استراتيجية الولايات المتحدة الامريكية للأمن السيبراني

م.م يونس مؤيد يونس مصطفى(*)

الملخص

ادت التدفقات الضخمة واللحظية للمعلومات عبر شبكات الانترنيت الدولية في ظل النظام الدولي الجديد في اطار العولمة وتصاعد العامل التكنولوجي كعنصر من عناصر قوة الوحدات الدولية– الدول وما دون الدول– الى تصاعد سرعة التفاعلات بين الفاعلين على المستويين الاقليمي والدولي والى انعكاس خطير على مفاهيم الامن القومي للدول التي لم تعد بعض هذه الدول قادرة على السيطرة على حركة التهديدات السيبرانية التي تتعرض لها، لذلك تسعى الولايات المتحدة الامريكية كونها الدولة المهيمنة على النظام الدولي وامنها القومي هو مرتبط بالأمن العالمي وكون اي اخراق تتعرض له يمس مكانتها الدولية الى التراجع في ظل وجود قوى دولية تعمل باستمرار من اجل تهديد المصالح الاستراتيجية القومية العليا لها الى تبني استراتيجية قومية لمحاولة منع أو التخفيف من هذه المخاطر نظراً لارتباطها الشديد بالأمن العالمي، والاعتماد الكثيف على أنظمة شبكات تتوافق مع الأمن القومي، وهو ما يتطلب استمرارية اتخاذ إجراءات وقائية من أجل جعل المخاطر المترتبة على الفضاء الإلكتروني في حدّها الأدنى.

Abstract

The massive and simultaneous flow of information through international Internet networks under the new international order within the framework of globalization and the rise of the technological factor as a component of the strength of international units - States and States - led to a rapid acceleration of interactions

(*)كلية العلوم السياسية / جامعة الموصل.

between actors at the regional and international levels. That some of these countries are no longer able to control the movement of cyber threats to them, so the United States seeks to be the United States as the dominant state of the international system and its national security is linked to global security and the fact that any penetration exposed to touch Mecca The international community has to retreat in the presence of international forces working continuously to threaten their national strategic interests to adopt a national strategy to try to prevent or mitigate these risks because of their strong connection to global security and the heavy dependence on network systems compatible with national security, Take preventive action in order to minimize the risks posed by cyberspace.

المقدمة

يعد موضوع التهديدات السيبرانية واثرها على الامن القومي للدول من الموضوعات التي تحظى بأهمية في مجال الدراسات الدولية والاستراتيجية لانه ذات اثر مباشر على المصالح القومية العليا للدول التي تخترق من قبل الوحدات الدولية او غيرها من الجماعات التي اصبح لها تاثير كبير على مسرح الاحداث الجيوستراتيجية مايهدد كيان الدولة المخترقة وامنها القومي، فشهد الامن الدولي العديد من التحديات العالمية التي لم تكن منظورة لدى صُناع القرار في العالم، وأصبحت حقيقة واقعة يجب التعامل معها بمنظومة علمية عالمية ووفق خطط مُنظَمة ذات نتائج محددة وفعالة. هذه التحديات العالمية وبما تحتويه من متغيرات متعددة ومترابطة مع بعضها أصبحت تُهدد الانسانية، لا بل الكون كله. تكمن دلالة تحديات الامن الدولي في إنها أكبر من قُدرة الدول فُرادى على مواجهتها، فهي تحديات تتجاوز حدود الدولة ذات السيادة، وذات مؤثرات تُهدد مستقبل العالم.

اهمية الدراسة

لقد تغيّر العالم مع بداية القرن الواحد والعشرين تغيراً يكاد يُعيد تشكيل خريطة النظام الدولي، في ظل صعو فاعلين من غير الدول ما اصبح النظام الدولي متعدد القوة وليس متعدد الاقطاب كما يطلق عليه بعض الباحثين، وهو الامر الذي جعل الشعوب تُدرك

بانها لأول مرة في التاريخ تعيش عالماً جديداً بحيث لا يستطيع الانسان التفكير فيه واتخاذ القرارات المناسبة، وكأنه فقد قدرته على التحكم في توازنه، وهو ماتتعرض له الولايات المتحدة الامريكية من اختراقات بين الفينة والاخرى من جماعات ارهابية او وحدات دولية – دول – التي تريد للولايات المتحدة الامريكية الانكشاف الاستراتيجي واختراق لامنها القومي كونها الدولة القائدة للنظام الدولي بعد تفكك الاتحاد السوفيتي وسيطرتها على التفاعلات الاستراتيجية الاقليمية والدولية، لذلك جهدت الادارات الامريكية المتعاقبة على ترصين الامن القومي لها من خلال بناء استراتيجيات فعالة لردع تهديدات الامن القومي الفضائية السيبرانية من خلال وثائق الامن القومي التي تصدر عنها لمعاجلة كيفية ردع تلك التهديدات.

اشكالية الدراسة

ما حدث في عالمنا اليوم من ثورة في الاتصالات والمعلومات، وضعت بصماتها على ما سمي لاحقا بعصر العولمة، أسهمت بقوة في تغيير وشائج عدة وأقنعت العالم بالرضوخ إلى ما نتج عن هذه الثورة العلمية الهائلة، ثم فتحت أمام جميع الأطراف جبهات للصراع لا تقل خطورة عن الصراعات العسكرية والاقتصادية والدبلوماسية، بل إنها تتفوق عليها في تحطيم قوة العدو في معظم الأحيان، لأنها تمس مجالات امنها القومي، بعد أن أصبحت المعلومة وفاعلية الاتصال وسعة قنوات المعرفة أسلحة جديدة يمكن أن تحسم النزاع لصالح من يجيدها ويسيطر عليها وهي التهديدات الفضائية السيبرانية، فتتمثل الاشكالية في بحث ودراسة كيفية استجابة الولايات المتحدة الامريكية وضرورة المراجعة المستمرة لوثائقها القومية بعد ظهور تهديدات غير منظورة التي كانت معروفة سابقا بتهديد الدول عن طريق زيادة قوتها المادية العسكرية والاقتصادية بل ظهر تهديد غير مرئي يهدد الامن القومي للولايات المتحدة الامريكية والاضرار بالمصالح القومية العليا والبنى التحتية وتزايد العمليات الفضائية الارهابية من قرصنة وتجسس لان تهديد الدولة الاولى في النظام الدولي ينعكس على الانفلات

الامن العالمي. مايجعل الولايات المتحدة ان تكون على اهبة الاستعداد دائما لمواجهة أي خرق لامنها الفضائي السيبراني.

فرضية الدراسة

تنطلق الدراسة من فرضية مفادها ان التهديدات الفضائية السيبرانية تؤثر بشكل مباشر وحيوي الامن القومي للولايات المتحدة الامريكية بما توفره تلك التهديدات من خطر على ارواح المواطنين الامريكية من حيث التهديدات بالقتل او الخسائر المادية الاقتصادية التي تتعرض لها في حالة الشركات الامريكية او الانكشاف الاستراتيجي للولايات المتحدة في حالة وصول هذه التهديدات الفضائية السيبرانية الى مبتغاها، لذلك تعمل الولايات المتحدة الامريكية عل صون امنها القومي من خلال الخطط الكفيلة لمعالجة تلك الاختراقات، ومن اجل اثبات الفرضية فقد عمدت الدراسة الى تبني عدد من التساؤلات، والسعي للاجابه عنها، واهم هذه التساؤلات هي :

- ماهو مفهوم الفضاء الالكتروني السيبراني؟
- ماعلاقة الامن الفضائي السيبراني بالامن القومي؟
- ماالتهديدات الفضائية السيبرانية للامن القومي الامريكي؟
- ماستراتيجية الولايات المتحدة الامريكية للامن الفضائي السيبراني؟

منهجية الدراسة

من اجل الاجابة عن التساؤلات التي تتبناها الدراسة تم الاعتماد على مناهج علمية سبيلا لاثبات الفرضية، فقد تم الاعتماد على المنهج الوصفي والتاريخي والتحليلي، لدراسة استاتيجية الولايات المتحدة الامريكية للامن الفضائي السيبراني لصون امنها القومي.

هيكلية الدراسة

بناءً على تحديد اهمية الدراسة والاشكالية والفرضية فقد توزعت الهيكلية الى اربعة محاور ومقدمة وخاتمة، فقد تضمن المحور الاول دراسة مفهوم الفضاء السيبراني،

وخص المحور الثاني علاقة الامن الفضائي السيبراني بالامن القومي، وتناول المحور الثالث التهديدات الفضائية السيبرانية التي تتعرض لها الولايات المتحدة الامريكية، اما المحور الرابع درس استراتيجية الولايات المتحدة الامريكية للامن الفضائي السيبراني.

المحور الاول: مفهوم الفضاء السيبراني

يعد الفضاء الالكتروني هو السمة التي تميزت بها الحياة العصرية والمكون الأساسي للبنية التحتية لمؤسسات الدولة المختلفة القطاعين العام والخاص واصبح منبراً للتعبير عن الحرية والتجمع والخصوصية الفردية والتدفق الحر للمعلومات والاتصالات الالكترونية ومعالجة البيانات ذات الطابع الشخصي والجرائم والمعاملات والتواقيع والإثبات والتجارة الإلكترونية وحماية المستهلك وحقوق الملكية الفكرية في المجال المعلوماتي السيبيري والأسس الضرورية للفرص والنمو التي بدورها تدفع الى قطاع عالمي مزدهر ، وتحولت الساحة الإلكترونية العالمية إلى أرض معارك حقيقيةً، في عالمٍ افتراضي وتقني يعتمد على كل ما هو جديد من صيحات التكنولوجيا الرقمية والاتصالية الحديثة. وتعددت أشكال هذه الحروب ما بين الفردية والجماعية، والدولية والمؤسساتية، والسياسية والاقتصادية والاجتماعية، والمتهمة بالإرهاب، وتلك المشرعنة الجانحة نحو المقاومة، وغيرها من ألوان الحروب الدائرة عبر الفضاء الإلكتروني، والبعيدةِ تقريباً عن أنظار ومسامع البشرية.

تذكر المراجع العلمية بأن عالم الرياضيات نوربرت وينر((Norbert wiener هو أول من استخدم مصطلح السيبرانية ويذلك في عام 1948". أثناء دراسته لموضوع القيادة والسيطرة وبالاتصال في عالم الحيوان، فضلا عن حقل الهندسة الميكانيكية.

وبالرجوع إلى قواميس اللغة، فلم تشر في الغالب إلى مصدر كلمة سايبر ((Cyber سوى وفقاً لما وجدناه في قاموس المورد فيعرفها السيبرانية هي علم الضبط،(Cybernetics) وهو مصدر يتطابق مع مفهوم الهجمات السيبرانية، أي ضبط الاشياء عن بعد والسيطرة عليها. وبما يؤكد ما طرح سلفا، إن معظم القواميس المتخصصة في المصطلحات العسكرية، لم ترجع كلمة سايبر إلى مصدرها، بل عرفتها

في نطاق استخدامها الفعلي أي العسكري، كقاموس المصطلحات العسكرية الامريكية فيعرفها أي فعل يستخدم عن طريق شبكات الكترونية بهدف السيطرة أو التعطيل لبرامج الكترونية أخرى[1].

أما كلمة سيبيرية أو سايبورغ فهي كلمة بدأ استخدامها عام 1960 والتي اطلقها مانفريد كلاينس وناثان كلاين في مقال لهما ويعني المصطلح: المزج بين الاليكترونيات والأنسان[2].

