تحديات الأمن في الفضاء السيبراني الأمريكي

م.د. علي محمد احنيف الرفيعي
كلية الحلة الجامعة-قسم القانون
dr.alialrufayee@gmail.com

الملخص

عمق الموضوع الذي انطلق منه البحث هو أن المقومات والمؤهلات السيبرانية التي تحظى بها الولايات المتحدة الامريكية، غدا العالم فيها يمثل على وفق المدرك الاستراتيجي مهم على النحو الذي جعل الولايات المتحدة الامريكية تعمل على أدارته في إطار مسمى هادف إلى استخدام موارد اغلب دول العالم وصياغة شراكات مع بلدانها باعتماد نهج الاحتواء والتفكيك وإعادة التركيب بما يتراكم وتحقيق الأهداف الأمريكية وهناك مناطق وأقاليم على سطح الأرض تستفرد بمقومات مؤاتيه لتنمية القوة الاستراتيجية يطلق عليها المناطق المحورية ، وتصنف منطقة الشرق الأوسط وجنوب شرق اسيا من ضمنها بحكم امكانياتها الفريدة في الامن السيبراني ومكانتها في المدرك الأمريكي .

كلمات مفتاحية: السيبراني، الفضاء ، الامن ، الاستراتيجية، المدرك

Security challenges in US cyberspace

Lecturer Dr. (Ali Mohammed Amneef), a teacher in the .Department of Law / Hilla University College

Abstract

The depth of the topic from which the research was launched is that the cyber components and qualifications that the United States of America possesses, tomorrow the world is represented according to the strategic perception important in the way that the United States of America works to manage it in a named framework aimed at using the resources of most countries of the world and forging partnerships with its countries By adopting the approach of containment, dismantling and recombination in

what accumulates and achieving the American goals. There are regions and regions on the surface of the earth that are unique in favor of the development of the strategic force called the pivotal areas, and the Middle East and Southeast Asia are classified, among them, by virtue of their unique capabilities in cybersecurity and their place in the American perception

Key words: cyber, space, security, strategy, perceptive

المُقدِّمة

تنبع أهمية دراسة الأمن السيبراني من المكانة المتميزة في الاستراتيجية الأمريكية، إذ أصبح أمراً ضرورياً لتعزيز المصالح القومية الأمريكية، لتحدد التكنولوجيات الرقمية عدد العمليات التي تصف عمل المجتمعات الحديثة التي تمتد من الاتصال إلى التمويل، ومن الكهرباء إلى النقل، ومن التجسس إلى الأمن القومي، والقدرة على التحكم في كيفية استخدام هذه التقنيات في الوقت الحاضر. كما أن هذه العناصر تؤثر على مسار تطورها في المستقبل، وهذا يعد أمر حيوي ومهم للأمن القومي.

حيث ترى الولايات المتحدة الامريكية ان أكبر وأكثر التهديدات التي يواجهها الأمن القومي الأمريكي في القرن الحادي والعشرين هي قضية الأمن الألكتروني، وهذه التهديدات متأتية من الصين، وكوريا الشمالية، وايران، اذ تعمل هذه الدول على سرقة معلومات التجارة الامريكية ومعلومات وأسرار عسكرية، مع توجيه هجمات الكترونية تعمل على تعطيل المنظومة الالكترونية لشبكات الدفاع والأستخبارات الامريكية.

وهنالك وجود تنافس دولي على ما يعرف بالذكاء الاصطناعي والقوة الألكترونية وبالتالي إستخدام هذه الإمكانيات في تنفيذ هجماتها وإحتمالات توجه الدولة المستهدفة الى إستخدامات التطور التكنولوجي والحصول عليها، وهذا ما اكدته ريفا جوجون كبيرة المحللين بمعهد سترانفورد الأمريكي للدراسات الأمنية والإستراتيجية بقولها "أن التنافس بين اقطاب العالم ودوله الصغيرة على أمتلاك أحدث برامجيات الذكاء الإصطناعي سيؤدي الى صراعات

جديدة بسبب تخوف الأطراف الدولية من بعضها" وبالتالي أن تقنية الذكاء الاصطناعي والحصول عليها أصبح تحدياً للدول الكبرى.

أهمية الدراسة: تكمن في حيوية الموضوع وهو أن الامن السيبراني في عالم اليوم وفي السياسة الدولية المعاصرة لها موقع وحضور اكثر من أي وقت. ومعرفة كيف ولماذا تتصادم او تتفاعل العلاقات الدولية وكيف يخطط الاخرون، ولاسيما الدول التي تتمتع بمقومات تكنلوجية وتقنية والتأثير والنفوذ كالولايات المتحدة الامريكية. كما وتكمن اهمية الدراسة في أنه، ومع مرور اكثر من ٧ سنوات على احداث ١١ سبتمبر، إلا ان مدلولاتها وتأثيراتها كانت أبلغ وأشد من ان يمسح في ذاكرة صناع السياسة الخارجية الأمريكية، لا بل انها ادت الى استمرارها في نهج الامن السيبراني اكثر فاكثر، وتتفنن في الستراتيجيات ربما لم تكتمل بعد ملامحها النهائية، مما يجعل الدراسة تدخل في باب التنظير والتطبيق والاهتمام بمواكبة الاحداث وافرازاتها، ومواكبة احدث النظريات المهمة في العلاقات الدولية ولاسيما نظرية الحرب الالكترونية والضربة الوقائية.

اشكالية الدراسة:

اخذ الأمن السيبراني يتراجع في السياسة الخارجية الامريكية في فترة ما بعد ١١/سبتمبر ٢٠٠١ ، حيث افرز نتائج وتداعيات سلبية على صعيدي الولايات المتحدة والعالم وذلك بسبب التغيرات المستمرة في هيكلية النظام الؤدولي.

وبناءً عليه، فالأمن السيبراني أخذ يرتبط مع السياسة العسكرية الأمريكية النابعة من استراتيجيتها الشاملة، برابطة أمن الموارد والأمن القومي الأمريكي نفسه، لتحقق لها ما لم تستطع تحقيقه من قبل تقسيم المنطقة وتحديد حدودها في إطار جديد وهذا مابرز بشكل جلي في تعاملات الولايات المتحدة مع ايران وكوريا الشمالية.

فرضية الدراسة:

ان الاستراتيجية الأمنية للولايات المتحدة الامريكية ليست استراتيجية مسالمة، فقد عمدت الى استخدام كافة الوسائل للحفاظ على امنها أكثر من أي دولة اخرى، حيث تعزز هذا المبدأ بعد احداث ١١/ سبتمبر ٢٠٠١ وما بعدها ان القوة المفرطة في السياسة الخارجية الامريكية، ليس الحل وأخذت انتهاج نوع أخر من القوة، واشدّ قوةً وعلى نحو انفرادي عبرت عنها أستراتيجية القوة السيبرانية.

المبحثُ الأوَّل: الامن السيبراني (المفهوم والفواعل)

هنالك مجموعة تعريفات لمفهوم الامن السيبراني بالاضافة الى الفواعل المؤثرة في المجتمع العالمي، ويترتب على وجودها نمط من النشاطات والفاعليات غير الرسمية، إذ لم يعد هناك مجال ودور لسيطرة رقابة الأجهزة الحكومية عليها، فقد تجاوزت الحدود الوطنية، وتعدَّت إلى ما فوق القومية، ورُبَّما أخذت أشكالاً متعددة، سيتم توضيحها من خلال مطلبين:

المطلب الأوَّل: المفهوم والفواعل الدولية

اولا_ مفهوم الامن السيبراني

يقول مختصون أن مصطلح الأمن السيبراني أتى من لفظ السيبر المنقول عن كلمة (Cyber) اللاتينية ومعناها (الفضاء المعلوماتي)، ويعني مصطلح الأمن السيبراني (أمن الفضاء المعلوماتي) من كل جوانبه، وهو عبارة عن تعبير شامل عن العالم الافتراضي الذي يحوي كل ما يتعلق باستخدامات وآليات وتطبيقات وتجهيزات تقنية المعلومات والحاسب الآلي، والترابط فيما بينها من خلال شبكات الحاسب والاتصالات والانترنت[1].

