة أجهزة الدولة، ما جعل من دولة إستونيا تستعين بحلف الناتو **NATO** من أجل مواجهة هذه الهجومات وقد وجهت إستونيا اتهامات للحكومة الروسية بكونها هي من قامت بتلك الهجمات ،وذلك بعدما اكتشفت إستونيا أن أنظمة التحكم التي تم شنها موجودة في روسيا وبالرغم من إنكارها

لعلاقتها بالهجوم ،إلا أنها اعترفت بأنه من الممكن أن يكون قد شن من داخل روسيا وذللك من قبل منظمات إجرامية ،وانه ليس هناك دخل ولا صلة للحكومة الروسية بهذا الهجوم لكن كل هذا النفي والإنكار لم يخدم روسيا خاصة أمام المجتمع الدولي فأغلب الدول وجهت أصابع الإتهام لروسيا[12].

_الهجوم الالكتروني اللاتماثلي (كوريا الشمالية ضد شركة صوني بيكتشرز للأفلام السينمائية والأعمال التلفزيونية والتوزيع) على غرار شركة غوغل لم تسلم شركة صوني بيكتشرز هي الأخرى من الهجمات السيبرانية، وقد كان هذا في نوفمبر من عام 2014 بسب فيلم المقابلة(**the interview**) الكوميدي الذي تدور أحداثه حول مسألة إغتيال زعيم كوريا الشمالية كيم جونغ أون(-**Kim jong un**) وقد أدى هذا الهجوم إلى نشر معلومات حساسة خاصة بالاستوديو السينمائي والتي تشمل معلومات شخصية ورسائل الموظفين الالكترونية، إضافة إلى أفلام لشركة صوني للأفلام السينمائية و الأعمال التلفزيونية والتوزيع لم تعرض بعد كما قد تعرضت أعمال الشركة بدرجة كبيرة. وقد تبنت هذا الهجوم مجموعة أطلقت على نفسها اسم حراس السلام (**Guardian of peace**) كما هددت أيضا بتنفيذ هجومات أخرى من بينها هجمات مادية على صالات العرض وهذا إذ واصلت شركة صوني بيكتشرز للأفلام السينمائية والأعمال التلفزيونية والتوزيع خطتها لإطلاق فيلم المقابلة.

وبخصوص مصدر هذا الهجوم ومن كان وراءه، ثم توجيه أصابع الإتهام لكوريا الشمالية وهذا بعد تدخل الولايات المتحدة الأمريكية وقيامها بفتح تحقيق حول مصدر الهجوم ودوافعه وهذا بالتعاون مع شركة صوني بيكتشرز للأفلام السينمائية والأعمال التلفزيونية والتوزيع، وقد خلص هذا التحقيق إلى بيان صدر عن مكتب التحقيقات الفيدرالي الأمريكي **FBI** بأن كوريا الشمالية هي من تقف وراء هذا الهجوم وهي المسؤول الأول عن هذه الهجمات كون أن هذه الأخيرة سبق لها وأن استخدمت وسائل التسلل والقرصنة الكترونية مماثلة في هجمات سابقة قامت بها ومن بينها دولة كوريا الجنوبية.

ثالثا: تقييم الاستراتيجية الأمريكية في مجال الأمن السيبراني

بغرض الإحاطة بدرجة اهتمام القرار الأمريكي بالأمن السيبراني اتجه دافيد بايسون – **David bisson** سنة 2015 إلى عمل دراسة حول التقارير الرسمية لاستراتيجيات الأمن القومي الأمريكية بالنظر في استخدامها لمصطلح (**Cyber**)، وقد توصل إلى وجود زيادة في تكرار استخدام المصطلح بـ 41 مرة في تقرير ترمب سنة 2017 ثم أوباما ب، 41 مرة في تقريري 2006 و 2010 فيما استعمل بوش المصطلح مرة واحدة، أما كلينتون فقد استخدم المصطلح 22 مرة[13]