ويظل التطور الحاصل بتكنولوجيا الحديثة والاتصال والانتشار الكبير للشبكات الالكترونية والسرعة التي توفرها جعل منها موردا مهما للعديد من الدول في بناء منظوماتها المالية والحكومية والعسكرية وبناء مجتمعاتها المعلوماتية، فقدرت الزيادة الحاصلة في استخدام الانترنت بحوالي 360 مليون نسمة لعام 2000 الى حوالي 2 مليار نسمة لعام 2010 والزيادة المتوقعة في ظل الانتشار الذي يشهده الفضاء الالكتروني وتشعبه في نسيج الحياة[3].

يعتمد الفضاء الالكتروني السيبراني كمجال افتراضي على نظم الكمبيوتر وشبكات الإنترنت ومخزون هائل من البيانات والمعلومات، بحيث يتم الاتصال بالشبكات عبر الحواسيب أو الهواتف أو غيرها من دون تقيد بالحدود الجغرافية. وقد ظهر مصطلح الفضاء الالكتروني السيبراني في ثمانينيات القرن العشرين في إحدى روايات الخيال العلمي للكاتب الأمريكي– الكندي ويليام جيبسون ويوصف العصر الحالي بأنه العصر الرقمي فهو يتضمن تطورات تكنولوجية هائلة تخدم جميع مناحي الحياة العامة والخاصة، وتنعكس على خدمة المجتمع الدولي بأكمله، حيث بات هذا العصر يتحرك من خلال تكنولوجيا المعلومات والاتصالات، التي واكبتها حركة إجرامية كبيرة، فانتشرت التهديدات الفضائية بشكل خطير في جميع دول العالم التي أصبحت عرضة للوقوع تحت تهديد هذه الجرائم باستخدام الفيروسات وبرامج التجسس وغيرها، وهي أدوات يمكن وصفها بالجراثيم المستحدثة او المخلقة[4].

والفضاء الالكتروني السيبراني مرتبط بالمعلومات فهذا يؤدي الى حدوث حروب تستخدم تكنولوجيا المعلومات كأداة تمد أطراف الصراع بوسائل غير مسبوقة من حيث

القوة والسرعة والدقة في تنفيذ العمليات العسكرية وتستهدف اشياء لا علاقة لها بالمعلومات، ولعل مصطلح الحرب المعلوماتية أقرب الى الحروب الالكترونية الحديثة[5].

وعرف جوزيف ناي الفضاء الالكتروني نطاق تشغيلي محكم باستخدام الالكترونيات لاستكشاف المعلومات عبر انظمة مترابطة ببعضها البعض وبنية تحتيه لها، وعرفته جامعة الدفاع الوطني الامريكية بانه مجال تشغيلي تجري فيه مجموعة من العمليات ذات الطابع الالكتروني الفريد والمحكم بمجموعة من الاستخدامات التي تعتمد على الالكترونيات والاطياف الكهرومغناطيسية لإنشاء وتخزين وابدال وتبادل واستغلال المعلومات من خلال مجموعة من نظم المعلومات المترابطة والمتصلة عبر الانترنيت والبنى التحتية الخاصة[6].

ويرتبط بالمفهوم السابق مفهوم اخر يطلق عليه الحرب الإلكترونية السيبيرية، يهاجم القراصنة الملفات والمواقع وغيرها التي تخص الاخرين وبذات الوقت يدافع الناس عن معلوماتهم من القراصنة عن طريق برامج وطرق متعددة[7].

وتعرف ايضا جزءً من العمليات التي يمكن ان يتم استخدمها في مستويات ومراحل الصراع المختلفة سواء اكان ذلك في الجانب التكتيكي ام العملياتي ام الاستراتيجي واستخدام تلك الهجمات في أي وقت سواء اكان في السلم ام الحرب ام الازمة[8].

فضلا عن التعريف الذي قدمه دانيال كويل عام 2009 القدرة على استخدام الفضاء السيبراني لخلق مزايا والتأثير على الأحداث في جميع البيئات العملياتية وعبر أدوات القوة، ويقصد بالبيئات العملياتية المجالات الخمسة للقوة وهي، البرية، البحرية، الجوية، الفضائية، والفضاء السيبراني، بينما يقصد بأدوات القوة الأبعاد الأربعة للقوة وهي، الدبلوماسية، المعلومات، الجيش، والاقتصاد، ويعد القوة السيبرانية أحد الأبعاد المهمة للجيوبوليتكس أمرا طبيعيا ولا مفر منه، تماما مثل المجالات الاستراتيجية الأخرى، فرغم أن تأثير القوة السيبرانية يبقى الأقل ملموسية ووضوحا مقارنة بتأثير غيرها من أشكال القوة، كالقوة الجوية والبرية مثلا، إلا أنه في الوقت نفسه لا يمكن عد ذلك أمرا يقلل من أهميتها في الأمن الفضائي السيبراني وفي مجال النظريات الإستراتيجية؛

لأن انتشار القوة الفضائية السيبرانية لا يمكن أن تلاحظ بشكل مباشر كون الأجهزة التي تولد نقل وتلقي المعلومات المتداولة، موجودة ماديا في كل مكان، كما أن المستفيدين المباشرين والذين قد يكونون ضحايا في بعض الحالات– هم أيضا متواجدون في كل مكان[9].

ويتعلق مفهوم الحروب الالكترونية (السيبرانية) بالتطبيقات العسكرية وتعني قيام دولة او فواعل من غير الدول بشن هجوم الكتروني في اطار متبادل، او من قبل طرف واحد، وبرغم ذيوع مسمى الحرب الالكترونية (السيبرانية) اعلاميا، فانه يعد مصطلحا قديما كان بالاساس مقصوراً على رصد حالات التشويش على انظمة الاتصال والرادار واجهزة الانذار بينما يكشف الواقع الراهن في الفضاء الالكتروني (السيبراني) عن دخول شبكات لاتصال والمعلومات الى بنية ومجال الاستخدامات الحربية[10].

وتُعرف الحرب الإلكترونية بأنها حربٍ تخيليةٍ أو افتراضية ذات طبيعةٍ غير ملموسة، تُحاكي الواقع بشكلٍ شبه تام. وهي حرب بلا دماء، فتتلخص أدوات الصراع فيها بالمواجهات الإلكترونية، والبرمجيات التّقنية، وجنود من برامج التخريب المحوسبة، وطلقاتٍ من لوحات المفاتيح ونقرات المبرمجين في بيئةٍ استراتيجية اصطناعيةٍ تُحاول _ما أمكن_ الوصول إلى صورةٍ حقيقيةٍ لملامح الحياة المادية والملموسة.

فالتهديدات الفضائية السيبرانية ستكون المشهد الصراعي المستقبلي في البيئات الاستراتيجية الاقليمية والدولية على مستوى التنافس والتماس القوة من قبل القوى المسيطرة في النظام الدولي والقوى الاقليمية الساعية الى ايجاد مكان لها في البيئة الاستراتيجية، ولكن بصورةٍ رقميةٍ وتكنولوجية، وهي صراعاتٌ قديمةٌ جديدةٌ، بدأت منذ الوقت الذي ابتكر فيه الإنسان أدوات تواصله الأولى، كالأصوات، والتخابر، والتلغراف، والهواتف السلكية، وأنظمة البرق الصوتية، وأنظمة الترميز، وآلات الطباعة وغيرها، والتي تم استخدامها في الحربين العالميتين الأولى والثانية، وما سبقهما من حروبٍ وثوراتٍ وقعت في عقدي الثورة الفكرية والصناعية[11].

ويُشير مصطلح التهديدات الإلكترونيّة إلى استخدام جُملة من الممارسات والإجراءات التي تسعى لإلحاق الخلل والعطل بالأنظمة والوسائل الإلكترونية الخاصة بالعدو،

بالإضافة إلى تحقيق الحماية للذَّات من الاستطلاع الإلكتروني المعادي ومقاومته، وتحقيق الاستقرار للنُّظم الإلكترونيّة الصديقة، ويعتبر استخدام الطاقة الكهرومغناطيسيّة في نطاق الحرب الإلكترونيّة ضرورياً؛ وذلك لغايات تعطيل حركة العدو، ومنعها من استغلال المجال الكهرومغناطيسي الصديق. إن الحرب الإلكترونيّة تتّخذ من شبكة الإنترنت حلبَة صراع لها، وتأتي الهجمات التي تُشّن فيها بسبب دوافع سياسيّة، وتُوجَّه الضربات الإلكترونيّة على مواقع الإنترنت الرسميّة للعدو، وكل ما يتعلق بشبكاته وخدماته الأساسيّة، وتكون الضربات بقرصنة وتعطيل المواقع، وسرقة البيانات السريّة وتخريبها، واختراق الأنظمة الماليّة[12].

وهناك من يفضل ان يستخدم تعبير الحروب الالكترونية (السيبرانية) او التهديدات الالكترونية جامعة كل مايدور في الفضاء الالكتروني من عمليات تجسس وارهاب وقرصنة بدلالة الحرب تعبيرا عن حالة التوجه الجديد، ولكن تبقي كلمة الحرب هي الأخرى محل جدل وبخاصة ان هناك العديد من المسميات التي تطلق على تلك الانشطة العدائية عبر الفضاء الالكتروني. وهو ما يدفع الى اعادة النظر في اطلاق مسمى الحرب على تلك الانشطة العدائية ،وذلك يرجع الى ان مفهوم الحرب "تقليديا" يرتكز بالأساس علي استخدام الجيوش النظامية، وكان يسبقها إعلان واضح لحالة الحرب وميدان قتال محدد. أما في هجمات الفضاء الإلكتروني، فإنها غير محددة المجال أو الأهداف، كونها تتحرك عبر شبكات المعلومات والاتصال المتعدية للحدود الدولية أو اعتمادها علي أسلحة إلكترونية جديدة تلائم السياق التكنولوجي لعصر المعلومات، والتي يتم توجيهها ضد المنشآت الحيوية أو دسها عن طريق العملاء لأجهزة الاستخبارات[13].

وتعني حرب المعلومات استخدام المعلومات ونظمها في العدوان والدفاع المعلوماتي؛ لاستخدام المعلومات ونظمها او تخريبها او تدميرها لدى الخصم، والمحافظة على المعلومات ونظمها سليمة، وتهدف هذه الاعمال الى تحقيق تقدم على جيش العدو واعماله الاخرى الداعمة للمجهود الحربي، وهي تمثل صراعا للحصول على المعلومات والسيطرة عليها، وهذا الصراع يحدث على مستويات ثلاثة هي[14]:

1-الصراع الفكري للخصم ويشمل الاليات النفسية والاعلامية والعسكرية والدبلوماسية المؤثرة في عقل الخصم سواء اكان قائداً عسكريا ام مجتمعا بأكمله.

2-السيطرة المعلوماتية وتشمل السيطرة على الشؤون الصراع المادي.

3-الدفاع عن التدقيق المعلوماتي، ويشمل التصدي للهجوم على أي بناء معلوماتي عسكري او مدني بما في ذلك مواجهة الدخلاء والمتطفلين والتدمير المادي للابنية المعلوماتية والخداع والعمليات النفسية.

فعَّد الفضاء السيبراني بانه يمثل البعد الخامس للحرب من حيث تشابكية العالم الافتراضي مع العالم المادي في ظل علاقة تاثيرية متبادلة قائم على نظرة تكاملية ووصف بانه الذراع الرابع لقوات الدولة الاستراتيجية البرية والجوية والبحرية[15].