ويعبر الأمن السيبراني عن مصفوفة من الأدوات التنظيمية والتقنية والإجرائية، والممارسات الهادفة إلى حماية الحواسيب والشبكات وما بداخلها من بيانات من

الاختراقات أو التلف أو التغيير أو تعطل الوصول للمعلومات أو الخدمات، ويعد توجها عالميا سواء على مستوى الدول أو حتى المنظمات الحكومية أو الشركات.

والأمن السيبراني هو عبارة عن مجموع الوسائل التقنية والتنظيمية والادارية التي يتم استخدامها لمنع الاستخدام الغير مصرح به وسوء الاستغلال واستعادة المعلومات الالكترونية ونظم الاتصالات والمعلومات التي تحتويها وذلك بهدف ضمان توافر واستمرارية عمل نظم المعلومات وتعزيز حماية وسرية وخصوصية البيانات الشخصية واتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين من المخاطر في الفضاء السيبراني. والأمن السيبراني هو سلاح استراتيجي بيد الحكومات والإفراد لا سيما أن الحرب السيبرانية أصبحت جزءاً لا يتجزأ من التكتيكات الحديثة للحروب والهجمات بين الدول[٢].

ثانيا:الشركات المتعدَّدة الجنـيَّة:

تمتلك بعض شركات التكنولوجيا موارد للقوة تفوق قدره بعض الدول، ولا تنقصها سوى شرعية ممارسة القوة التي مازالت حكراً على بعض الدول، فخوادم الشركات مثل: جوجل، وفيسبوك، وميكروسوفت، تسمح لها بامتلاك قواعد البيانات العملاقة التي من خلالها تكتشف وتستغل الأسواق، وتؤثر مباشرة في اقتصاديات الدول، وفي ثقافة المجتمعات.

فعلى سبيل المثال، يتقدم محرك بحث في الصين شركة (بايدوانك) على محرك البحث الأمريكي العملاق (جوجل)، إذ يسيطر على أكثر من (٦٠%) من سوق محركات البحث في الصين. وقد تستغل هذه الشركات امتيازاتها في النشاط السيبراني المتمثل بـ: الهجمات السيبرانية، وتهديد البُنى التحتية للولايات المتحدة الأمريكية[٣].

دخول الشركات المتعددة الجنسيات معترك الامن السيبراني كان ضرورة ملحة لأغلب الدول كون التطور الحاصل على كافة الاصعدة والمستويات غير من مفهوم الحرب والهيمنة واصبحت هذه الشركات رأس حربة في الصراع الدولي ونخص منها التقنية المتطورة

بالاضافة اللى ذلك اخذت هذه الشركات تتداخل مع الدول من خلال بناء شراكات استراتيجية مؤثرة وفاعلة على الصعيد الأمني والدفاعي والهجومي وهذا ماحصل فعلا بين (الولايات المتحدة الامريكية وكوريا الشمالية وأيران) من خلال الهجمات الألكترونية على المنشأات النووية.

ثالثا: حرية الإنترنت وحقوق الإنسان

يشكل الإنترنت التهديد الحقيقي والفوري للدول الإستبدادية، فاستخدام التكنولوجيات السيبرانية يدعم حرية الإنسان ويتبنى إجراءات قوية وفعالة لتعزيز قيم الليبرالية الديمقراطية في الفضاء السيبراني وفي هذا المجال ينبغي على الولايات المتحدة الأمريكية[٤].

١- إستخدام جميع العناصر الدبلوماسية والإقتصادية الأمريكية التي تثني الدول الإستبدادية عن ممارسة الرقابة والقمع.

٢- توسيع كبير في وسائل الأعلام الإجتماعية الأمريكية وغيرها من جهود الإتصالات الرقمية للتأثير بالتواصل الفعال وتعزيز الحريات الأساسية على الإنترنت.

٣- إضفاء الطابع الرسمي وتوسيع وتعزيز تحالف حرية الإنترنت.

٤- تشجيع زيادة الوصول إلى الإنترنت من خلال سياسات التسويق.

٥- تعزيز دور منظمات المجتمع المدني في الدراسة ودعم حرية الإنترنت.

٦- توسيع وتكثيف ودعم كل من القطاعين العام والخاص للمشاركة في المحافل الدولية حيث تم تعيين سياسات الإنترنت.

رابعا: التجارة الدولية والتجارة الرقمية

نجاح الوصول التجاري الأمريكي إلى نظام الإنترنت، يعد مصدرا إستراتيجيا هائلا ومميزا للحفاظ على تكافؤ فرص التجارة الرقمية –التي تعزز المنافسة– الأمر الحيوي أن يكون ذلك للمصلحة الوطنية الأمريكية[٥].

١- تطوير وتنفيذ محكمة كاملة التي تهدف إلى تغيير سلوك الصين فيما يتعلق بالتجارة

الرقمية وسرقة الملكية الفكرية.

٢- إتخاذ إجراءات ملموسة فعالة ضد السرقة على الإنترنت.

٢- من الواضح أن الولايات المتحدة سترد على التنفيذ العدواني المفرط لقانون الأمن القومي للدول المنافسة.

٤- مقاضاة الرقابة للدول المعادية من خلال منظمة التجارة العالمية.

٥- السعي بقوة إلى التفاوض على اتفاق متعدد الأطراف مع الإتحاد الأوروبي.

٦- دمج الحماية ضد مشاركة الدولة في سرقة الإنترنت في الإتفاقات المتعددة الأطراف.

٧- تشجيع خفض تنظيم شركات الإنترنت.

٨- مواصلة تطوير وتعزيز سياسة التجارة الرقمية.

٩- لا يطلب من الشركات الأميركية إنشاء بوابات خلفية في برامج التشفير والإتصالات.

١٠- تعزيز أولويات التجارة الرقمية بواسطة إتفاقيات تجارية متعدد الأطراف.

١١- التأكد من ضوابط التصدير بموجب قانون الولايات المتحدة وبموجب ترتيبات (وسينار) متعددة الأطراف لا تضع الشركات الأمريكية بشكل غير ضروري في المنافسة المساوية.

المطلب الثاني: الأرهاب السيبراني

ظهر مصطلح (الإرهاب السيبراني) في الآونة الأخيرة، وعُرَّف بأنه: "استخدام تكنولوجيا المعلومات بواسطة الجماعات الإرهابية، أو الأفراد لتحقيق أهدافهم. وقد يشمل ذلك استخدام تقنية المعلومات للتنظيم، وتنفيذ الهجمات ضدَّ الشبكات وأنظمة الكمبيوتر والاتصالات السلكية واللاسلكية، والبُنى التحتية، وتبادل المعلومات، وأداء التهديد السيبراني"[٦].

كما عَرَّفتْ المباحث الفيدرالية الأمريكية الإرهاب السيبراني بأنه: "كل هجوم مخطط له بدافع سياسي ضدَّ المعلومات، وأنظمة الحاسب الآلي، وبرامج الحاسوب والبيانات، مما يؤدي إلى العنف ضدَّ أهداف غير حربية من قِبَلِ مجموعات وطنية فرعية، أو عملاء متخفي. ويستخدم الإرهابيون الأنترنيت لأغراضٍ عدَّة، منها"[٧]:

١- الدعاية: وتتخذ شكل اتصالات عبر وسائط متعددة تحمل تعاليم إديولوجية، ويتم
عن طريقها التجنيد والتحريض.

