تأثير الحرب السيبرانية على رفع مستوى الصراع بين الولايات المتحدة الأمريكية و إيران

باخان ئاكو نجم الدين

قسم السياسة والعلاقات الدولية، كلية العلوم السياسية، جامعة السليمانية، السليمانية، إقليم كردستان، العراق.

البريد الإلكتروني: bakhan.najmadin@univsul.edu.iq

الملخص:

على الرغم من أنّ التقنيات الحديثة وأنظمة الاتصالات تجعل الحياة البشرية أسهل من جهة، فقد أوجدت ثورة في مجالات الأمن الدولي والعلاقات الدولية من ناحية أخرى. ومع ذلك، يجب عد التقنيات الحديثة والفضاء السيبراني سببين بارزينِ للأضرار والمخاطر الجسيمة على الأمن الدولي. يُعدُ الفضاء السيبراني المجال الخامس لإدارة القتال إلى جانب الأرض والمياه والجو والفضاء. ففي الفضاء السيبراني حدث نوع جديد وفريد من الحرب، سُميَ بالحرب السيبرانية. مما أصبحت حماية الفضاء السيبراني في الوقت الحاضر جزءًا حيويًا من الاستراتيجيات على المستوى الوطني. لأنّ الحرب السيبرانية في ظل الفضاء السيبراني ظاهرة حقيقية في العلاقات الدولية، والحرب السيبرانية بين والولايات المتحدة وإيران مثال واضح على ذلك. إذ يحاول كلا البلدين مهاجمة البنية التحتية لتكنولوجيا المعلومات وأنظمة اتصالات الشبكة للدولة الأخرى بهدف إحداث أضرار جسيمة مالياً واقتصادياً وسياسياً وعسكرياً. وهكذا، ومن المرجح أن تصبح الحرب السيبرانية هي الأكثر تميزًا في القرن الحادي والعشرين ضمن العمليات العسكرية المستقبلية.

الكلمات المفتاحية: الحرب السيبرانية، الولايات المتحدة الأمريكية، إيران، الفضاء السيبراني، الصراع.

المقدمة:

تغيرات مستمرة وسريعة شهدها المجتمع البشري منذ ظهوره، وهذه التغييرات وصلت ذروتها مع الثورة المعلوماتية وانتشار وسائل الاتصال والتكنولوجيا، كما إنّ تطور تكنولوجيا المعلومات والاتصالات أحدث تغيراً كبيراً في كل المجالات المختلفة كالاقتصاد والاجتماع والتجارة والسياسة. وانعكست هذه التطورات على طبيعة النظام الدولي وتفاعلاتها الداخلية بشكل أدى إلى تغيّر مفاهيم التفاعلات الدولية وأشكالها، وتغير الفواعل داخلها، بحيث أنّ معظم المفاهيم المرتبطة بالنظام الدولي أصبح لها غطاء ألكتروني، واصبحت توجد حاجة إلى إعادة تعريف، فعلى سبيل المثال، الأمن السيبراني والقوة السيبرانية والسيادة السيبرانية وفوق كل ذلك الحرب السيبرانية.

وعلى الرغم من الإيجابيات التي حملها عصر التكنولوجيا على المستويين الفردي والدولي، إلا أنّه حمل معه المخاطر والتحديات. لا سيما مع تزايد انتشار التكنولوجيا زادت معها تهديدات ومخاوف على الأمن والاستقرار الدوليين. وبات جليا أنّ الفضاء السيبراني عُدَّ ساحة جديدة للحروب والصراعات في القرن الحادي والعشرين، كما عُدّت الحرب السيبرانية الشكل الأكثر تطورا والأكثر بروزاً في هذا القرن؛ والحرب السيبرانية بين الولايات المتحدة الأمريكية وإيران مثال حي في هذا المجال. لذلك تسعى كلا الدولتين لاكتساب القوة السيبرانية بشقيها الهجومي والدفاعي.

تعُد الولايات المتحدة الأمريكية من أبرز الدول التي لجأت إلى تطوير فضائها السيبراني وتقويتيه والهدف الرئيس هو ضمان هيمنتها الخارجية والحفاظ على استقرارها الداخلي.

أما فيما يتعلق بإيران، فتعد من أهم الدول التي تدافع عن فضائها السيبراني، لأنّها متعلق بشكل مباشر بجميع التفاعلاته الدولية والداخلية خصوصاً ببرنامجها النووي، وأيّ ضعف في فضائها السيبراني من الممكن أن يعرض أمن واستقرار هذه الدولة للخطر.

مشكلة الدراسة:

الإشكالية التي نحاول معالجتها من خلال هذه الدراسة هي: إلى أي مدى يمكن أن تؤثر الحرب السيبرانية على رفع مستوى الصراع بين الولايات المتحدة الأمريكية وإيران؟

وللوصول إلى الإجابة عن هذا التساؤل؛ تم طرح مجموعة من التساؤلات الفرعية كما يأتي:

١. ما خلفية الفضاء السيبراني وخصائصهِ؟
٢. ما الحرب السيبرانية؟
٣. ما أوجه الاختلاف بين الحروب السيبرانية والحروب التقليدية؟
٤. كيف أثر التقدم التقني والتكنولوجي على تغيير طبيعة النظام الدولي؟
٥. كيف تستخدم الولايات المتحدة الأمريكية وإيران الحرب السيبرانية لتقوية موقفها ومكانتها ضد الآخر؟
٦. ما أهم الإجراءات التي اتخذتها كلٌ من إيران والولايات المتحدة الأمريكية تجاه بعضهما البعض لحماية فضائهما السيبراني من الحروب السيبرانية؟