اختصر الفضاء الالكتروني حاجز المكان والزمان وخلق مساحات للتفاعلات الداخلية والخارجية في الواقع الافتراضي بين الفاعلين الدوليين سواء اكانوا دول ام غير الدول نتيجة امتلاكه سمات عدة هي[16]:

1- ساحة صراع افتراضية بين الدول ويشارك فيها المدنيين والعسكريين وترتبط بالتطورات المادية والعسكرية على الارض واقل تكلفة واكثر تحديداً للهدف.

2- زيادة الاعتماد الالكتروني فباتت الدول الحديثة تربط بنيتها التحتية بشبكة المعلومات الدولية لاسيما الكهرباء والماء والبنوك وسوق الاسهم المالية والاتصالات وانظمة السيطرة العسكرية وجمع المعلومات كالأقمار الصناعية والطيارات بدون طيار.

3- تماهي حدود الداخل والخارج أي وجود حالة من التأثير الشبكي المتزايد داخل الدول وخارجها من حيث استخدام الافراد والجماعات والدول للتكنولوجيا سواء اكانت مواقع التواصل الاجتماعية ام الهواتف اللوحية ام مواقع عامة للتعاملات المالية والتجارية.

4- صعوبة الردع الالكتروني على عد الفضاء الالكتروني (السيبراني) ساحة هلامية افتراضية يصعب على الدول وضع الحدود لسيادتها وسيطرتها كما لو ان الدول في الوقت الراهن وفي ظل الفضاء الالكتروني (السيبراني) فاقدة لركن من اركان قيامها،

فيغيب الردع في ظل التنكر على شبكة المعلومات الدولية مادى الى مجهولية مصدر الهجمات الالكترونية وزيادة خبرة المهاجمين.

5- غياب الشفافية الدولية من حيث عدم القدرة على معرفة هوية المهاجمين على الامن القومي نشب معضلة غياب الشفافية والقوانين المقيدة للصراعات في المجال الالكتروني (السيبراني).

المحور الثاني: مفهوم الامن الفضائي (السيبراني) وعلاقته بالأمن القومي

اهم مايسعى اليه واضعو وثائق الامن القومي والسياسات الدفاعية للدول هو حماية مصالح الدولة داخل البيئة الاستراتيجية التي تم تعريفها وفق كلية الحرب الامريكية بانها نظام عالمي حافل بتهديدات واسعة ومثيرة للشكوك والصراع متاصل فيها وغير قابلة للتنبؤ وتكون القدرات الوطنية للدفاع عن المصالح القومية العليا للدولة مقيدة بقيود مرتبطة بحجم الموارد البشرية والمادية وهي متسمة بسمات التقلب والتوجس والتعقيد والغموض[17].

تم تعريف الامن وفق الباحث السياسي باري بوزان العمل على التحرر من التهديد. وفي سياق النظام الدولي فهو قدرة الدول والمجتمعات على الحفاظ على كيانها المستقل وتماسكها الوظيفي ضد قوى التغيير التي تعدها معادية في سعيها للأمن. فأساس الامن هو البقاء لكنه يحوي على جملة من الاهتمامات الجوهرية حول شروط الوجود ولايعني العمل على التحرر من التهديدات تحييده كلياً لان الامن يكون نسبياً ولا يمكن ان يكون مطلقاً[18].

وللأمن بصورة عامة مستويات عدة منها الامن القومي الذي يعرف وفق المنهج الحديث بانه مفهوم شامل يتعلق بالدولة بكافة الأبعاد السياسية والاقتصادية والاجتماعية وغيرها من الأبعاد، ويذهب إلى أن مجموعة التهديدات الموجهة ضد الدولة لا تنشأ من مصادر خارجية فحسب وإنما من المصادر الداخلية والعابرة على الأغلب لحدود الدول، ويضع مجموعة بدائل غير عسكرية، ذات التأثير الشامل مثل (الشرعية السياسية، التعايش الديني والقومي، والقدرات الاقتصادية وتوفر الموارد الأولية

الأساسية، فضلا عن البدائل العسكرية والتي تشكل احد المتطلبات الضرورية للأمن على مستوى الدولة[19].

يعد الامن الركيزة الاساسية للمجتمع، بحيث لا يمكن تصور نمو اي نشاط بعيدا عن تحققه، سواء اكان ذلك، على المستوى التقني، ام على المستوى القانوني. وقد تحول الامن، مع بروز مجتمع المعلومات، والفضاء السيبراني، الى واحد من قطاع الخدمات، التي تشكل قيمة مضافة، ودعامة اساسية، لأنشطة الحكومات والافراد على السواء، كما هو الحال مع التطبيقات الخاصة بالحكومة الالكترونية، والصحة الالكترونية، والتعليم عن بعد، والاستعلام، والتجارة الالكترونية، وغيرها الكثير. الا ان الوجوه المتعددة للامن السيبراني، ومضاعفاتها الخطيرة التي لا تقف عند حدود الاساءة الى الافراد، والمؤسسات، بل تتعداها الى تعريض سلامة الدول والحكومات، وتزيد مهمة القيمين على الموضوع تعقيدا وصعوبة، وتستدعي مقاربة، شاملة، ومتكاملة، لجميع التحديات، التي يطرحها الفضاء (السيبراني)، بحيث تأتي الردود، والحلول المقترحة، ناجعة وفاعلة. فتحقيق الامن، وبناء الثقة في الفضاء السيبيري، من أساسيات تسخير تقنيات المعلومات والاتصالات، في مجالات التنمية خدمة للمجتمعات الانسانية[20].

فالامن الفضائي السيبراني هي اجراء من دولة ضد دولة اخرى بما يعادل الاستراتيجية الهجومية او الدفاعية اوم استخدام القوة في الفضاء الالكتروني قد يؤدي بنتائج ردية مقاربة للفعل الاصلي على المستوى الالكتروني العملياتي ليكون متفوقا على التهديدات الفضائية المتأتية من الدول الاخرى[21]

شاع استخدام مصطلح أمن المعلومات عصرنا الحالي، ليحدث ثورةً أمنيةً في عالم الاتصالات الحديثة، واختلافاً ملحوظاً في الأدبيات التي تناولت تفسير هذا المفهوم. وفي هذا الشأن؛ يؤكد الاختصاصي القانوني في دراسة المعاملات الإلكترونية وأمن المعلومات خالد إبراهيم على أنه ولمعرفة المقصود من الامن الفضائي السيبراني؛ يقتضي تناوله في ثلاثة زوايا مختلفة، وهي[22]:

1- الزاوية الأكاديمية: يقصد بأمن المعلومات الإلكترونية من هذه الزاوية، العلم الذي يبحث في نظريات واستراتيجيات ووسائل حماية المعلومات من المخاطر

والأخطار التي تُهددها، وحمايتها أيضاَ من أية أنشطةٍ اعتدائيةٍ ضارةً قد تؤثر على فحواها وجوهرها.

2- الزاوية التّقنية: تُشير هذه الزاوية إلى الإجراءات والأدوات التكنولوجية الواجب توافرها لضمان حماية المعلومات من التهديدات الداخلية والخارجية؛

3- الزاوية القانونية: تتناول هذه الزاوية الدراسات والتدابير الحمائية والسرية اللازمة لتوفير الغطاء الأمني والقانوني للمعلومات، ومكافحة أية أنشطةٍ تهدف لاستغلالها أو تنظيمها لارتكاب الجرائم بحق مالكيها، وسن التشريعات القانونية الهادفة لحمايتها من الأنشطة غير المشروعة، والتي قد تُهدد سلامة صحتها البيانية والقانونية.

فيتضمن البعد المعلوماتي للأمن مدى جديد وأوسع لحماية المصالح الحيوية والإستراتيجية للمجتمع والدولة، فكثير من الدول توصفه مكوناً أمنياً وطنياً يؤثر بصورة مباشرة على مصالح ونشاطات المجتمع والدولة، بل أنّ الكلام عن الأمن القومي لا يجدي نفعاً إذا لم يكن هنالك أمن معلوماتي، فهو يرتبط بالأمن المالي والسياسي والإقتصادي والعسكري للبلد، إذ يُعرف بأنه حصيلة مجموعة أنشطة تتكاتف لتنفيذها مجموعة من المؤسسات المختلفة لاسيما الأمنية والعسكرية منها لتحقيق كفاية معلوماتية أمنية وطنية، ضد الثغرات والاختراقات المعلوماتية التي تسببها تحديات إستخدامات ثورة تكنولوجيا المعلومات والإتصالات على شكل (أسلحة معلوماتية) في تدمير وإنهاك وسرقة المصادر المعلوماتية وأنظمة الطاقة والإتصالات والحاسوب وغيرها من التحديات التي تدخل في إطار حرب المعلومات، أو الإرهاب المعلوماتي الذي يتضمن إستخدام مجموعات من الأفراد لتكنولوجيا السيطرة المعلوماتية وشبكات الإتصال والإنترنيت لكسر دخول أنظمة الحماية الوطنية والحواسيب الخاصة بأقسام الوزارات العسكرية والمالية والإقتصادية، وتدمير البنى التحتية التكنولوجية للدولة والمجتمع[23].

فالأمن السيبيري هو مجموع الأدوات والسياسات ومفاهيم الأمن وضوابط الأمن والمبادئ التوجيهية ونهج إدارة المخاطر والإجراءات والتدريب وأفضل الممارسات وآليات الضمان والتكنولوجيات التي يمكن استخدامها في حماية البيئة السيبيري ة

وأصول المؤسسات والمستعملين. وتشمل أصول المؤسسات والمستعملين أجهزة الحوسبة الموصولة بالشبكة والموظفين والبنية التحتية والتطبيقات والخدمات وأنظمة الاتصالات ومجموع المعلومات المنقولة و/أو المحفوظة في البيئة السيبيرية، ويسعى الأمن السيبيري إلى تحقيق خصائص أمن أصول المؤسسات والمستعملين والحفاظ عليها وحمايتها من المخاطر الأمنية ذات الصلة في البيئة السيبيرية[24].

فالامن الفضائي السيبراني هو مجموع القواعد التي يضعها مسؤولو الامن في اي مكان والتي يجب ان يتقيد بها جميع الاشخاص الذين يمكنهم الوصول اليه فمفهوم الامن مفهوم واسع يطال جميع عمليات الدخول والخروج والبقاء او التصرف في مكان ما وعليه يشمل الامن في الفضاء السيبيري قواعد واصول ضبط الاتصال وانتقال المعلومات وتخزينها وحفظها كما يشمل أمن المواقع وامن الانظمة الالكترونية وعمليات استثمارها إضافة إلى امن الاتصالات

وتبدو العلاقة واضحة بين الأمن الفضائي السيبراني والامن القومي لضمان حقوق الوصول الى البيانات والى مصادر النظام وذلك عبر آلية تحقق من الهوية ورقابة تسمح بحصر مستخدمي النظام ضمن مجموعة الاشخاص الذين اعطي لهم هذا الحق، فالأمن في الفضاء السيبيري ليس الا مكونا من مكونات الامن في المجتمع بشكل عام وهو الركيزة الأساسية لتحقيق الثقة في نمو وازدهار مجتمع المعلومات. وفي اشارات واضحة الى أهمية الامن في الفضاء السيبيري برزت دعوات في الولايات المتحدة الاميركية الى اسناد مهمة الدفاع عن الفضاء السيبيري الوطني الى الوكالة الوطنية للامن[25].