٢- التمويل: ويُقسَّم إلى أربع فئاتٍ، وهي: الطلب المباشر، والتجارة الإلكترونية، واستغلال أدوات الدفع عبر الأنترنيت، واستغلال المنظمات الخيرية.

٣- التدريب: يستخدم الإرهابيون الأنترنيت كساحة تدريبٍ بديلةٍ للإرهابيين، وهناك مجموعة متزايدة من الوسائط التي توفر منصاتٍ بصورة كُتيبات إلكترونية، ومقاطع صوت وفيديوهات.

٤- التخطيط: إذ ينطوي على الاتصال عن بُعدٍ بين عدَّة أطراف.

٥- التنفيذ: يمكن أن يبث الإرهاب عمليات بشكل تهديدات صريحة باستخدام العنف.

وقد قال بان كي مون (الأمين العام للأمم المتحدة السابق): "إن الأنترنيت هو خير مثال، إذ يوضح كيف يمكن للإرهابيين أن يمارسوا نشاطهم على نحوٍ عابرٍ للحدود حقاً وتصدياً. لذلك، ينبغي للدول أن تفكر وتعمل على نحوٍ عابر للحدود أيضاً"[٨].

كما ذكر مدير وكالة المخابرات المركزية CIA (جورج تينيت) في بيانه عام ٢٠٠٠، حول التهديدات الأمنية العالمية، بما اسماهم بـــ(الجماعات الإرهابية) لدعم عملياتهم باستخدام الملفات المحوسبة، ورسائل البريد الإلكتروني والتشفير، إذ استخدم الإرهابي الميداني (رمزي يوسف) المخطط للهجوم على مركز التجارة العالمي في نيويورك، الملفات المُشفرة في

جهاز الكمبيوتر المحمولة تخزين خطط مفصلة لتدمير طائرات في الولايات المتحدة. وقد تابعت بعد ذلك المجموعات الإرهابية نشاطها.

وقدَّم مركز الاتصالات الاستراتيجية لمكافحة الإرهاب التابع لوزارة الخارجية في الولايات المتحدة في آيار عام ٢٠١٢، أن المركز قد ردَّ في غضون ٤٨ ساعة، على لافتات إعلانية تروج للعنف بداعي التطرف، نشرها تنظيم القاعدة في شبه الجزيرة العربية على مختلف المواقع. كما أن المركز يستخدم منصات إعلامية مثل: فيسبوك، ويوتيوب، وذلك لبث رسائله المعنوية على شكل خطابات مضادة(٩).

ولطالما مثَّل الإرهاب بكل اشكاله إضافة مصدر تهديد وقلق للولايات المتحدة. ولذا، تعمل الولايات المتحدة على تعزيز دفاعاتها السيبرانية.

المطلب الثالث: الأفرادُ والجرائم السيبرانيَّة

شهدت فترة ثمانينيات القرن الماضي أولى حملات القبض على قراصنة الحاسوب، بعد أن قامت جماعة منهم باختراق أكثر من (٦٠) جهاز بولاية (ميلوا كي) الأمريكية، وتلا هذه المرحلة سن عدد من القوانين للنشاط السيبرانية ومعاقبة مرتكبي جرائم القرصنة، ولم يقف إلى هذا الحد، فقد تطور في عقد التسعينيات ليشمل النطاق العالمي(١٠).

وقد ظهر مجتمع القرصنة، وصدرت العديد من الدورات المتخصصة بالقرصنة، مثل: مجلة (هاكر كوارتري) التي كان أغلبها يعكس النصائح والإرشادات لتعليم القرصنة (الهاكر) للمبتدئين، وقد توسعت خدمات الاختراق لتشمل أجهزة الدفاع والجيش وإدارة العدل الأمريكية، ووكالة ناسا، ومكتب التحقيقات الفدرالي **FBI**.

وبناءً على تلك التطورات، فقد انتقل الناس من العالم الواقعي إلى العالم الافتراضي، وكذلك انتقلت الجريمة إلى الفضاء السيبراني الذي ينتج أنواع جديدة من الجريمة، إذ تُسمى بـــ(الجريمة السيبرانية **Cyber crime**). كما أنَّها مكَّنت مجرمي الفضاء السيبراني من

تصفح الأنترنت، وارتكاب الجرائم مثل: القرصنة، والاحتيال، والتخريب للكمبيوتر، والاتجار بالمعلومات، والتعامل في معلومات العدالة والمواد الإباحية.

وبحسب اللجنة الأوروبية، فإن مصطلح (الجريمة السيبرانية) يضم كل المظاهر التقليدية للجريمة، مثل: الغش، وتزييف المعلومات، ونشر مواد إلكترونية ذات محتوى مخل بالأخلاق، أو نشر دعوى للفتن الطائفية. كما عَرَّفتْ وزارة العدل في الولايات المتحدة الأمريكية (الجريمة السيبرانية) بأنها: جريمة لفاعلها معرفة فنية بتقنية الحاسبات، وتمكنه من ارتكابها. وذهب الاتجاه العالمي الجديد إلى تقسيم هذه الجرائم إلى:

١- الجرائم التي تستهدف عناصر المحتويات والنظم.

٢- الجرائم المرتبطة بالكمبيوتر (التزوير، والاحتيال).

٣- الجرائم المرتبطة بالمحتوى (الأفعال الإباحية والأخلاقية).

٤- الجرائم المرتبطة بحقوق المؤلف، والحقوق المجاورة..

كما يمكن تقسيم (الهاكرز) بمفهومه السيئ إلى فريقين: "الهواة، ويعتمدون على برامج التجسس الجاهزة والمتاحة[١١]. أمَّا المحترفون، فهم الفريق الأخطر، لأنهم يعملون على استخدام البرامج الجاهزة المتطورة، وكذلك يعتدون على خبرتهم في لغات البرمجة والتشغيل والتصميم والتحليل وتشغيل البرامج بسرعة"[١٢].

وقد أوضح التقرير السنوي الثامن لمكتب التحقيقات الفدرالي الأمريكي الصادر عام ٢٠٠٣، بعنوان: (جرائم الحاسوب)، أن أكثر خسائر المؤسسات في الولايات المتحدة الأمريكية تأتي من الاستيلاء على المعلومات، إذ تكبَّدت خلال هذا العام خسائر تتعدى الـــ(٧٠) مليون دولار، ويأتي في المركز الثاني، نشاط تعطيل نظم المعلومات محققاً بذلك خسائر تتجاوز الـــ(٦٥) ونصف مليون دولار[١٣].

كما ذكر تقرير مكتب التحقيقات الفدرالي الأمريكي (FBI) التطور السنوي للخسائر المادية للشركات الأمريكية، من الجرائم الالكترونية في الأعوام: من (٢٠٠٠ إلى ٢٠٠٣) ، إذ عزى جنوح أغلب الجرائم إلى الانخفاض في حجم الخسائر المادية النا[١٤]. ناجمة

عنها حوالي (١٨) مليون دولار عام(٢٠٠٢)، وما يقارب من (٦٥) مليون دولار عام (٢٠٠٣).

وتشير مجلة (لوس أنجلس تايمز) في عددها الصادر في ٢٢ مارس– عام(٢٠٠٠)، إلى أن خسارة الشركات الأمريكية وحدها من جراء الممارسات التي تتعرض لها، والتي تندرج تحت بند الجريمة السيبرانية تُقدر بحوالي (١٠) مليار دولار سنوياً.