مع انتخاب الرئيس السابق أوباما تزيد استخدام مصطلح "السيبرانية" في تقارير استرايتيجية الأمن القومي الأمريكي وتم إنشاء قيادة للحرب السيبرانية الأمريكية عام 2010 فيما أضحت الأنترنت واحدة من أخطر التحديات الأمنية الوطنية وتهديدا للسلامة العامة ، فيما تميز عام 2015 بالتركيز على التجسس السيبراني والمعايير الدولية والحاجة للحفاظ على فضاء سيبراني عالمي مشترك، أما في عهد ترامب فقد أولت الوثيقة أهمية قصوى للعصر السيبراني والأمن السيبراني وتحديد الفاعلين والتحديات والفرص التي يخلقها بالإضافة إلى محاربة الجريمة السيبرانية وبناء القدرات السيبرانية

وعلى اعتبار الدور المركزي للولايات المتحدة الأمريكية في إنشاء الأنترنت فقد ظلت رائدة في هذا المجال وهو ما ينعكس على استراتيجياتها في الأمن القومي

- الجهود الوطنية لمواجهة التهديدات السيبرانية:

فيما يتعلق بالجهود الوطنية نجد أنه بالرغم من تكتل الدول والمنظمات الدولية الحكومية وغير الحكومية في إطار دولي وإقليمي لوضع استراتيجيات بخصوص الأمن السيبراني أو التهديدات التي تنجم عنه، لم يمنع هذا الدول فرادى أن تضع هي الأخرى استراتيجيات تخص أمنها القومي، فعلى سبيل الذكر نجد الولايات المتحدة الأمريكية بالرغم من أنها تعد قوة كبرى إضافة إلى تحكمها في المجال التكنولوجي إلا أنها قامت بوضع استراتيجيات لمجابهة الأخطار التي تنجم عن الهجمات السيبرانية خصوصا وأننا في عصر الحروب الذكية والتي تعتمد بالدرجة الأولى على الأسلحة الالكترونية لمواجهة العدو دون قدرته على تحديد مصدر الهجوم أو حتى اكتشافه في بعض الأحيان إلا بعد فوات الأوان.

ومنه نجد الولايات المتحدة الأمريكية تضع الأمن الالكتروني على قمة أولويات الأمن القومي الأمريكي، حيث يرى المسؤولون في الولايات المتحدة الأمريكية أن هذه التهديدات السيبرانية يمكن أن تتجاوز ظاهرة الإرهاب خلال السنوات القادمة، كما أن أغلب التقارير والدراسات التي تعنى أو تهتم بمناقشة قضايا التهديدات الالكترونية والتي تتوقع حدوث حرب سيبرانية في العقود القادمة هي دراسات أمريكية كما أن بعضها صادر عن المؤسسات الرسمية[14].

ومن أهم الإدارات التي تعنى بالأمن الالكتروني على المستوى الفدرالي نجد وزارات الداخلية والدفاع، كذلك مكتب الأمن الإلكتروني والاتصالات كذلك مركز حماية البنى التحتية الوطنية، بالإضافة إلى قطاع جرائم الحاسب الآلي، كما قامت وزارة الدفاع بإنشاء قيادة فرعية تحت اسم

"وحدة القيادة الالكترونية" وتعمل هذه الوحدة للقيادة الالكترونية على تحقيق خمسة أهداف أساسية أولها اعتبار مجال الفضاء السيبراني مجال عملياتي مثله مثل الجيش والمجالات الجوية، البرية والبحرية أيضا استخدام مفاهيم جديدة لمصطلح الأمن وهذا يشمل كافة الأبعاد ومن بينها البعد الالكتروني ومن بين الأهداف أيضا بناء علاقات مع شركاء دوليين، كذلك التعاون مع القطاع الخاص. كما تهدف أيضا وحدة القيادة إلى اكتساب الخبرة والمهارات اللازمة والتي تمكن الجيش الأمريكي من تحقيق انتصارات في هذا المجال، ومن بين الاستراتيجيات أيضا التي تضعها الولايات المتحدة المريكية لضمان فضاء سيبراني آمن خال من الافتراءات والجوسسة.