أما الباحث حسن طاهر عرف الامن الفضائي السيبراني: العمليات التي تؤمن حماية كافة الموارد والآليات المستخدمة والمتبعة في معالجة المعلومات أمنياً، بحيث يتم تأمين كافة الموارد البشرية وغير البشرية المختصة بجهةٍ معنيةٍ، بوسائل وإجراءاتٍ وعملياتٍ أمنيةٍ وتّقنيةٍ تُوفر لها سلامة محتواها المعلوماتي من أية مخاطر، فالمعلومات هي الكنز الثمين الذي يتوجب على أية دولةٍ في العالم حمايته من أية مخاطر داخليةٍ أو خارجية[26].

يتضح مما سبق، أن لمفهوم الامن الفضائي السيبراني أهميةً بالغةً في حياتنا المعاصرة، نظراً لاعتمادنا الكبير على المعلومات في شتى عملياتنا اليومية، والتي أصبح تتُشكل عصب حياتنا القائمة. إذ أضحت المعلومة سلاحاً ينافس الأسلحة التقليدية وغير التقليدية في عصرنا الحالي، فهي قد تُساهم في تعالي شؤون الدول، أو ربما تؤدي إلى تهاوي دولٍ كثيرةٍ إذا ما تم الكشف عن جوهر معلوماتها الأمنية. لذلك، يمكن القول أن أمن المعلومات الإلكترونية هو عبارة عن محاولة تكثيف الجهود السياسية والاقتصادية والاجتماعية والتكنولوجية الرامية لحماية المحتوى المعلوماتي للأفراد والمؤسسات والحكومات والدول من أية ثغراتٍ داخليةٍ أو خارجية، ويمكن تحديد أبرز الاتجاهات في الأمن الفضائي السيبراني لعام 2017 بالأتي[27]:

1- سنشهد المزيد من عمليات التخلص من البيانات القديمة.

2- ستزيد البرامج الخبيثة أصبحت البرامج الخبيثة (رانسوم) إحدى التهديدات السيبرانية المنتشرة بشكل متزايد خلال السنوات الثلاث الماضية. وحتى وقت ليس ببعيد، كانت معظم هذه البرامج انتهازية وأثرت على مستخدمين أفراد أو أجهزة حواسيب خاصة بشركات صغيرة. كما كانت مطالب هذه البرامج الخبيثة بشكل شائع مساوية لبضع مئات الجنيات ثمن جهاز كمبيوتر شخصي. ومع ذلك، يستهدف مرتكبو الجرائم السيبرانية المؤسسات الكبيرة التي تمتلك ملفات وأنظمة كمبيوتر ذات أهمية بالغة لعملياتهم اليومية وما إلى ذلك، مما يمكنهم من طلب مبالغ فدية أكبر. وفي السنة المقبلة، سترتفع مخاطر البرامج الخبيثة (رانسوم) ويتوجب على المؤسسات أن تزيد مستوى جاهزيتها، وأخذ نسخ احتياطية لأعمالها وتطبيق برامج أكثر تقدمًا يمكنها الكشف عن أي نشاط يشتبه به وإنهائه.

4- تعريف التهديدات الداخلية سيتغير. اذ كانت المؤسسات تعمل بشكل تقليدي على تركيز جهود التخفيف من آثار الاختراقات وعلى الكشف عن التهديدات الخارجية والحد منها – ومع ذلك، فإن معظم اختراقات البيانات التي تحدث في الوقت الحالي تشير إلى تنامي التهديدات الداخلية. وما يتبين من ذلك هو أن التهديدات الداخلية لا تدل على أن الموظفين يسرقون المعلومات أو يقومون بتسريبها بشكل متعمد أو ضار.

كما يوجد هؤلاء الموظفين الذين يصبحون مساعدين بشكل غير متعمد لتهديد خارجي. وسيصبح هذا الأمر تحديًا أكبر للشركات التي ستعمل على تخصيص موارد أكثر لتدريب الموظفين والمقاولين، وتستثمر في أدوات تعمل على تحديد الأنشطة المشبوهة في حال قام أحد الأفراد بفتح رابط خطر بشكل غير مقصود.

5-ستتصدر البنية التحتية الحيوية الوطنية القائمة المفضلة الخاصة بالمخترقين. فقد شهدنا الضربة التي تلقاها القطاع المالي جرّاء الهجمات على نظام سويفت المصرفي وبنك تيسكو التي أعطت مؤشرًا على حجم الضرر الذي يمكن التسبب به وخسارة للأموال في حال استطاع المخترقون تجاوز أنظمة الدفع الأمني التقليدية.

6-ستصبح الاستخبارات الأمنية المعلوماتية أكثر أهمية. وستعمل الشركات على الاستثمار بشكل أكبر في الاستخبارات الأمنية المعلوماتية لاستكمال الأدوات التقليدية. ويتضمن هذا الأمر تطبيق رقابة مستمرة حتى يتم تحديد أو الكشف عن أي اختراق أو نشاط مشبوه والتخفيف من آثاره في أقرب وقت. قبل سنوات عدة، ذكر تقرير غارتنر بأن الوقاية أصبحت أمرًا غير مجدٍ، وأنه بحلول عام 2020 ستكون الاستراتيجيات الأمنية بحاجة إلى تضمين مشاركة الاستخبارات الأمنية.

المحور الثالث: التهديدات الفضائية السيبرانية للأمن القومي الامريكي

ادت الصراعات الدولية حول الموارد والمصالح والقيم القومية العليا للدولة الى زيادة الاعتماد على التكنولوجيا والاتصال والمعلومات فاصبح الفضاء الالكتروني نتيجة ذلك ساحة للصراع بشكله التقليدي ولكن بثوب جديد الكتروني يتجاوز الحدود القومية ويهدد الامن القومي للدول ويسعى الى تحقيق اكبر المكاسب مقابل اكبر قدر ممكن من الخسائر وفق قواعد اللعبة الصفرية بين اطراف الصراع في البيئة الاستراتيجية، وترتكز قوة التصارع بين الدول في هذا الجانب على البنية والاسلحة التكنولوجية وادارة العمليات الالكترونية بما تتضمنه من مهاجمة شبكات الحاسب الالي والدفاع عنه واستطلاع شبكاته وبنية مؤسسية وقانونية وخطة استراتيجية لتوظيف القوة الالكترونية فضلا عن العنصر البشري[28].

اصبحت قضية امن الفضاء الالكتروني (السيبراني) تدخل ضمن استراتيجيات الامن القومي للعديد من الدول؛ للحيلولة دون تعرض بنيتها التحتية الحيوية للخطر الذي ينجم جراء قطع شبكة المعلومات الدولية او توقف رسائل البث الاذاعي او تزوير الانتخابات او التجسس الالكتروني او سرقة الملكية الفكرية للاختراعات او اختراع انظمة الصواريخ العسكرية ادوات مهددة للأمن القومي للدول؛ لانه ترتب على دخول المجتمع الدولي مرحلة جديدة تؤدي هجمات الفضاء الالكتروني السيبرانية التماس جديد للقوة التي تسعى اليها الدول بدلالة التوازن الاستراتيجي لاحقاق اذات الاستراتيجية للدولة وعنصرا حيوياً الى تعظيم القوة او الاستحواذ على عناصرها، واصبح المجال الالكتروني احد المحددات الجديدة للقوة من حيث طبيعتها وانماط استخدامها وطبيعة الفاعلين الدوليين، ويقدم جوزيف ناي مصطلح القوة الالكترونية لتعريف الدور الذي تؤديه في تشكيل قدرة الاطراف الدولية على تحقيق اهدافها؛ لانها تمنح القدرة والقوة وبالوقت نفسه فرضت تحديات كبرى على القوى الكبرى مثل الولايات المتحدة الامريكية التي كان لديها ما يشبه الاحتكار لمصادر القوة كونها القطب الاوحد الذي برز بعد انتهاء الحرب الباردة في البيئة الاستراتيجية العالمية وتحكمها في النظام الدولي وفق مصالحها واهدافها القومية، لكن مع دخول المجال الفضائي (السيبراني) ادى الى انكشاف استراتيجي للدول تحاول بشتى الوسائل الحد من هذا الانكشاف الاستراتيجي والعمل على حماية امنها القومي[29].

واعطت القوة السيبرانية دفعاً رئيساً في اتجاهين هما الاول: تدعيم القوة الناعمة للدول لان الفضاء الالكتروني السيبراني اصبح مسرحا لشن هجمات تخريبية بنشر المعلومات المظللة والحرب النفسية والتأثير في الراي العام والنشاط السري والاستخباراتي، والثاني: تبني الدول زيادة الانفاق في سياسات الدفاع الالكتروني وحماية شبكاتها الوطنية من خطر التهديدات، فتنشط الجماعات الدولية للقرصنة للتعبير عن مواقف سياسية مثل جماعة ويكليكس وانونيموس، والاختراقات المتبادلة بين الولايات المتحدة الامريكية والصين وروسيا الاتحادية، او بين ايران والولايات المتحدة الامريكية وهذا الامر الذي ينعكس على الامن القومي الامريكي الامر الذي يتطلب منها الرد

على مثل هكذا تهديدات لأمنها القومي ضد الخصوم عندما شنت بأسلحة الميكروويف عالية القدرة عبر فايروس ستاكسنت ضد المنشأت النووية الايرانية بالتعاون مع اسرائيل عام 2010 لان امنها القومي يتطلب الحد من القوة الايرانية[30].

بعد احداث الحادي عشر من ايلول عام 2001 بدأ التركيز على الفضاء الالكتروني كتهديد امني من حيث استخدام القوى الاقليمية والدولية والتنظيمات الارهابية لهذا المجال الحيوي قليل الجهد والتكلفة من ناحية تنفيذ الهدف وذات نتيجة هائلة من حيث الاستخدام العملياتي ضد الولايات المتحدة الامريكية[31].

وابرز التهديدات التي توجهها الولايات المتحدة الامريكية في امنها الفضائي (السيبراني) وله انعكاس على امنها القومي هي:

1- التجسس الالكتروني السيبراني يكون من خلال الدخول الى الانظمة الخاصة بالولايات المتحدة الامريكية لاضعافها وضرب مصالحها القومية، واصبح موضوعا مثيرا للنقاش اكثر من أي وقت مضى في جميع انحاء العالم[32]، من قبل الدول التي تريد للولايات المتحدة الامريكية الافول عن مكانتها في النظام الدولي سواء اكانوا دول منافسه مثل روسيا الاتحادية والصين وكوريا الشمالية فيعترض المرتكبون خطوط الاتصالات السلكية واللاسلكية (البريد الإلكتروني أو اتصالات الصوت على الإنترنت) ويتم هذا الأمر لضرب مصالحها القومية العليا، وإما لكشف أمور سرية وفضحها أمام الجمهور، او لبيع المعلومات نظراً لقيمتها التجارية أو لكشف أسرار مالية أو صناعية عن الشركات المنافسة، إو لسرقة كلمات السر للحسابات المصرفية أو البريد الإلكتروني، أو لأسباب سياسية إذا كان موجهاً ضد دولة معينة[33]، قدرت الولايات المتحدة الامريكية خسائرها نتيجة القرصنة عام 2002 8,455 بليون دولار وقدرت وزارة العدل الامريكية ان بحدود 150 الف شخص تاثروا بخسائر تجاوزت 215 مليون دولار، وفي عام 2003 اصدرت لجنة التجارة الفيدرالية الامريكية تقريرا بان هناك 9,9 مليون شخص تعرضوا لهجمات القرصنة والتجسس مع متوسط خسائر 120 مليار دولار امريكي والقضية المتهم فيها 43 مصريا عام 2009 بالسطو على بنك اوف امريكا بولاية كاليفورنيا والاستيلاء على مبلغ حوالي مليون دولار 700 الف