وللتأكيد على جانب قد تغفله الكثير من مؤسسات الأعمال، فأن نسبة (٤٢ %) من تلك الجرائم تحدث من خارج المؤسسة، وعن طريق شبكة الأنترنت، بينما تشكل نسبة الإباحية (٣٨%) من تلك الخسائر، من ممارسات داخل المؤسسات.

كما أفاد تقرير للبيت الأبيض بأن (القرصنة السيبرانية) كلفت الولايات المتحدة بين (٥٧) مليار، و(١٠٩) مليار دولار عام (٢٠١٦)، إذ أشار التقرير إلى عمليات القرصنة التي استهدفت مؤسسات خاصة وعامة، ومنها: قطع الخدمة، وانتهاك البيانات، وسرقة الحقوق الفكرية. ونشط (الهاكرز) في تسعينيات القرن الماضي، وكان أشهرهم (كيفن منتنك) الذي قام بسرقات كبرى التي شغلت مكتب التحقيقات الفدرالي في وقتها، إذ اخترق شبكة الكمبيوترات الخاصة **equipment digital company**.

وقد عقب هذه الحالة، نجد أن هناك عشرات (الهاكرز)، من المراهقين الذين اخترقوا شبكات مهمة، مثل: "هواتف الطوارئ الأمريكية، والبنوك، والشركات، وأجهزة ناسا، وبطاقات الائتمان (الفيزا كارد)، و(الماستر كارد)" [١٥].

وشغلت الإدارة الأمريكية قضية (**PHISH PHRY**)، إذ تم الاستيلاء على أموال مواطنين أمريكيين. وبدأت عملية (القرصنة السيبرانية) منذ عام (٢٠٠٧)، فقام مجموعة من الشباب المصريين بالاستعانة بمجموعة من الأمريكيين في بعض الولايات: (كاليفورنيا، ونيفادا، ونورث كارولينا) بإنشاء صفحات وهمية مماثلة تماماً لصفحات دخول مواقع حسابات بعض البنوك الأمريكية، مثل: (**bank of America**)، وبنك (**AOL**)، وبنك (**wels fargo**).

وبفضل تعاون مصري– أمريكي، فقد تم من خلاله القبض على الشبكة، وهو الأول من نوعه في إطار ملاحقة الجرائم السيبرانية[١٦].

وفي بيان صحفي نُشر في ٣١ آيار(٢٠١٧)، من قبل مكتب المدعي العام في وزارة العدل الأمريكية في المنطقة الشمالية وجورجيا، ظهرت تفاصيل حول كيفية استخدام أربعة رجال للأسواق المُشفرة على (الأنترنت المظلم)*، لبيع الأسلحة النارية لبلدان من حول العالم مستخدمة الاسمين المستعارين: (cherry flavor)، و(world wide arms).

وعلى الرغم من أن البدائل التي تصبح أكثر شهرة (Altcoin) [١٧]. إذ يشار إلى أن انتشار (الجريمة السيبرانية) تزداد بشكل ملحوظ بالعالم مع ارتفاع الأجهزة الإلكترونية، إلَّا أنه يسبب تحديات جديدة للأمن العالمي بشكلٍ عام، وأن الولايات المتحدة خاصة[١٨].

في ختام هذا المبحث توصلنا الى نتيجة حتمية ان الامن السيبراني لاينحصر على الدول فقط وأنما هنالك فواعل من غير الدول لها اليد العليا في التأثير في هذا الملف وغالبا مايتم الاستعانة بها من قبل بعض الدول لتحقيق اهداف استراتيجية للدوول انفسها من خلال التقنيات والربط الألكتروني العالمي.

المبحث الثاني: الاتفاقيات الدَّولية

تعمل الاتفاقيات الدولية على الحدِّ من الأنشطة السيبرانية: كعمليات التجسس، والمراقبة وغيراها. وقد دخلت الولايات المتحدة طرفاً في هذا الاتفاقيات، إذ حدَّت من عملياتها السيبرانية، ويمكن ذكر أهم هذه الاتفاقيات من خلال المطالب الآتية:

المطلب الأوَّل: تحالف خمس عيون Five eyes

وهو عبارة عن مجموعة من وكالات استخباراتية لخمسٍ من الدول تعمل معاً، وتتبادل المعلومات، وهي: (استراليا، نيوزلندا، المملكة المتحدة، كندا، الولايات المتحدة) [١٩]. وقد بدء هذا التحالف باتفاقية (Bursa)، إذ تم توقيعها في مارس (١٩٤٦)، وانضمت إليها كلاً: (بريطانيا، وكندا، واستراليا، ونيوزلندا) في عام(١٩٥٦).

وتطورت الاتفاقية الأصلية إلى هذا التحالف، وتذكر مسودة (٢٠٠٥)بتوجيهات وكالة الأمن القومي (NSA): إن الشركاء يتحفظون بالحق في إجراء عمليات استخباراتية ضد مواطنين بعضهم البعض عندما يكون يصب ذلك في مصلحة الأمة.

وفي يوليو عام (٢٠١٧)، رُفعت الخصوصية الدولية، إذ أُقيمت دعوى قضائية ضدَّ وكالة الأمن القومي الأمريكي (NSA)، ومكتب مدير الاستخبارات الوطنية، ووزارة الخارجية، والإدارة الوطنية للمحفوظات، والسجلات، من قبل الدول الأعضاء في التحالف، وذلك بسبب عدم الالتزام بتحالف الخمس عيون، وبموجب قانون حرية المعلومات[٢٠].

وبموجب هذه الدعوى القضائية، أُتهمت الولايات المتحدة بانتهاك الخصوصية، ومخالفة بنود الاتفاقية التي تلزم بعدم تجسس الأطراف على مواطني بعضهم البعض.

المطلب الثاني: اتفاقية مجلس أوروبا المتعلَّقة بجرائم الفضاء السيبرانية

وهي اتفاقية متعددة الاطراف، وملزمة قانوناً وقعت في نوفمبر (٢٠٠١)، إذ دخلت حيز التنفيذ في يوليو(٢٠٠٤). وقد وقعت عليها (٤٦) دولة، بما في ذلك: كندا، واليابان، وجنوب إفريقيا، والولايات المتحدة الأمريكية، وصُدَّق عليها من قِبل (٢٦) دولة فقط، ولم تصدَّق عليها روسيا.

وتقتضي اتفاقية المجلس الأوروبي أن تلتزم أطرافها بالتشريعات، لتلزم مقدمي خدمات الانترنت بحفظ بيانات معينة تُخزَّن على خوادمها لمدة تصل إلى تسعين يوم قابلة للتجديد، إذا طلب منهم ذلك مسؤول انقاذ القانون. ويُعدُّ هذا الأمر أمراً بالغ الأهمية، نظراً للصيغة المؤقتة للبيانات الإلكترونية. كما أن الإجراءات التقليدية للمساعدة القانونية المتبادلة غالباً ما تستغرق وقتاً طويلاً في القضايا العابرة للحدود الوطنية[٢١].

المطلب الثالث: دليل تالين (Tallin manual)

تم إبرام صك قانوني عام ٢٠١٣، وهو دليل تالين الذي أعده مجموعة من خبراء القانون الدولي بدعوة من حلف الشمال الأطلسي (NATO)، قصد دراسة مدى إمكانية

تطبيق قواعد القانون الدولي الإنساني على الحروب السيبرانية، وذلك إثر الهجوم السيبراني الشامل الذي شنته روسيا على استونيا عام(٢٠٠٧) [٢٢].