وعلى غرار كل هذا نجد أن الولايات المتحدة الأمريكية قد بادرت باستراتيجيات لنشر قدرات الدفاع السيبرانية الحالية للدفاع بشكل استباقي عن الوكالات الحكومية المدنية، والبنية التحتية الحيوية. كذلك التفكير في إنشاء خدمة الأمن السيبراني الإتحادي للانخراط في الوقت المناسب في العمليات الدفاعية، إعطاء أولوية أكبر للوكالات الاستخباراتية الأمريكية وذلك من أجل جمع المعطيات الاستخباراتية التكتيكية على الانترنيت لمجابهة أي تهديد على الحكومة ومختلف البنى التحية الحيوية للدولة ،كما قامت أيضا بإنشاء إطار دائم للشراكة بين القطاعين العام والخاص، وهي الأخرى سعت أيضا إلى دمج الحماية ضد مشاركة الدولة في سرقة الانترنيت في الاتفاقيات متعددة الأطراف.

هذا فيما يتعلق بالاستراتيجية الأمريكية أما فيما يتعلق بالاستراتيجية الروسية فهذه الأخيرة إستراتيجيتها الأمنية المتعلقة بالأمن السيبراني تختلف عن الاستراتيجية الأمنية الأمريكية فهي تؤمن بضرورة تحقيق السيادة الوطنية في مجال الانترنيت **Internet Sovereignty** كما تعتمد روسيا في استراتيجيتها على استخدام الوسائل الالكترونية الهجومية. فهي تعمل على تعطيل البنية التحتية المعلوماتية للخصم، وكذلك الاتصالات المدنية والعسكرية له قبل الخوض في العمليات العسكرية التقليدية.

تولي الولايات المتحدة الامريكية عدة أولويات من أجل بناء فضاء سيبراني آمن ومفتوح:

- الميدان الاقتصادي: بتعزيز المعايير الدولية والابتكار والأسواق الحرة والمحافظة على بيئة للتجارة الحرة التي تشجع الإبتكار التكنولوجي وإمكانية الوصول إلى الشبكات العالمية وحماية الملكية الفكرية

- ميدان حماية الشبكات بتعزيز الأمن والموثوقية والمرونة لاسيما بشأن قواعد السلوك الدولي والأمن السيبراني ومحاربة الإختراقات والتداخل بين الشبكات الذي يقوض الأمن القومي وبناء قدرات

لاستعادة البنية التحتية للمعلومات مع توفير الأجهزة والبرمجيات الموثوق بها لسلامة البنية التحتية للشبكات والمعلومات

- ميدان تطبيق القانون بتوسيع القانون الدولي وإرساء سيادة القانون والمشاركة في تطوير سياسة مكافحة جرائم الأنترنت ومناقشة تطوير المعايير والتدابير الدولية ذات الصلة بالجرائم السيبرانية بغرض مواءمة قوانين الجريمة السيبرانية على الصعيد الدولي

- في الميدان العسكري بتكييف استراتيجيات مختلفة مع المتطلبات العسكرية المتزايدة لشبكات آمنة وموثوقة والعلم على جاهزية الجيش الأمريكي للتحرك في بيئة يسعى بعض الفاعلين لتعطيل أنظمتها أو تدمير البنية التحتية الحيوية للدفاع الوطنية إلى جانب تعزيز وحتى بناء تحالفات عسكرية لمواجهة التهديدات الفعلية والمحتملة في الفضاء السيبراني

- في ميدان حوكمة الأنترنت يتعزيز الهياكل الفعالة والشاملة وإعطاء الأولوية للإنفتاح والإبتكار فالقدرة على توزيع المعلومة بكفاءة في الفضاء السيبراني يعتبر جوهر النشاط الإستهلاكي والتجاري والسياسي والعلمي الحديث بالإضافة إلى السعي للحفاظ على أمن واستقرار الشبكة العالمية وتثمين النقاش بين الفاعلين في إدارة الأنترنت

- ميدان التنمية الدولية وبناء القدرات وتوفير المعرفة الضرورية والتدريب لصالح الدول التي تسعى لبناء قدرات تقنية وتحقيق الامن السيبراني وتوفير التواصل المنتظم والمستمر مع الخبراء

خاتمة:

أضحى الفضاء السيبراني ساحة هامة لمختلف التفاعلات الدولية ومع تصاعد الهجمات السيبرانية بين الدول تأثر الأمن القومي لهذه الأخيرة فسعت الدول بصورة فردية أو جماعية إلى انتهاج سياسات من أجل تطوير قدراتها وسلوك إجراءات وقائية كافية لضمان صد كافة الهجمات السيبرانية فعلية كانت أم محتملة واتجهت إلى صياغة استراتيجيات تستجيب لتحديات الانترنت، سياسيا: إنشاء هيئات وطنية للأمن السيبراني، عسكريا: تشكيل جيوش وقوى سيبرانية تهتم بعمليات الدفاع والحماية وحتى الهجوم، قانونيا، قانونيا: تطوير منظومة قانونية وطنيا وإقليميا ودوليا تتلاءم مع التهديدات السيبرانية الجديدة وتراعي خصوصية الفضاء السيبراني

النتائج والتوصيات:

- تواجه الولايات المتحدة الأمريكية رغم كونها أقوى الدول السيبرانية تهديدات حادة ومنافسة شرسة في الفضاء السيبراني وهو ما يهدد امنها القومي ويعيق أدوارها في الفضاء العالمي

- تعمل الولايات المتحدة الأمريكية من خلال هيئات ووكالات متنوعة وبالاستناد إلى جملة من التشريعات على مواجهة تحديات الأمن السيبراني عبر التعاون الدولي وتوحيد الرؤية المستقبلية من أجل فضاء سيبراني آمن يساهم في التقدم والنمو

- ارتباط الأمن السيبراني بقضايا التنمية بأبعادها المتعددة يستدعي ضرورة إدماجه في العقيدة الأمنية للدولة الوطنية وصياغة استراتيجية سيبرانية واضحة المعالم

- بناء وتحديث التشريعات التي تؤطر الفضاء السيبراني خصوصا قوانين مواجهة الجرائم السيبرانية والإرهاب السيبراني

- خلق أطر مؤسساتية للأمن السيبراني وإنشاء جيوش سيبرانية

- تعزيز التعاون الإقليمي والشراكات الدولية الرشيدة بين كافة الفاعلين من أجل ترسيخ قواعد السلوك الفعال ونشر قيم وثقافة الفضاء السيبراني السلمي

الهوامش:

[1] Ney, Joseph, S. (2010). Cyber power, Harvard Kennedy School, p04.

[2] Ney, Joseph, S. (2011). Power and national security in cyberspace America's cyber future, center for a new America security, volume 2, p 16.

[3] Ney, Joseph, S. (2011). Power and national security in cyberspace America's cyber future, center for a new America security, volume 2, p 16.

[4] خليفة، إيهاب. (2019). مجتمع ما بعد المعلومات: تأثير القوة الصناعية الرابعة على الأمن القومي، القاهرة: العربي للنشر والتوزيع، ص 125.

[5] Lord, M Kristin. and Sharp, Travis. (2011), America's cyber future, Center for a new America security, Vol 1, p 18.

[6] عبد الصادق، عادل. (أبريل 2017). أنماط الحرب السيبرانية وتداعياتها على الامن العالمي. مجلة السياسة الدولية، العدد 208، ص ص 34، 35.

[7] عبد الصادق، عادل. (أبريل 2017). أنماط الحرب السيبرانية وتداعياتها على الامن العالمي. مجلة السياسة الدولية، العدد 208، ص ص 34، 35

[8] Siboni, Gabi and Kronenfeld, Sami. (December 2012), Iran and Cyberspace Warfare, **Military and Strategic Affairs**, Volume 4, No.3, pp 15- 18.

[9] (http://www.washingtoninstitute.org).

[10] عبد الصادق، عادل. (أبريل 2017). أنماط الحرب السيبرانية وتداعياتها على الامن العالمي. مجلة السياسة الدولية، العدد 208، ص ص 34، 35.

[11] [11] Lumetal, Thomas. (2012), China Internet Freedom and US Policy, Congressional Research Service, pp 8,9.

[12] Lumetal, Thomas. (2012), China Internet Freedom and US Policy, Congressional Research Service, pp 8,9.

[13] Lumetal, Thomas. (2012), China Internet Freedom and US Policy, Congressional Research Service, pp 8,9.

[14] لوديرميلك، ميكا. (2018)، الأزمة الإيرانية تنتقل إلى الفضاء السيبراني. على الرابط:
http://www.washingtoninstitute.org/ar/policy-analysis/view/iran-crisis-moves-into-cyberspace