دولار امريكي كل ذلك له اثر على الامن القومي[34]، فخلال العام 2014 بعد هجمات حجب الخدمة 2012–2013، على القطاع المالي اعلن بنك جي بي مورغان عن انفاقه 250 مليون دولار للأمن السيبراني، وتم اختراق شركة هوم ديبوت لبطاقات الائتمان، ومكتب ادارة شؤون الموظفين، هذه التهديدات للأمن القومي تأتي من دول قومية تمتلك برامج حاسوبية متطورة للغاية مثل روسيا الاتحادية التي انشئت قيادتها الالكترونية والصين التي لاتزال تعمل على التجسس الاقتصادي ضد الشركات الامريكية وهذا تهديد مستمر اما من دول ذات قدرات تقنية قليلة بمقاصد تخريبية مثل ايران التي تورطت في هجمات DDOS بين عامي 2012 و 2013 ضد الولايات المتحدة ومؤسساتها المالية وفي هجوم عبر الانترنت في شباط 2014 على شركة كازينو لاس فيغاس ساندز وكوريا الشمالية المسؤولة عن الهجوم الالكتروني الذي نفذ في تشرين الثاني عام 2014 ضد شركة سوني بيكتشرز انترتينمنت او المجرمون الذين يقصدون الربح او القراصنة ذو الدوافع الايدلوجية او المتطرفون[35]، واوضحت الولايات المتحدة الامريكية ان التهديد الرئيس ياتي من الصين؛ لان جهاز الاستخبارات العسكرية الصيني يسعى الى الحصول على التكنولوجيا الامريكية العسكرية؛ بناء على تقرير شركة لوكهيد مارتن انه عام 2013 تم اطلاق هجوم سايبري يستهدف النموذج الجديد الذي تصعنه الشركة من طائرة الشبح المقاتلة ذات المهام المشتركة[36].

2- الإرهاب السيبراني ويتمثل بالاعتداء على شبكة الإنترنت بغية تعطيل خدماتها وإشاعة عدم الثقة في الإنترنت في صفوف المستخدمين. والأهم من ذلك هو الهجمات على البنية الأساسية المعلوماتية التي تشغل كثيراً من القطاعات الحساسة، كالنقل والطاقة والطيران. ويمكن أيضاً استخدام الإنترنت للترويج للأفكار الإرهابية أو لنشر مواد تدريبية (كصنع متفجرات) أو لجمع التمويل أو لتجنيد أشخاص أو للتواصل بين الشبكات الإرهابية وهو ما تتخوف منه الولايات المتحدة الامريكية منذ احداث الحادي عشر من ايلول عام 2001[37]، فالدور الذي اداه الإنترنت في انتشار ظاهرة الإرهاب، ثم تناول الاستراتيجيات الإعلامية التي اعتمدها أسامة بن لادن قائد تنظيم

القاعدة الارهابي، حيث أنشأ إدارة إعلام القاعدة عام 1988، وذلك لتكريم المجاهدين ضد الاتحاد السوفييتي، ثم تحولت هذه الأداة للهجوم على الولايات المتحدة الامريكية وتكفيرها، وكل الدول التي لا تطبق الشريعة[38]، مثَّلت حوادث القرصنة الإلكترونية لأنظمة الطائرات، والمخاوف من استهداف مجموعات إرهابية للنقل الجوي، دافعًا للدول لمواجهة تلك المخاطر الإلكترونية لأمن الطائرات المتصل بالامن القومي للولايات المتحدة الامريكية وبحسب قرار الحظر الذي اتخذته، فإنه يسري على الرحلات القادمة مباشرة من 10 مطارات في 8 دول، وينطبق على 9 شركات جميعها غير أمريكية بسبب عدم امتلاكها خطوط طيران مباشرة من المطارات المذكورة للولايات المتحدة، وهي: شركة الخطوط الجوية الملكية الأردنية، وشركة مصر للطيران، وشركة الخطوط الجوية التركية، وشركة الخطوط الجوية العربية السعودية، وشركة الخطوط الجوية الكويتية، وشركة الخطوط الملكية المغربية، وشركة الخطوط الجوية القطرية، وشركة الخطوط الجوية الإماراتية، وشركة الاتحاد للطيران[39]

3- الحروب الالكترونية (السيبرانية) وتعني قيام دولة او فواعل من غير الدول بشن هجوم الكتروني في اطار متبادل، او من قبل طرف واحد، وبرغم ذيوع مسمى الحرب الالكترونية (السيبرانية) اعلاميا، فانه يعد مصطلحاً قديما مقصوراً على رصد حالات التشويش على انظمة الاتصال والرادار واجهزة الانذار بينما يكشف الواقع الراهن في الفضاء الالكتروني (السيبراني) عن دخول شبكات لاتصال والمعلومات الى بنية ومجال الاستخدامات الحربية[40].

4- الحض على الكراهية والعنف والعنصرية تستخدم مجموعات متطرفة المواقع الإلكترونية لنشر أفكارها، وهذه المواقع في ازدياد مستمر، القدح والذم والتشهير والتهديد والابتزاز عبر شبكة الإنترنت، ولا سيما على المواقع الإلكترونية ومواقع التواصل الاجتماعي من اجل جعل سمعة الولايات المتحدة الامريكية سيئة الصيت امام الراي العام الداخلي او العالمي[41] .

5- الاستخبارات المضادة وروسيا الاتحادية او الصيني هي المصدر الرئيس للتهديد لاختراق اجهزة صنع القرار الوطني ووكالة الاستخبارات السرية للولايات المتحدة من

قبل استخبارات الدول الاجنبية وهو استهداف لامن المعلومات الوطنية والمعلومات السرية للشركات والمؤسسات الامريكية المتعاقدة مع الدفاع والطاقة والمالية وغيرها[42]

6- الفضاء والفضاء المضاد: تزايد التهديدات لأنظمة الفضاء التابعة الولايات المتحدة وخدماتها في العام 2015 وما بعده، وذلك مع تزايد الخصوم المحتملين وإظهارهم قدرات الفضاء المضاد التخريبية والهدامة، فلدى الصين قدرات التشويش على الأقمار الصناعية وتسعى إلى بناء أنظمة مضادة للأقمار الصناعية،. أصرت العقيدة الروسية القتالية في العام 2010 على اعتبار الدفاع الفضائي مجالا حيويا للدفاع عن أمنها القومي. أكد القادة الروس علنا أن القوات المسلحة الروسية تملك أسلحة مضادة للأقمار الصناعية وتطور بحوثا لأنظمة مضادة جديدة، لدى روسيا مشوشات على الأقمار الصناعية وتسعى إلى أنظمة مضادة للأقمار الصناعية[43]، وأجرت الصين في تموز عام 2014 تجربة صواريخ غير مدمرة مضادة للأقمار الصناعية، إن النقطة المفصلية في تزايد المخاوف الدولية من سباق عالمي حاد حول التسلح في الفضاء الخارجي جاءت بعد قيام الصين عام 2007 بتدمير القمر الصناعي "فنغ يون 1سي" المخصص للأحوال الجوية في الفضاء بصاروخ مضاد للأقمار الصناعية، وهو ما اعتبرته الولايات المتحدة في وقتها نقلة نوعية وتطوراً تكنولوجياً غير مسبوق بالنسبة إلى الصين، وفي السياق نفسه فقد جاء في تقرير مفصّل بالصور عن طريق الأقمار الصناعية الأمريكية، ونُشِرَ في مارس/آذار 2014 مجموعة من الأدلة الإضافية على أنّ إطلاق صاروخ صيني في مايو/أيار 2013 الذي وصِفَ على أنّه مهمة بحثية بحسب تصريحات المسؤولين في الصين كان في الواقع اختباراً لسلاح جديد مضاد للأقمار، أن الإدارات الأمريكية المُتَعاقبة تنظر إلى الفضاء الخارجي كونه "مسرحاً للهيمنة الأمريكية"، وترسيخاً لهيمنتها في الأرض، وكنظام مُتطوّر قد يُساعد أمريكا في حال تعرضها لغزو أو لضربة باليستية أو نووية، عبر أنظمة التجسس والمراقبة والتعقب المُستمرة، ومن ثم فلم يكن غريباً أنْ تكون الولايات المُتحِدة الأمريكية أكثر دول العالم امتعاضاً من التقدم الصيني في استخدام الفضاء الخارجي، سواء لأغراض

عسكرية أو غير عسكرية؛ لأن استمرار السيادة على الفضاء الخارجي جزءٌ مهم من العقيدة العسكرية الأمريكية[44]. فابرز الاهداف الالكترونية التي يتم استهدافها في الولايات المتحدة الامريكية تتمثل في[45]:

1- على المستوى الاتحادي البيت الابيض والكونغرس الامريكية ووزارة الداخلية؛ كونها رموز للأمن القومي الامريكي.

2- على المستوى العسكري يتم استهداف وزارة الدفاع والوحدات القيادية القتالية لعرقلة العمليات العسكرية كما هو الحال في العراق وافغانستان.

3- على المستوى المدني استهداف البنية التحتية المؤسسات المالية ومحطات الطاقة والاتصالات؛ لانها تصيب اكبر عدد من مواطني الولايات المتحدة الامريكية، وتعد من اخطر الاهداف لانها لاتقتصر على الاستخدامات المدنية بل والاستخدامات العسكرية وتشمل تهديد المصالح الحيوية القومية الامريكية المختلفة، وهذه بنى حرجة للولايات المتحدة الامريكية لانها تتضمن النظم والاصول سواء اكانت مادية ام افتراضية والتي يتسبب تدميرها او التلاعب بها في تهديد للأمن القومي الامريكي او الاقتصاد الامريكي او الرعاية الصحية او الامن العام.

المحور الرابع: استراتيجية الولايات المتحدة الامريكية للأمن السيبراني

ظلت الولايات المتحدة الامريكية رائدة فيما يتعلق بقدرتها على تفسير التهديدات السيبرانية الجديدة والناشئة؛ كونها الناشئة لشبكة الانترنيت وهي موقع القيادة في النظام الدولي سعت إلى نقله في استراتيجياتها الامنية القومية لاسيما وانا هناك نشطا ومساهمة لفواعل غير الحكومية في الفضاء السيبراني وتأثيرهم يقارب من تاثيرات الفواعل الحكومية على الامن القومي، لذلك تنقسم حروب الفضاء الإلكتروني طبقًا للمؤسسة العسكرية الأمريكية إلى قسمين رئيسيَّين: الدفاع الإلكتروني (Defensive Counter Cyber DCC)، والهجوم الإلكتروني (Offensive Counter) Cyber OCC)، ويشمل الأول التعرّف على أي أنشطة إلكترونية عدوانية، وكشف هوية القائمين عليها، واعتراضها بنجاح، وتدميرها أو

على الأقل وقف آثارها التخريبية، في حين تشمل الثانية كافة العمليات الرامية إلى تدمير، أو تعطيل، أو تحييد، الإمكانيات الإلكترونية الخاصة لأي بلد قبل أو بعد استخدامه ضد الولايات المتحدة أو أي من حلفائها، بالإضافة إلى جمع المعلومات من أي أجهزة كومبيوتر وأنظمة وشبكات معلوماتية، وتعديلها أو تعطيلها أو تدميرها، فبدأت الولايات المتحدة في الاهتمام بمجال حروب الفضاء الإلكتروني عام 1993، حين دشنت مركز الحروب المعلوماتية التابع للقوات الجوية، وكانت عمليات الدفاع والهجوم آنذاك تتم معًا تحت قيادة وحدة الحرب المعلوماتية رقم 609، ورغم ذلك، فإن دورها ظل مقتصرًا على التنسيق مع البنتاجون وتقديم الاقتراحات له، دون القدرة على شن هجمات أو حملات دفاع في المجال الإلكتروني.