ويحتوي دليل تالين على (٩٥) قاعدة، إذ تتمثل تحدياته الرئيسة في ضمان توجيه الهجمات ضد الأهداف العسكرية فقط، وتوخي الحذر لحقن دماء المدنيين والبُنية التحتية الضرورية. وكُلُّ ذلك جاء نتيجةً لوجود فضاء سيبراني واحد، تتقاسمه القوات المسلحة والجيوش السيبرانية مع باقي المستخدمين المدنيين[٢٣].

المطلب الرابع: واقعية ومستقبل الامن السيبراني

اولا_ التحديات السيبرانية التي واجهتها الولايات المتحدة الامريكية وسيتم توضيحها وفق الدول الأتي:

مخطط رقم: (١)

الحادث	السنة التي بدأ فيها	التأثير	تحديد المصدر في النظام العام
١- مختبر لورنس بيركلي الوطني	١٩٨٦	اختراعات بيانات حساسة واستخراجها	محاكمه جنائية من المانيا الغربية ١٩٩٠
٢- هجمات القطع الموزع للخدمة على المصارف الأمريكية	٢٠١٢	هجمات القطع الموزع للخدمة على اكثر من (٤٦) من أبرز المؤسسات المالية في U . S . A	اتهام الجهات الفاعلة الحكومية الإيرانية في آذار ٢٠١٦
٣- حساب وكالة اسوشيتدبرس ٢٠١٣ Associate Press على تويتر	٢٠١٣	قرصنة حساب وكالة اسوشيتدبرس على تويتر ونشر تغريده كاذبة على هجوم على البيت الأبيض مما أدى إلى هبوط حاد في أسعار الأسهم	تبني الجيش السوري الإلكتروني Syrian electronic army
٤- البيت الأبيض ووزارة الخارجية	٢٠١٤	اختراق كبير لأنظمة الكومبيوتر غير السرية	عزي بدرجه كبيره إلى روسيا ولكن لم تحدد الحكومة الأمريكية رسمياً المصدر
٥- سوني بكتشرز Sony pictures	٢٠١٤	سرقة بيانات حساسة وتسريبها تعطيل كبير للأعمال	عزاها الرئيس الأمريكي الى جهات فاعلة حكومية كورية شمالية في ديسمبر ٢٠١٤

٦- غيت هاب Git Hub	٢٠١٥	هجوم قطع موزع للخدمة كبير و متواصل على مواقع التعاون لتطوير البرمجيات	عزته الشركات الخاصة والباحثين بدرجة كبيرة إلى جهات فاعلة حكومية صينيه
٧- المكتب الامريكي لإدارة شؤون الموظفين	٢٠١٥	استخراج ٢١،٥ مليون سجل خاص بموظفي حكومة U . S . A	عزي بدرجة كبيرة إلى الصين علما ان الحكومة الامريكية لم تحدد رسميا المصدر
٨- اللجنة الديمقراطية الوطنية DNC	٢٠١٦	استخراج وثائق خاصة باللجنة الديمقراطية الوطنية والحملة الانتخابية ونشرها تدخل بالانتخابات الرئاسية الامريكية عام ٢٠١٦	عزته شركة كراود ستريك Crowed Strike حزيران ٢٠١٦ وتقرير مكتب مدير الاستخبارات القومية الأمريكي يناير ٢٠١٧ إلى جهات فاعلة حكومية روسية
٩- دين DYN	٢٠١٦	هجوم قطع موزع للخدمة باستخدام شبكة مصابة من أجهزة أنترنت الأشياء أستهدف مزود نظام اسماء النطاقات دين وعطل عدداً كبيراً من المواقع الإلكترونية	لم يحدد المصدر رسمياً عزي بدرجة كبيرة إلى منظمة قرصنة ناشطة مثل: انونيموس، أو نيوورلد هاكرز، أو سباين سكواد
١٠- وانا كراي عالمياً	٢٠١٧	هجوم برنامج فدية طال قطاعي الرعاية الصحية والنقل والبنية التحتية للاتصالات من جميع أنحاء العالم.	لم يحدد المصدر رسميا ربطته بعض الشركات الخاصة بمجموعة لازاروس ألقت روسيا باللائحة على U . S . A لابتكارها برمجية exploit القادرة على تفعيل برنامج واناكراي

ينظر: فيكتور ماير شونبرغر وديبورا هيرلي، الحكم في عالم يتجه نحو العولمة، ط١، تحرير جوزيف س. ناي وجون د. دونهايو، العبيكان، الرياض،٢٠٠٢، ص ص٢١٢-٢١٧.

ثانيا_ مستقبل الامن السيبراني الامريكي

بعد أشهر من الانتقادات لإدارة الرئيس الأمريكي (ترامب)، لافتقارها إلى مقاربة فيدرالية متماسكة للأمن السيبراني، كشف البيت الأبيض عن (الاستراتيجية السيبرانية القومية) في العشرين من سبتمبر الماضي، بعد أن أخفقت سياسات الإدارات الأمريكية السابقة للأمن السيبراني في منع تعرض المؤسسات الأمريكية المدنية والعسكرية – على حد سواء – لتهديدات من خصومها ومنافسيها، لا سيما بعد التدخل الروسي، حسب كثير من التقارير الاستخباراتية، في الانتخابات الرئاسية الأمريكية التي أجريت في الثامن من نوفمبر (٢٠١٦)، وتوقعاتها بأن يكون هناك تدخل آخر في انتخابات التجديد النصفي للكونجرس المقرر لها في نوفمبر من هذا العام[٢٤].

يؤدي ضعف المؤسسات والوكالات الأمريكية لصون الأمن السيبراني للولايات المتحدة إلى تعرّضها للمزيد من الحوادث الأمنية، والهجمات السيبرانية التي قد تمكّن المنافسين والخصوم من الوصول إلى معلومات أمريكية حساسة، أو الإفصاح عنها، أو تعديلها، أو إتلافها، الأمر الذي يهدد الأمن القومي للولايات المتحدة، ورفاهيتها الاقتصادية، والصحة والسلامة العامة للأمريكيين[٢٥].

وتعد الاستراتيجية السيبرانية الجديدة، وفقاً لبيان مجلس الأمن القومي عنها، أول استراتيجية مفصلة للولايات المتحدة منذ عام (٢٠٠٣) عندما أصدرت إدارة الرئيس الأمريكي الأسبق (جورج دبليو بوش) استراتيجيتها القومية لحماية الفضاء السيبراني. وتحدد استراتيجية إدارة (ترامب) الأولويات الحاسمة لصون المصالح الأمريكية في الفضاء السيبراني، انطلاقاً من قناعة بأن الولايات المتحدة هي التي أنشأت الإنترنت، وأن عليها أن تحافظ على دورها المهيمن في تحديد الفضاء السيبراني، وتشكيله، وحمايته[٢٦]. ومع انخراط منافسي وخصوم الولايات المتحدة (الصين، وروسيا، وكوريا الشمالية، وإيران) في التجسس الاقتصادي، وأنشطة سيبرانية معادية، والنظر إلى الفضاء السيبراني على أنه ساحة يمكن فيها تحييد القوة الاقتصادية، والعسكرية، والسياسية الأمريكية الساحقة، وتقويض الديمقراطية

الأمريكية، تجيز الاستراتيجية العمليات السيبرانية الهجومية ضدهم، تماشياً مع سياسة أمريكية جديدة تخفف من قواعد استخدام الأسلحة السيبرانية لحماية البلاد من هجمات سيبرانية لا تهدد فقط الديمقراطية الأمريكية، ولكن المؤسسات الاقتصادية والأمنية الأمريكية، والتي ستؤثر في التحليل الأخير على قيادة الولايات المتحدة للنظام الدولي الذي أسسته في أعقاب الحرب العالمية الثانية، والذي تنفرد بالهيمنة عليه في أعقاب نهاية الحرب الباردة، وانهيار الاتحاد السوفييتي السابق مع نهاية ثمانينات القرن المنصرم(٢٧).