وبدأت الادارة الامريكية في تصور مصطلح السيبرانية في عهد الرئيس الامريكي السابق بيل كلينتون عام 1998، وجميع وثائقه المتعلقة باستراتيجية الأمن القومي للاعوام 1998 و 2000 و 2001 وهي تهديدات إلكترونية ذات صلة عامة بحماية الهياكل الأساسية الوطنية الحرجة، والجريمة، والشراكات بين الولايات، فأنشأت وزارة الدفاع الامريكية البنتاغون قوة دفاع شبكات الكومبيوتر المشتركة (JTF-CND) لتولي مسؤولية الهجوم والدفاع الإلكتروني، قبل أن يتم الفصل بينهما، لتؤول مهمة الهجوم إلى وكالة الأمن القومي، ومهمة الدفاع إلى وكالة الدفاع عن أنظمة المعلومات، واللتين اجتمعتا لاحقًا تحت مظلة القيادة الإلكترونية الأمريكية عام 2009، والتي يقودها مدير وكالة الأمن القومي نظرًا لتمتّعها بإمكانات كبيرة في مجال تكنولوجيا المعلومات والاتصالات، كما تدل على ذلك التسريبات الأخيرة بخصوص تجسس الوكالة على دول مختلفة حول العالم (USCYBERCOM)[46].

فبناء الهيكل الالكترو حكومي يستدعي حمايته من المتطفلين وجماعات التخريب اي الحفاظ على الحدود الوطنية الالكترونية كاهم مقومات الامن القومي الامريكي مثلما الحفاظ على الحدود الجغرافية في الحكومات الكلاسيكية، وهو ما طرح مشكل الامن المعلوماتي في الدولة واجهزتها الحكومية الامريكي ومن ثم تطوير تشكيلات جديدة

داخل الحكومة كوحدة رقابية امنية المعلوماتية للحفاظ على امن البلاد القومي الالكتروني، وانجاز جهاز مناعة معلوماتي، يجنب الحكومة نسف مشروع التحول الالكتروني ومن ثم زعزعة ثقة المواطنين بالنموذج الالكتروني – حكومي، وهو ماحذا بالولايات المتحدة الامريكية عام 2000 الى تطوير برنامج سمي كارنييفور او الملتهم وظيفته التجسس على جميع انواع الاتصالات التي تتم عبر الانترنيت لاسيما مع وجود شبكة تجسس عالمية امريكية اوربية اسمها ايشلون، اسستها وكالة الامن القومي الامريكي مع عدد من المؤسسات الاستخبارية العالمية هدفها التجسس على الاتصالات الرقمية السلكية واللاسلكية والاتصالات عبر الاقمار الصناعية، وهذا البرنامج الملتهم هو نظام الكتروني مصمم يسمح لوكالة المباحث الفيدرالية الامريكية بالتعاون مع الشركة المزودة بالانترنيت بتطبيق حكم محكمة جمع المعلومات محددة حول رسائل البريد الالكتروني لمستخدم يستهدفه التحقيق[47].

بين عامي 2000 و 2001، بدأنا نرى عسكرة مصطلح السيبرانية، والتي تعكس جزئيا الصراع المتنامي بين الصين وتايوان في ذلك الوقت. واعترافا بهذا التحول، شدد البيت الأبيض على بناء خطة شاملة للمرونة السيبرانية، شملت الشراكات بين القطاعين العام والخاص في مجال تبادل المعلومات، وتدابير الكشف عن التهديدات، وقوة عاملة قادرة، بالإضافة إلى حماية البنى التحتية كما أعدت الولايات المتحدة الامريكية نفسها للحرب على تنظيم القاعدة الارهابية بقيادة الرئيس السابق جورج دبليو بوش، في حين أن السيبرانية في عام 2006 كانت مقترنة بالفضاء كوسيلة لتقديم الدعم العسكري لإسقاط القوة الحركية في الخارج[48].

تقوم الولايات المتحدة الامريكية منذ عام 2005 بعمل مناورات عسكرية تعرف باسم ceber storm لاختبار قدراتها على مواجهة الاخطار كان اخرها عام 2010 مع تزايد عمليات الاختراق لشبكاتها الدفاعية لما تسببه من خسائر اقتصادية عالمية تقدر 100 بليون دولار سنوياً، واخذت هذه القضية منحى اخر بعد تزايد الاختراقات لوزارة الدفاع الامريكية في اطار الحرب الباردة مع الصين لانها المتهمة الاولى في هذه

الاختراقات في ظل التجسسات الالكترونية التي تتبعها الدول من اجل خرق الامن القومي للولايات المتحدة الامريكية[49].

وحددت استراتيجية الولايات المتحدة الامريكية للأمن القومي 12 عنصرا من عناصر الامن القومي لعام 2006، هي الاتصالات السلكية واللاسلكية ومحطات الطاقة والكهرباء والبنية التحتية الخاصة بصناعة نظم الدفاع والاسلحة، ونظم استخراج وصناعة ونقل وتخزين الغاز والنفط، ونظ الزراعة وتوزيع الاطعمة والخدمات المصرفية والمالية، ونظم المواصلات وامدادات المياه، والخدمات الطبية وخدمات البريد والنقل وخدمات الطوارئ واخيرا الحكومة نفسها، وهذه البنى تصبح مرمى الهجمات الالكترونية، لدرجة ان لجنة المصالح القومية للولايات المتحدة الامريكية اكدت على حماية هذه البنى من التهديدات السسيبراني في استراتيجية الامن القومي لعام 2010، هذه البنية التحتيةهي بمنزلة اصل قومي لتدعيم الامن القومي الامريكي[50].

صدرت عام 2006 الاستراتيجية القومية العسكرية لعمليات الفضاء الالكتروني، وهي استراتيجية للقوات المسلحة الامريكية هدفها تحقيق التفوق وبسط النفوذ على الفضاء الالكتروني من خلال العمليات المعلوماتية وعمليات الشبكة فتساعد في السيطرة على المعلومات وتبادلها وتوظيفها بما يخدم الاهداف المرسومة دون التلاعب او تدميرها والقدرة على اختراق ومراقبة بيانات العدو، والتطبيقات الحركية حرية الحركة داخل الفضاء الالكتروني سواء اكانت حركات هجومية ام دفاعية، وتطبيق القانون من خلال سرعة اجراء التحقيقات في الاعمال الاجرامية لردع الجناة، ومكافحة التجسس من خلال معرفة الخصم ونواياه واهدافه وقدرته في استغلال المجال الالكتروني التي يقوم بها[51].

فالولايات المتحدة الامريكية في محاولة منها لاختبار النظم الالكترونية لمواجهة الارهاب الالكتروني فقامت بعقد مناورة الكترونية في شباط عام 2006 لمدة اسبوع وسميت بعاصفة الحواسيب الاولى، من قبل وكالة الاستخبارات الامريكي المركزية اذ وضعت بناها التحتية الحيوية في محاكاة هجوم الكتروني برعاية وزارة الامن الداخلي واشترك في هذه الحرب 115 وكالة تراوحت من وكالة الاستخبارات المركزية ومكتب

التحقيقات الفيدرالي الى الصليب الاحمر الدولي، من اجل اختبار كفاءة التنسيق بين خدمات الطوارئ بين القطاعين الحكومي والخاص لدعم الامن الالكتروني، وتم اجراء مناورة اخرى في شباط عام 2008، سميت عاصفة الحواسيب الثانية شاركت فيها الولايات المتحدة الامريكية وكندا واستراليا وكند ونيوزيلاندا والمملكة المتحدة[52] فضلا عن وزارة الدفاع والعدل الامريكية وتمت دعوة ولايات امريكية للمشاركة و 40 شركة خاصة واستمرت مدة 18 شهرا بتكلفة 2.6 مليون دولار[53].

واعلنت الولايات المتحدة الامريكية عام 2009 بتشكيل قيادة عسكرية للفضاء الالكتروني لحماية شبكات الجيش الامريكي ليبر اهمية الفضاء الالكتروني بما يتضمنه من قضايا عدة ذات صلة وثيقة بأمنها القومي في ظل الاعتماد الدولي عليه فيما يتعلق بتسيير عمل البنية التحتية الكونية للمعلومات امام المنشأت المدنية والعسكرية من خلال تعرضه لهجوم يستهدفه كوسيط وحامل للخدمات او بشل عمل انظمتها المعلوماتية فان التحكم في تنفيذ هكذا هجمات يعد ادارة سيطرة ونفوذ استراتيجية بالغة الاهمية في زمن السلم والحرب[54].

وتم تعيين الجنرال الكسندر كيث لادارة حروب الفضاء الالكتروني من اجل عسكرة فضاء الانترنيت فل اجهزة القوات المسلحة، وعينت الحكومة الامريكية هوارد شميت الذي اطلق على فريقه بالمبادرة القومية لتعليم امن الفضاء الالكتروني منسقا في هيئة الامن القومي، وحظى الفضاء الالكتروني باهمية بارزة في استراتيجية الامن القومي الامريكي عام 2010 على عد ان الخطر الاكبر الذي يتعرض له الامن القومي ياتي من اسلحة الدمار الشامل والنووية والفضاء الالكتروني ما يجعل امننا القومي معرض للتهديد المستمر[55].

وتجري الولايات المتحدة الامريكية سنويا محاكاة التعرض لحرب الكترونية، وخصصت 500 مليون دولار في ميزانية عام 2012 لمواجهة التهديدات الالكترونية وتطوير اسلحة وادوات الحرب الالكترونية تشمل فايروسات قادرة على تخريب شكات العدو الحساسة، واعلنت عن جهود تصنيع اسلحة انترنيت هجومية لمواجهة احتمال تعرضها

لهجوم، وزادت تمويل الابحاث الالكترونية من 120 مليون دولار الى 208 مليون دولار عام 2012 والامر في تزايد كل عام[56].

لحظت وزارة الداع الامريكية في تقريرها الاستراتيجي حول الموازنة المالية لعام 2014، اعادة تنظيم على مستوى الموارد البشرية والكفاءات لديها لتعزيز قوتها السيبراني في مواجه تهديدات امنها القومي ضمن فرق متخصصة في مجالات ثلاثة هي حماية الشبكات، وشل قوة العدو السيبرانية، وحماية الدفاع الوطني. وانشاء قوة سيبرانية عام 2016، مؤلفة من اربعين فرقة موزعة على مهمات هجومية ودفاعية، ووتتوزع مسؤولية الامن السيبراني فيها بين وزارة الداخلية ومكتب التحقيقات الفيدرالي ووزارة الدفاع بما فيها قيادة الامن السيبراني التي تضم وكالة الامن القومي التي تستند اليها العمليات الهجومية فضلا عن وحدات من وكالة الاستخبارات المركزية، في المقابل يتولى الجهاز القيادي السيبراني التابع للقيادة الفيدرالية مسؤولية حماية البنية التحتية السيبرانية العسكرية، ويضم هذا الجهاز القيادة السيبرانية للجيش وقيادة القوات الجوية والبحرية، وتتعاون الوزارتين على تنسيق جهودهما بموجب اتفاق عام 2010، فاستخدمت الولايات المتحدة الامريكية بعد هجمات الحادي عشر من ايلو عام 2001، مكافحة الارهاب كذريعة لاستخدامها تقنيات حديثة للمراقبة والتجسس على مواقع شبكة المعلومات الدولية – الانترنيت – والاتصالات الهاتفية وبرامج الكترونية للتجسس[57].

فالولايات المتحدة الامريكية ادركت صعوبة تعقب الارهابين والقضاء على نشاطهم عبر الانترنيت، لذلك اعلنت عن زيادة حصة الحرب المعلوماتية في ميزانية الدفاع لعام 2017 بنسبة 15% لتصل الى 6,5 مليار دولار، بعد التحذيرات التي اطلقت من ان داعش الارهابي له قدرات في تدمير البنية التحتية غير المحمية او المساكن التي تستخدم خوادم الانترنيت لأهداف عامة وخاصة في اطار ما يعرف الويب المظلم، فاعلن وزير الدفاع الامريكي السابق اشتون كارتر ان الولايات المتحدة الامريكية تستخدم اسلحة معلوماتية في حربهم ضد الارهاب من اجل اضعاف قدرتهم على العمل

والاتصال في ساحة المعركة الافتراضية، لكن يبقى الكشف ع هذه الاسلحة سرية لانها جديدة ومفاجئة وقابلة للاستخدام ضد خصوم غير التنظيمات الارهابية[58].

و تعزيزاً للجهود الخاصة بمواجهة تنظيم داعش على الإنترنت بعده خطرا على الامن القومي الامريكي حاله حال بقية التنظيمات الارهابية المتطرفة، عملت الولايات المتحدة الامريكية على تشكيل فريق الأحلام التكنولوجي الذى يجمع عمالقة التكنولوجيا حول العالم لمحاربة تنظيم داعش على الإنترنت، ويضم هذا الفريق حوالى خمسين شركة تكنولوجية ، وتقوم هذه الشركات بوضع استراتيجيات لمنع انتشار رسائل داعش على المواقع، ووضع خطط لمواجهة الدعاية الإرهابية، لذا عرض المسئولين التنفيذيين في شركة أبل و تويترو فيسبوك، قدراتهم التي يمكن أن يساعدوا بها لمكافحة انتشار رسائل داعش على المواقع المختلفة ، وقد قامت الإدارة الأمريكية بزيارة وادى السليكون يناير 2016 فى محاولة للضغط على منع داعش من استخدام منصات وسائل الإعلام الاجتماعية الشعبية لتجنيد الإرهابيين[59].

وقامت وكالة الاستخبارات الامريكية بتوظيف الفا من خبراء امن المعلومات وقوة ضاربة على مدى 24 ساعة لمواجهة الارهاب الالكتروني[60].

تعد الولايات المتحدة الامريكية من اكثر الدول تمكنا في مجال القوة الالكترونية والقادرة على توفير اقصى درجات الامن السيبراني نتيجة التخوف المستمر من سيطرة جماعات ارهابية سواء اكانت دولا ام جماعات ارهابية كفاعلين من غير الدول تهدد الامن القومي من خلال السيطرة على المنشات الحيوية المدنية والعسكرية والسياسية بما يفسد عملها حتى وان كان الامر يستغرق بعض ساعات، ما ادى الى نقل التفاعلات من ارض الاقع الى الفضاء الالكتروني كحالة الصراع بين تنظيم القاعدة وداعش الارهابيان والولايات المتحدة الامريكية او بين الولايات المتحدة والدول التي تريد ضرب الامن القومي لها مثل كوريا الشمالية وايران وروسيا الاتحادية والصين[61].

أكد روجرز أن التهديد الإلكتروني آخذ بالازدياد، فالهجمات السيبرانية لا تسعى لتعطيل أو عرقلة القدرات السيبرانية الأمريكية فحسب، إنما تسعى لـ"تأسيس وجود دائم على شبكاتنا"، واتهم روجز حكومات إيران وروسيا والصين بتوجيه هجمات

قراصنة الانترنت "الهاكرز" الفردية على الشبكات الأمريكية، حيث أوضح أنه يوجد رابط قوي ومباشر ما بين هذه الهجمات وتوجيهات هذه الدول بالهجوم أو بالتدخل، وزاد من إصرار خصومنا على مواصلة قيامهم بالهجمات بشكل يهدد أمننا القومي على نحو متزايد[62]. فعمدت الادارة الامريكي في عهد الرئيس السابق باراك اوباما الى اتخاذ التدابير الاتية[63]:

1- تعزيز الاطار التشريعي والقانوني عبر اصدار قانون خاص لمكافحة الارهاب على الانترنيت باسم قانون حماية الشبكات السيبرانية.

2- تعزيز دور مركز الاتصالات الاستراتيجي لمكافحة الارهاب التابع لوزارة الخارجية ويعمل فيه متخصصون لنشر مواد مناهضة للإرهاب.

3- اطلاق مشروع مخصص للتصدي للهجمات الارهابية السيبرانية ومحاولات التجنيد عبر الانترنيت يعتمد على بث تغريدات مضادة للإرهاب واستهداف حسابات الارهابيين.

4- ارساء قواعد تعاون مع الدول الاخرى باطلاق مبادرات مثل مبادرة التعامل مع الامارات العربية المتحدة والمملكة المتحدة سواء اكان لمحاربة الاعلام الارهابي ام من خلال تفعيل تبادل المعلومات بين اجهزة طوارئ الانترنيت، وانشاء خلايا مشتركة لرصد التهديدات السيبرانية.

5- يقوم جهاز من المتجسسين فيها بتمشيط مواقع التواصل الاجتماعي، لتمحيص بيانات الارهابين والمواد التي ينشرونها وتتبع تحركات.

تسعى الأنظمة الحكومية التي تتعرض لهجمات قاسية من الدول الأخرى للحصول على معلومات استخباراتية وطنية وأخرى صناعية. وعلى الرغم من أن الصين متهمة علانية بالقيام بهذا النوع من النشاط، فهناك دول أخرى كثيرة من المعروف أنها مضطلعة في الأمر أيضا. علاوة على ذلك، لم يقتصر استخدام الدول للإنترنت بشكل عدائي على قطاع المعلومات الاستخباراتية. فقد أعطى نموذج المراهقين الذين قاموا في فيلم المناورات **War Games** باقتحام أنظمة الدفاع وعمل مناورات، أدلة موثوقة في الحالات مثل حالة استونيا، تثبت أن هناك هجمات تتم برعاية الدولة بمعرفة

جيوش محترفة من المحاربين الإلكترونيين داخل الجيش أو يعملون تحت رعايته. في الواقع، ابتكرت الولايات المتحدة برنامج (CyberCorps9) الخاص بها لأنها تعتبر الهجوم الإلكترونيً حاليا أحد مكونات أي حملة تنفذها[64]. كذلك ضمن التوجه الحكومي الامريكي ضمن استراتيجية الامن السيبراني ، وافق الجيش على برنامج لتجنيد خبراء الامن السيبراني من ذوي الخبرة مباشرة في الخدمة كضباط الكترونيين لمحاولة لتعزيز حقل متنامي يرى القادة العسكريون انه امر حيوي بالنسبة للأمن القومي، وأعطى الكونغرس الامريكي وزارة الدفاع الامريكية الإذن حتى عام 2020 لدراسة إمكانات توسيع برامج التكليف المباشر، عن طريق التخلي عن دورة التدريب الاساسية القتالية للجيش التي تستغرق 10 اسابيع من اجل جذب القادة الموهوبين بالامن السيبراني من اجل ان تكون استراتيجية الامن السيبرانية القومية قادرة على ردع أي تهديد[65].

الخاتمة

نظرا لطبيعة التهديدات الفضائية السيبرانية المتجددة بصورة مستمرة فهناك عناصر تغير واستمرار حيوية في الطرق والمعالجات التي تتضمنها استراتيجيات الولايات المتحدة الامريكية للأمن القومي فيما يخص الامن الفضائي السيبراني، وهي استراتيجيات استباقية وقائية لردع الهجمات الفضائية السيبرانية شاملا لكل الابعاد السياسية والاقتصادية والعسكرية والمدنية، من حيث ادخالها الوحدات السيبرانية في جيوشها، وتعزيز الاطر التشريعية والقانونية لملاحقة مصادر التهديدات، والتعاون مع الدول الاخرى لمكافحة هذه الظاهر لان الامن القومي مهدد بصورة مستمرة من قبل هذه التهديدات السيبرانية وليس من طريقة فعالة لمواجهة ذلك الا بالتعاون مع الدول الاخرى على عدّ ان الامن القومي الامريكي له انعكاس على الامن الدولي بأكمله، ولكن الردع الفضائي للتهديدات السيبرانية على الامن القومي صعب الاحكام عليه بصورة دائمة؛ لأنه على الرغم من الاحتياطيات المستمرة من قبل الولايات المتحدة الامريكية نلاحظ بعض الاختراقات وعمليات القرصنة وتسريبات المعلومات لان مجال

التهديدات الفضائية السيبرانية مجال حيوي ومتجدد ما ان تتوصل الى طرق لمعالجة الاختراقات الفضائية وترصين الشبكات حتى يظهر نوع ونمط جديد للتهديدات وهذا يعتمد على فعالية وحيوية الوحدات الدولية – الدول والافراد – لاكتشاف الثغرات التي يمكن من خلالها الوصول الى الاهداف المبتغاة.

[01] احمد عبيس نعمة الفتلاوي، الهجمات السيبرانية: مفهومها و المسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مجلة المحقق الحلي للعلوم القانونية والسياسية، جامعة بابل، العراق، العدد 4، 2016، ص 614.

[02] ايهاب شوقي، الحرب السيبيرانية: حرب المستقبل المفزعة، ملفات خاصة، 19/2/2015، شبكة الاخبار العربية، شبكة المعلومات الدولية– انترنيت – http://www.anntv.tv/new/showsubject.aspx?id=101954.

[03] حمزاوي ميلود، الامن الالكتروني، قسم العلوم السياسية والعلاقات الدولية، كلية الحقوق، جامعة الحاج لخضر باتنة، الجزائر، 2014، ص 4.

[04] ربيع محمد يحيى، اسرائيل وخطوات الهيمنة على ساحة الفضاء السيبراني في الشرق الاوسط: دراسة حول استعدادات ومحاور عمل الدولة العبرية في عصر الإنترنت 2002–2013، مجلة رؤى استراتيجية، مركز الامارات للدراسات والبحوث الاستراتيجية، الامارات العربية المتحدة، حزيران 2013،

[5]() فادية عباس هادي، استراتيجية اوباما في الحرب المعلوماتية، اوراق دولية، العدد 193، مركز دراسات دولية، جامعة بغداد، بغداد، 2010، ص 15.

[06] ايهاب خليفة، القوة الالكترونية: كي يمكن ان تدير الدول شؤونها في عصر الانترنيت، دار العربي للنشر والتوزيع، بيروت، 2017، ص 27.

[07] المصدر نفسه، ص 27.

[08] المصدر نفسه، ص 27.

[09] د.فريدة طاجن، سياسات الدفاع الماليزية في ظل التهديدات الأمنية للبيئة الرقمية: الواقع والتحديات، برنامج الملتقى الدولي حول سياسيات الدفاع الوطني للمدة 30–31 كانون الثاني 2017، ص 342.

[010] د.عادل عبد الصادق، انماط الحرب السيرانية وتداعياتها على الامن العالمي، ملحق مجلة السياسة الدولية، مركز الاهرام للدراسات السياسية والاستراتيجية، مصر، العدد 208، نيسان 2017، ص 31.