وتعمل الاستراتيجية السيبرانية لإدارة (ترامب) على الحد من القيود التي وضعتها إدارة الرئيس الأمريكي السابق (أوباما) المقيّدة للقيام بهجمات سيبرانية على خصوم ومنافسي الولايات المتحدة. وفي المؤتمر الصحفي للكشف عن الاستراتيجية قال مستشار الأمن القومي (جون بولتون)، إن "أيدينا ليست مكتوفة كما كانت في عهد إدارة أوباما". وأضاف أن الاستراتيجية تتضمن توجيهاً رئاسياً جديداً حل محل التوجيه الصادر في عهد الإدارة السابقة يسمح بأن تقوم المؤسسة العسكرية الأمريكية والوكالات الأخرى بعمليات سيبرانية، تهدف لحماية أنظمة وشبكات الولايات المتحدة الحرجة التي يؤثر استهدافها في القوة والمكانة الأمريكية الدولية(٢٨).

وتتفق تصريحات (بولتون) مع توجه الإدارة الأمريكية لتبني سياسة ردع سيبرانية أكثر هجومية مقارنة بمواقف الإدارات الأمريكية السابقة، وسعيها لإنشاء هياكل الردع التي ستثبت للخصوم والمنافسين أن تكلفة استهدافهم وتحديهم لمصادر القوة والنفوذ الأمريكي يكون مكلفاً أكثر مما يتحملونه.

وتأتي الاستراتيجية السيبرانية الجديدة للولايات المتحدة في إطار مساعي الرئيس الأمريكي لإنشاء فرع سادس للجيش الأمريكي يركز على الفضاء، ويُحقق هيمنة أمريكية عليه، بعد أن حقق أعداؤها والقوى المنافسة لها تفوقاً عليها في الفضاء الخارجي، ما يمثل تهديداً للتفوق العسكري الأمريكي. كما أنها صدرت بعد يومين من إعلان وزارة الدفاع الأمريكية (البنتاجون) في الثامن عشر من سبتمبر الماضي عن استراتيجيتها السيبرانية التي تكشف عن

دور قوي للوزارة في حماية الانتخابات، والدفاع عن البنية التحتية الأمريكية من هجمات سيبرانية، وتنسيق وتبادل المعلومات حول التهديدات السيبرانية مع القطاع الخاص الأمريكي[٢٩].

وقد أصدرت وزارة الدفاع والبيت الأبيض استراتيجيتهما لتعزيز الأمن السيبراني بعد تقرير صادم لمكتب المحاسبة الحكومي الأمريكي في سبتمبر من العام الجاري عن حالة الأمن السيبراني داخل الولايات المتحدة، وانتقد غياب استراتيجية أمريكية شاملة للأمن السيبراني، ما قد يجعل الوكالات الفيدرالية، والبنية التحتية الحيوية للولايات المتحدة، بما في ذلك الطاقة، وأنظمة النقل والاتصالات، والخدمات المالية، معرضة للخطر. وتزداد مخاطر الأمن السيبراني هذه مع تنامي التهديدات الأمنية وتعقّدها.

وتقوم استراتيجية الإدارة الجديدة لتعزيز الأمن السيبراني الأمريكية على أربع ركائز رئيسية، هي على النحو الآتي[٣٠]:

أولا– تعزيز الأمن القومي الأمريكي، من خلال تبادل المعلومات عبر الوكالات الفيدرالية، لحماية شبكات الكمبيوتر الاتحادية، وتأمين البنية التحتية الحيوية للبلاد، وذلك من خلال إعطاء وزارة الأمن الوطني مزيداً من الصلاحيات لرقابة جهود الأمن السيبراني المدنية، ومكافحة الجرائم السيبرانية من خلال التعاون مع الدول الأخرى لتعقب منفذيها.

ثانياً– تعزيز الاقتصاد الأمريكي الرقمي، بتشجيع الابتكار في قطاع التكنولوجيا، وذلك من خلال العمل مع شركات التكنولوجيا لتعزيز اختبارات الأمن السيبراني في المنتجات الجديدة. بالإضافة إلى بناء قوة عاملة حكومية في مجال الأمن السيبراني من خلال توظيف المتخصصين من ذوي الكفاءات في مجال الأمن السيبراني في المؤسسات والوكالات الأمريكية.

ثالثاً– مكافحة التهديدات السيبرانية، من خلال استخدام كافة أدوات القوة الأمريكية لردع أي هجمات سيبرانية، وتعزيز المعايير الدولية في الفضاء السيبراني.

رابعاً– الدعوة إلى حرية الإنترنت في جميع أنحاء العالم، وتزويد حلفاء الولايات المتحدة بقدرات سيبرانية، للتعامل مع التهديدات السيبرانية التي تستهدف المصالح المشتركة.

وعلى الرغم من أن الاستراتيجية التي جاءت في أربعين صفحة لم تحتوي إلا على القليل من المقترحات الجديدة، حيث إن معظمها مستمد من سياسات الإدارات السابقة، فإنها لقيت ترحيباً من بعض السياسيين، والمشرعين، وخبراء الأمن السيبراني، لأنها تسمح للولايات المتحدة باتباع نهج أكثر هجومية ضد الهجمات السيبرانية التي تتعرض لها، وبالتصدي العاجل والوقائي لأي هجوم وشيك. كما أنها تحقق التوازن الجيد بين الإجراءات الدفاعية وفرض عواقب مكلفة على منفذي الهجمات السيبرانية.

وعلى الجانب الآخر تعرضت الاستراتيجية لبعض الانتقادات، لأن البيت الأبيض لم يقدم إلا القليل من التفاصيل حول كيفية تطبيقها بالفعل على أرض الواقع.

الخاتمة

إن التأمل الفكري والواقعي يظهر في المحصلة النهائية، وأن طبيعة الأشياء لا تتغيَّر في إطارها العام وشكلها النهائي الحاسم، وإنما تتغيَّر طريقة التكيُّف والتعبير عنها وتطبيقها على أرض الواقع.

كما أنها تنسحب على مفردات السياسية الدولية ما شاع منها، وما اقتصر على طرف دون آخر، ومن مسلمات القول: إن الجوانب الإلكترونية بين أعضاء المجتمع الدولي تزداد أهمية باضطراد نتيجة التزايد الواقعي لحجم التأثير، والضغط المتبادل الذي يمارسه الأمن السيبراني في استقرار وديمومة أقطاب المجتمع الدولي.

وهناك الكثير من المتغيِّرات التي حكمت وأثَّرت في الاستراتيجية الشاملة الأمريكية، إذ لم تزل منذ ما يربو على القرن، وهي هي مصادر السبرانية التي شكَّلت الحراك الأمريكي في العالم، لكون السبرانية غدت مستقبلاً استراتيجياً واقتصادياً، إذ لم يكن ذلك المتغيَّر، بل كان باستمرار في معادلات القوى في المنطقة.

ولا جدال في أن تحديات الأمن السيبراني غدت تمثِّل أهميةً بالغةً للعديد من الأطراف الإقليمية والدولية، إذ باتت تكشف معضلة مزمنة لارتباط الوضع الإقليمي

بالدولي، والاهتمام الأمريكي بها لكي تصبح الحالة المتحققة في المنطقة ليس أمناً، بل ترتيبات إقليمية أمنية جديدة من الخارج.

وبعد أن فتح (الناتو) باب عضويته، بدت الأنظار الأمريكية تتجه نحو جنوب المتوسط والشرق الأوسط بشكل عام، وخصوصاً هذه المنطقة التي باتت تتمثَّل بالمنظور الغربي– الأمريكي مصدراً للتهديد، وعدم الاستقرار. وفي ضوء ذلك، اندفعت الولايات المتحدة لمعالجة التحديات الإلكترونية التي تواجهها لترك الباب مفتوحاً على مصراعيه أمام الدول الراغبة بالانخراط في عضوية (الناتو)، وبلورة التعاون مع تلك التي ليست لديها الرغبة في ذلك.

وقد أُريد لتلك الأطلسية أن تكون للتوسع وإعطاء الحلف مهام جديدة خارج نطاق عمله التقليدي الجغرافي، أي بمعنى أن الحلف أصبح جزءاً من المنظومة السبرانية الأمريكية لمواجهة التحديات الخارجية، إذ تُعدُّ حماية البنية التحتية الحيوية ضد الهجمات الإلكترونية، تحدياً معقَّداً، لأن لكل قطاع صناعي حالات ومتطلبات فريدة للاستخدام. ومع ذلك، فأفضل الممارسات الأمنية التي يمكن وضعها، تبقى بحاجةٍ إلى تحديثٍ مستمرٍّ، لتكون فاعلة للغاية في حماية هذه الأنظمة الحيوية.

النتائج

ومن خلال كُلِّ ما تقدَّم، نستنتج الأتي:

١– وضع وتنفيذ عقيدة متماسكة بشأن استخدام الأمن السيبراني، وذلك من أجل الردع، والاستباق، والمنع، والانتقام من النشاطات الخبيثة التي تقوم بها فواعل سيادية، أو غير سيادية.

٢– نشر قدرات الدفاع السيبراني الأمريكية الحالية للدفاع بشكلٍ استباقي عن الوكالات: الحكومية المدنية، والبنية التحتية الحيوية، والتفكير في إنشاء خدمة الأمن السيبراني الاتحادية، للانخراط في الوقت المناسب بالعمليات الدفاعية.

٣- زيادة القدرة، وإعطاء أولوية أكبر لجهود وكالات الاستخبارات الأمريكية، لجمع العمليات: الاستخبارية التكتيكية، والاستراتيجية على الإنترنت، لمواجهة أي تهديدٍ للحكومة والبنية التحتية الحيوية للدولة.

٤- تعزيز المؤسسات والمعايير، وعند الضرورة إنشاء مؤسسات جديدة تمكّن الحكومات الملتزمة بالقانون من التحرك ضدَّ التهديدات السيبرانية.

٥- إعطاء الأولوية للحفاظ على مكانةٍ بارزةٍ للشركات الأمريكية والغربية في الإنترنت.

٦- مستقبل التكنولوجيات الرقمية ودورها في تحسين وضع الإنسان، يتمثَّل التحدي لضمان أن الثورة الرقمية سوف تواصل تطورها بطريقةٍ تحترم وتعزز المُثل: الأمريكية، والعالمية، التي تتمظهر بالحرية الفردية، وبحقوق الإنسان.

٧- وأخيراً، نعتقد أن التحديات التي تواجه أمريكا في الفضاء الإلكتروني، هي تحديات كبيرة، وتتطلب أكثر من إجراءاتٍ استباقيةٍ، واستجابة للاستراتيجية هي أكثر ما يتجسد في السياسات الجارية.

الهوامش

(١) حيدر علي حسين، سياسة الولايات المتحدة الأمريكية ومستقبل النظام الدولي، ط١، دار الكتب العلمية للطباعه والنشر والتوزيع، بغداد، ٢٠١٧، ص٢٧٩.

(٢) اشرف محمد كشك، حلف الناتو: من الشراكة الجديدة إلى التدخل في الازمات العربية، مجلة السياسة الدولية، مؤسسة الاهرام، القاهرة، العدد١٨، المجلد ٤٦، ٢٠١٨، ص ص ٢٢-٢٧.

(٣) ريتشارد هاس و مارتن أنديك ،ما بعد العراق،إستراتيجية أمريكية جديدة للشرق الأوسط ترجمة سميرة إبراهيم عبد الرحمن ،سلسلة ودراسات مترجمة العدد ٣٨،مركز الدراسات الأولية جامعة بغداد،آذار ٢٠٠٩،ص٤٢.

(٤) كلود إينيس ، النظام الدولي والسلام العالمي، ترجمة: د. عبد الله العريان، ، دار النهضة العربية، القاهرة ، ٢٠١٥، ص ١١٢.

(٥) ينظر: جورج سوروس، اوهام التفوق الامريكي، سقوط اوهام جورج بوش، ترجمة: سمير مالك، ط١، دار الحمراء للنشر، بيروت، ٢٠١٧، ص ص١٦٣ – ١٦٤.

(٦) سليم دحماني ، اكثر التهديدات السيرانية على الامن القومي الولايات المتحدة انموذجاً ٢٠٠١- ٢٠١٧ ، رسالة ماجستير منشورة ، قسم العلوم السياسية – كلية الحقوق والعلوم السياسية ، جامعة محمد ضياف ، ٢٠١٨- ص ٢٦ .

(7) Mitko Bogdnoski & Drage petreski ، cyber terror ism- global security threat، international scientific defense، security and peace Journal، 327.88-004-5-027.22،p59.

(٨) زياد خلف عبدالله ومحمد شطب عيدان ، القرصنة التكنولوجية واثرها العلاقات الامريكية – الصينية ، مجلة جامعة تكريت للعلوم الانسانية ، المجلد ١٥ ، العدد ٩، ايلول ٢٠٠٨ ، ص ٤٣٢.

(9) Peter T. Lee son،The Economics computer - Hacking، department of economics west virgin ia university of Michigan press, U.S.A, 2007, p.p.181-187.

(١٠) ذياب البدانية ، الجرائم الالكترونية : المفهوم والأسباب (ورقة مقدمة في الملتقى العلمي للجرائم المستخدمة في ظل التغيرات والتحولات الاقليمية والدولية)، كلية العلوم الاستراتيجية، عمان (٢-٤/٩/٢٠١٤)، ص ٢.

(١) محمد محمود عمارة ، تاريخ القرصنة الالكترونية بين العبقرية وانتهاك الخصوصية ، شبكة صيد الفوائد ، على الرابط الالكتروني: http://www.Saaid.net/Minute

(١٢) هادي قبيس ، السياسة الخارجية الامريكية بين مدرستين ، الدار العربية للعلوم ، بيروت، ٢٠١٤ ، ص ٧٨.

(١٣) محمود حجازي ، جرائم الحاسبات والانترنت والجرائم المعلوماتية، المركز المصري للملكية الفكرية ، مارس ٢٠٠٥ . ص ١٢.

(١٤) هادي قبيس ، السياسة الخارجية الامريكية بين مدرستين ، الدار العربية للعلوم ، بيروت، ٢٠١٤ ، ص ٧٨.

(١٥) جياكومو بيروسي باولي وآخرون ، خلف الستار : التجارة غير المشروعة بالأسلحة النارية المتفجرات والذخيرة على الانترنت المظلم ، مؤسسة RAND ، سانتامونيكا ، ٢٠١٧ ، ص ٩ .

(16) Tom Bradbury، The Five Eyes alliance is always watching 13،mio 2019 : privacy hub http://www.cyberchostvpn.com.