[011] وليد غسان سعيد جلعود، دور الحرب الالكترونية في الصراع العربي الاسرائيلي، اطروحة دكتوراه غير منشورة، كلية الدراسات العليا، جامعة النجاح الوطنية، فلسطين، 2013، ص ص 81–82.

[12]() ايمان الحيارى، مفهوم الحرب الالكترونية، 12/12/2016، مقالة منشورة على شبكة المعلومات الدولية– انترنيت– http://mawdoo3.com.

[13]() عادل عبد الصادق، الحروب السيبرانية : تصاعد القدرات والتحديات للأمن العالمي، المركز العربي لأبحاث الفضاء الالكتروني، 12/3/2017، شبكة المعلومات الدولية – انترنيت

http://accronline.com

[14]() ذياب البدانة، الامن وحرب المعلومات، دار الشروق للنشر، الاردن، 2002، ص 150.

[15]() نورة شلوش، القرصنة الالكترونية في الفضاء السيبراني: التهديد المتصاعد لأمن الدول، مجلة مركز بابل للدراسات الانسانية، المجلد 8، العدد 2، 2018، ص 190.

[16]() سماح عبدالصبور، الصراع السيبراني: طبيعة المفهوم وملامح الفاعلين، في اتجاهات نظرية في تحليل السياسية الدولية، ملحق مجلة السياسية الدولية، مركز الاهرام للدراسات السياسية والاستراتيجية، القاهرة، العدد 208، 2017، ص 6

[17]() هاري آر.يارغر، الاستراتيجية ومحترفوا الامن القومي: التفكير الاستراتيجي وصياغة الاستراتيجية في القرن الحادي والعشين، ترجمةراجح محرز علي، مركز الامارات للدراسات والبحوث الاستراتيجية، ابو ظبي، الامارات العربية المتحدة، 2011، ص 56.

[18]() تباني وهيبة، الامن المتوسطي في استراتيجيات الحلف الاطلسي: دراسة حالة ظاهرة الارهاب، كلية الحقوق والعلاقات الدولية، جامعة مولود معمري – تيزي وزو، الجزائر، 2014، ص 20.

[19]() ياسر عبدالرزاق وهيب، مستقبل الامن الاقليمي في آسيا الباسفيك، رسالة ماجستير غير منشورة، كلية العلوم السياسية، جامعة النهرين، بغداد، 2007، ص ص 14–15.

[20]() وليد غسان سعيد جلعود، مصدر سبق ذكره، ص ص 39–40.

[21]() فرج مفتاح فرج، تهديد الامن القومي العربي المعاصر 2003–2016، رسالة ماجستير غير منشورة، كلية الآداب والعلوم، جامعة الشرق الاوسط ، الاردن، 2017، ص 12.

[22]() وليد غسان سعيد جلعود، مصدر سبق ذكره، ص ص 39–40.

[23]))ياسر عبدالرزاق وهيب، مصدر سبق ذكره، ص 13.

[24]) الاتحاد العالمي للاتصالات، الامن السيبراني القرار 181 الصادر في غواداخارا، صحيفة اخبار الاتحاد، تشرين الثاني، 2010، ص 20، شبكة المعلومات الدولية – انترنيت –

http://www.itu.int/net/itunews/issues/2010/09/pdf/201009_20-ar.pdf

[25]( ) حمزاوي ميلود، مصدر سبق ذكره، ص 6

[26]() حسن طاهر، الحاسب وامن المعلومات، مكتبة الملك فهد الوطنية، المملكة العربية السعودية، 2000، ص 23.

[27]() مازن عدنان الديوه جي، سبع اتجاهات في الامن السيبراني لعام 2017،

[28] ايهاب خليفة، مصدر سبق ذكره، ص ص 80–81.

[29]) عادل عبد الصادق، القوة الالكترونية: اسلحة الدمار الشامل في عصر الفضاء الالكتروني، مجلة السياسية الدولية، مركز الاهرام للدراسات السياسية والاستراتيجية، القاهرة، العدد 188، 2012، ص ص 29–30.

[30]) عادل عبد الصادق، انماط الحرب السيرانية وتداعياتها على الامن العالمي، ملحق مجلة السياسة الدولية، مركز الاهرام للدراسات السياسية والاستراتيجية، مصر، العدد 208، نيسان 2017، ص ص 33–34.

[31]) نورة شلوش، مصدر سبق ذكره، ص 192.

[32] لمزيد من التفاصيل ينظر: د. عبدالهادئ محمود الزيدي، التجسس الاسرائيلي الالكتروني على الدول العربية، مجلة دراسات دولية، مركز الدراسات الدولية، جامعة بغداد، العراق، العدد 58، 2014، ص 141.

[33] اللجنة الاقتصادية والاجتماعية لغربي اسيا الاسكوا، الامان في الفضاء السيبراني ومكافحة الجرائم السيبرانيةفي المنطقة العربية: توصيات سياسياتية، الامم المتحدة، 9 شباط 2015، ص 72.

[34] عادل عبد الصادق، الفضاء الالكتروني وتهديدات جديدة للامن القومي، مجلة السياسة الدولية، مركز الاهرام للدراسات السياسية والاستراتيجية، القاهرة، العدد 180، 2010، ص 45.

[35] جيمس اركلابر، تقييم التهديد العالمي للولايات المتحدة الامريكية للعام 2015، ترجمة موقع السوري الجديد، وكالة الاستخبارات الامريكية، 26/3/2015، شبكة المعلومات الدولية –انترنيت – ولمزيد من التفاصيل ينظر الى النص الاصلي:

https://newsyrian.net/ar / James r. Clapper, Statement For the Record Worldwide Threat Assessment of the U.S Intelligence Community Senate Armed Services Committee, 26 February 2015, pp1-4.

[36] مارك بيردسول، مستقبل الاستخبارات في القرن الحادي والعشرين، سلسلة محاضرات الامارات 169، مركز الامارات للدراسات والبحوث الاستراتيجية، ابوظبي،2014، ص 17.

[37] لمزيد من التفاصيل ينظر: د. فاطمة الزهراء عبدالفتاح، تطور توظيف جماعات العنف للارهاب السيبراني، ملحق مجلة السياسة الدولية، مركز الاهرام للدراسات الاستراتيجية والسياسية، العدد 208، نيسان 2017، ص ص 25–29.

[38] المعهد المصري للدراسات، استخدام القوة الالكترونية في التفاعلات الدولية، 29/10/2016، شبكة المعلومات الدولية – انترنيت –**http://eipss-eg.org/**

[39] محمد عزت هلال، اليات المواجهة: تهديدات الامن الالكتروني في قطاع الطيران المدني، مركز المستقبل للابحاث والدراسات المتقدمة، الامارات العربية المتحدة، 25/5/2017، شبكة المعلومات الدولية – انترنيت –**https://futureuae.com/ar**

[40] د.عادل عبد الصادق، مصدر سبق ذكره، ص 31.

[41]الجنة الاقتصادية والاجتماعية لغربي آسيا الاسكوا، مصدر سبق ذكره، ص 73.

[42] المصدر نفسه، ص 3.

[43] جيمس اركلابر، ممصدر سبق ذكره، ص 3.

[44] هشام شير، التنافس على عسكرة الفضاء، صحيفة الخليج، السعودية 24/4/2014، شبكة المعلومات الدولية – انترنيت – **http://www.alkhaleej.ae**

[45]ايهاب خليفة، مصدر سبق ذكره، ص 114، ص 120.

[46] موقع نون بوست، حروب الفضاء الالكتروني، 2/2/2015، شبكة المعلومات الدولية –انترنيت –

http://www.noonpost.org/content

[47] سعد عطوة الزنط، الارهاب الالكتروني واعادة صياغة استراتيجيات الامن القومي، ورقة بحثية مقدمة الى مؤتمر الجرائم المستحدثة: كيفية اثباتها ومواجهتها للمدة 15–16 كانون الاول عام 2010، المركز القومي للبحوث الاجتماعية والجنائية، مصر، 2010، ص 20.

[48])**(David Bisson, a Cyber Study of the U.S National Security Strategy Report, 17 february 2015. https://www.tripwire.com/state-of-security/government/a-cyber-study-of-the-u-s-national-security-strategy-reports/**

[49] عادل عبد الصادق، الفضاء الالكتروني وتهديدات جديدة للامن القومي، قضايا استراتيجية، المركز العربي لابحاث الفضاء الالكتروني، مصر، 2011، ص 8، شبكة المعلومات الدولية – انترنيت –

http://www.accronline.com/print_article.aspx?id=8745

[50] ايهاب خليفة، مصدر سبق ذكره، ص ص 120–121.

[51] المصدر نفسه، ص 137.

[52] تحالف استخباراتي سمي بالعيون الخمسة يتكون من الولايات المتحدة الامريكية وكندا واستراليا والمملكة المتحدة ونيوزيلندا بموجب اتفاق (يو كيه يو اس ايه) التي تختص بمجال التعاون المشترك في مجال استخبارات الاشارة

[53] عادل عبدالصادق، الارهاب الالكتروني: القوة في العلاقات الدولية نمط جديد وتحديات مختلفة، مركز الدراسات السياسية والاستراتيجية، القاهرة، 2009، 364.

[54] عادل عبد الصادق، الفضاء الالكتروني وتهديدات جديدة للأمن القومي، مصدر سبق ذكره، ص 46.

[55] ايهاب خليفة، مصدر سبق ذكره، ص 149، ص 151.

[56] مصطفى تاهمي، البعد المعلوماتي في الحروب اللاتماثلية: دراسة التنظيمات الارهابية داعش انموذجاً، رسالة ماجستير غير منشورة، كلية الحقوق والعلوم السياسية، جامعة زيان عاشور الجلفة، الجزائر، 2017، ص 51.

[57] منى الاشقر جبور، السيبرانية هاجس العصر، المركز العربي للبحوث القانونية والقضائية، جامعة الدول العربية، بت، ص 75– 77.

[58] المصدر نفسه، ص ص 75–76.

[59] نورا بنداري عبدالحميد، دور وسائل التواصل الاجتماعي في تجنيد اعضاء التنظيمات الارهابية: دراسة حالة داعش، المركز الديمقراطي العربي، المانيا، 14/12/2017، ص 20، شبكة المعلومات الدولية – انترنيت– http://democraticac.de/

[60] سامر مؤيد عبداللطيف، الارهاب الالكتروني وسبل مواجهته، مجلة جامعة كربلاء العلمية، جامعة كربلاء، العراق، العدد 3، 2016، ص 61.

[61] عادل عبد الصادق، مصدر سبق ذكره، ص ص 28–31.

[62] إلين ناكاشيما، الجهود الامريكية لردع الهجمات الالكترونية ضد الولايات المتحدة غير مجدية، ترجمة موقع نون بوست، 20/3/2015، شبكة المعلومات الدولية – انترنيت–

https://www.noonpost.org/content/5921

[63] منى الاشقر جبور، مصدر سبق ذكره، ص ص 90–91.

[64] ستيوارت هانز ومالكولم شور وميلز جاكمان، الوجه المتقلب لامن الفضاء الالكتروني، isaca journal، المجلد 6، 2012، ص 3، شبكة المعلومات الدولية – انترنيت–

https://www.isaca.org

[65] مجلة المسلح، الجيش الامريكي يطلق برنامج التكليف المباشر لخبراء الامن السيبراني المدنيين، بيروت، 7/12/2017، شبكة المعلومات الدولية – انترنيت

http://www.almusallh.ly/ar/news–