* بأنه جزء من الأنترنت، إذ لا يمكن للمستخدم العادي الوصول إليه مثل: (Tor)، و(I2P). ويتمثل فرق (بارزين) في أسواق الأنترنت الواضح الأنترنت المظلم بشكل الدفع، إذ يتم الدفع لأسواق الأنترنت المظلم باستخدام عملات مُشفرة، وهي: الأولى من بينها والأكثر شهرة (BIT coin).

(17) Joe Carter، what you should Know about The " Five eyes" intelligence community providence، Journal of christnty and American foreign policy: http://www.providencemag.com

١. ريتشارد هاس و مارتن أنديك ،ما بعد العراق،إستراتيجية أمريكية جديدة للشرق الأوسط ترجمة سميرة إبراهيم عبد الرحمن ،سلسلة ودراسات مترجمة العدد ٣٨،مركز الدراسات الأولية جامعة بغداد،آذار ٢٠٠٩.

٢. سليم دحماني ، اكثر التهديدات السيرانية على الامن القومي الولايات المتحدة انموذجاً ٢٠٠١- ٢٠١٧ ، رسالة ماجستير منشورة ، قسم العلوم السياسية – كلية الحقوق والعلوم السياسية ، جامعة محمد ضياف ، ٢٠١٨.

3. Mitko Bogdnoski & Drage petreski , cyber terror ism- global security threat, international scientific defense, security and peace Journal, 327.88-004-5-027.

٤. زياد خلف عبدالله ومحمد شطب عيدان ، القرصنة التكنولوجية واثرها العلاقات الامريكية – الصينية ، مجلة جامعة تكريت للعلوم الانسانية ، المجلد ١٥ ، العدد ٩، ايلول ٢٠٠٨.

5. Peter T. Lee son,The Economics computer - Hacking, department of economics west virgin ia university .

٦. ذياب البدانية ، الجرائم الالكترونية : المفهوم والأسباب (ورقة مقدمة في الملتقى العلمي للجرائم المستخدمة في ظل التغيرات والتحولات الاقليمية والدولية) ، كلية العلوم الاستراتيجية ، عمان (٢-٤/٩/٢٠١٤).

٧. محمد محمود عمارة ، تاريخ القرصنة الالكترونية بين العبقرية وانتهاك الخصوصية ، شبكة صيد الفوائد ، على الرابط الالكتروني: http://www.Saaid.net/Minute

٨. محمود حجازي ، جرائم الحاسبات والانترنت والجرائم المعلوماتية، المركز المصري للملكية الفكرية ، مارس ٢٠٠٥ .

٩. اشرف السعيد احمد ، إستراتيجية امن المعلومات ، ط١ ، رقم الايداع ٢٤٦٤، ٢٠١٤.

١٠. جياكومو بيروسي باولي وآخرون ، خلف الستار : التجارة غير المشروعة بالأسلحة النارية المتفجرات والذخيرة على الانترنت المظلم ، مؤسسة RAND ، سانتامونيكا ، ٢٠١٧ .

11. Tom Bradbury, The Five Eyes alliance is always watching 13,mio 2019 : privacy hub http://www.cyberchostvpn.com.

12. Joe Carter, what you should Know about The " Five eyes" intelligence community providence, Journal of christnty and American foreign policy: http://www.providencemag.com.

١٣. جيفري أي . إيسيناش ، ترجمة : باسم علي خريسان ، الاستراتيجية الامريكية للفضاء السيراني : تعزيز الحرية والامن والازدهار ، مركز المستقبل للدراسات الستراتيجية ، ٢٠٠١- ٢٠١٧ .

١٤. سلسلة ودراسات مترجمة العدد ٣٨،مركز الدراسات الأولية جامعة بغداد،آذار ٢٠٠٩،.

١٥. زياد خلف عبد الله ، الفاعل الدولي (الفرد) في العلاقات الدولية ، مجلة تكريت للعلوم السياسية ، المجلد ٣ ، العدد ١٠ السنة (٣) ، جامعة تكريت .

١٦. جون ب. الترمان ، الجانب الاخر من العالم : الصين والولايات المتحدة الامريكية والصراع من اجل الشرق الأوسط ، مقال معهد بريجنسكي ، مركز الدراسات الاستراتيجية والدولية ، واشنطن ، ٢٠١٦.

١٧. تغريد صفاء مهدي ، افريقيا في المدرك الاستراتيجي الصيني : القرن الافريقي إنموذجاً ، رسالة ماجستير غير منشورة ، قسم الاستراتيجية – كلية العلوم السياسية ، جامعة النهرين ، ٢٠١٥.

١٨. إيهاب خليفة ، مجتمع ما بعد المعلومات ، تأثير الثورة الصناعية الرابعة على الأمن القومي ، المستقبل للأبحاث والدراسات المتقدمة العربي للنشر والتوزيع ، ابو ظبي ، ٢٠١٦.

(١٩) جيفري أي . إيسيناش، الاستراتيجية الامريكية للفضاء السيراني : تعزيز الحرية والامن والازدهار، ترجمة : باسم علي خريسان ، مركز المستقبل للدراسات الستراتيجية ، ٢٠٠١- ٢٠١٧، ص٢٦٥ .

(٢٠) ريتشارد هاس و مارتن أنديك ،ما بعد العراق،إستراتيجية أمريكية جديدة للشرق الأوسط، مصدر سبق ذكره، ص٢٦.

(٢١) جيفري أي . إيسيناش، الاستراتيجية الامريكية للفضاء السيراني : تعزيز الحرية والامن والازدهار، مصدر سبق ذكره ،٤٦.

(٢٢) ينظر: علي محمد امنيف الرفيعي، القوة الناعمة وأثرها في مستقبل الهيمنة الامريكية،ط١، مكتبة السنهوري، بغداد. ٢٠١٦، ص٨٧.

(٢٣) زياد خلف عبد الله ، الفاعل الدولي (الفرد) في العلاقات الدولية ، مجلة تكريت للعلوم السياسية ، المجلد ٣ ، العدد ١٠ السنة (٣) ، جامعة تكريت ، ص ١٤٩ .

(٢٤) جمال سند السويدي، آفاق العصر الأمريكي: السيادة والنفوذ في النظام العالمي الجديد، أبو ظبي، ٢٠١٨، ص٥٧.

(٢٥)جورج فريدمان، الإمبراطورية والجمهورية في عالم متغير، ترجمة: أحمد محمود، الدار المصرية اللبنانية، القاهرة، ٢٠١٧.، ص١٠٠.

(٢٦) جهاد عودة ، الصراع الدولي: مفاهيم وقضايا، ط٢، شركة الدليل للدراسات والتدريب واعمال الطباعة والنشر، ٢٠١٧، ص٩٧.

(٢٧) ينظر: عبادة محمد التامر، سياسة الولايات المتحدة وإدارة الأزمات الدولية (إيران–العراق–سورية–لبنان أنموذجاً)، المركز العربي للأبحاث ودراسة السياسات، بيروت، ٢٠١٨، ص٨٢.

(٢٨) جهاد عودة ، الصراع الدولي: مفاهيم وقضايا، ط٢، شركة الدليل للدراسات والتدريب واعمال الطباعة والنشر، ٢٠١٧، ص٩٧.

(٢٩) حيدر علي حسين، سياسة الولايات المتحدة الأمريكية ومستقبل النظام الدولي، مصدر سبق ذكره،٢٠١٧، ص٢٧٩.

(٣٠) محمد سعد ابو عامود، حرب باردة جديدة .. نقطة الصراع (سوريا)، مستقبل العالم الإسلامي، الامانة العامة للندوة العالمية للشباب الاسلامي، المملكة المتحدة، العدد٢١٥، ٢٠١٧، ص٤٥.