DOI:https://doi.org/10.26750/Vol(8).No(4).Paper14 http://journal.uor.edu.krd/index.php/JUR Vol.8. No.4,December.2021

أهمية الدراسة:

أهمية هذه الدراسة مرتبطة بأهمية موضوع الدراسة وحداثته وحيويتهِ، على الرغم من أن هذا الموضوع ما يزال جديداً ولكن هذا لم يمنع البعض من المحاولة والبحث حول هذا الموضوع. لأن موضوع الفضاء السيبراني وتفاعلاته يحتل مرتبة متقدمة في الدراسات الأمنية والعلاقات الدولية خاصة بعدما شهد النظام الدولي في الفترة الراهنة نوعاً حديثاً من الصراعات والحروب بعد تطور القدرات التكنولوجية ووسائل الاتصالات. كما تكمن أهمية الموضوع في اختيار الدراسة الحالة التي تتمحور حول الحرب السيبرانية بين الولايات المتحدة الأمريكية وإيران إذ تعد النموذج الأمثل لدراسة الحروب السيبرانية في ظل الفضاء السيبراني.

أهداف الدراسة:

تستهدف هذه الدراسة تحليل وتفسير تأثير الحرب السيبرانية على رفع مستوى الصراع بين الولايات المتحدة الأمريكية وإيران بالشكل الآتي:

١. معرفة ماهية الحرب السيبرانية، واختلافها مع الحروب التقليدية.

٢. تهدف هذه الدراسة إلى تفسير تأثير التطورات التكنولوجية ووسائل الاتصالات الألكتروني في العلاقة بين الولايات المتحدة الأمريكية وإيران، ودور تلك التطورات ووسائلها.

٣. تحليل ومراجعة واقع الفضاء السيبراني والقدرات السيبرانية لكلا الدولتين المذكورتين.

٤. تفسير إسهامات الولايات المتحدة الأمريكية في وسائل الاتصالات الحديثة ومدى الإفادة منها في تضعيف المؤسسات الإيرانية بشكل عام وضرب برنامجها النووي بشكل خاص.

المنهجية المستخدمة في الدراسة:

من أجل الحصول على الإجابة من إشكالية الدراسة المطروحة، والتحقيق من صحة الفرضيات، فإنّ المنهجية التي اتبعها الدراسة هي:

تم الاعتماد على المنهج الوصفي منهجاً رئيساً للبحث العلمي. استخدام المنهج الوصفي لعرض مفهوم الفضاء السيبراني والحروب السيبرانية، وتعريفها، والجدل المثار حولهما. واستعانة بمنهج دراسة الحالة من خلال الاعتماد على العلاقة بين الولايات المتحدة الأمريكية وإيران في ظل الفضاء السيبراني نموذجاً، لنوضح من خلاله مدى تأثير التطورات التكنولوجية والتقنية على العلاقة بين الدولتين. فضلاً على استخدام منهج تحليل المضمون لتفسير مضامين أهم خطابات الرؤساء والسياسيين لكلتا الدولتين (الولايات المتحدة الأمريكية وإيران)، مع استخدام المنهج التحليلي النقدي للوثائق لتفسير الوثائق الرسمية المتخصصة بالهيئات الرسمية والمتخصصة بهذا المجال.

الدراسات السابقة:

ثمة رسائل جامعية، ودراسات مقدرة، اتخذت بوصفها دراسات سابقة، من أبرزها دراسة للباحث (كرار محمد جواد العامري) بعنوان (دور تكنولوجيا المعلومات والاتصالات في التفاعلات الدولية بداية الألفية الثالثة)، تناول الباحث فيها تفسير دور تكنولوجيا المعلومات على النظام الدولي والسياسة الدولية، إلا أنها لم تتناول دراسة حالة محددة، لتكون ميدانا تطبيقيا للدراسة. وثمة دراسة أخرى مقدرة، للباحثة (بن صفية وداد) بعنوان (تأثير المتغير التكنولوجي على الفواعل الدولية الجديدة الإرهاب الالكتروني -أنموذجا-)، وقد ركزت الدراسة على التطور التكنولوجي بعمق، وقد اقتصرت على فاعل معين في النظام الدولي متمثلا بالجماعات الإرهابية. وثمة دراسة أخرى للباحثة (فيان

DOI:https://doi.org/10.26750/Vol(8).No(4).Paper14 http://journal.uor.edu.krd/index.php/JUR Vol.8. No.4,December.2021

فاروق الجزراوي) بعنوان (تطورات الاقتصـاد الرقمي وإنعكاسـاتها على مكانة الدولة في النظام العالمي "نماذج مختارة")، تناولت التطورات الرقمية وإنعكاسـاتها على مكانة الدولة، وقد ركزت بوضـوح على تأثير التطورات الرقمية على الجانب الإقتصـادي، دون التعمق في تأثيره على الجوانب السـياسـية والدولية. وبهذا يمكن القول أنّ لدراسـتنا هذه مكانتها بين تلك الدراسـات، فقد تميزت، من حيث اختيار موضـوع الدراسة، وفي اختيار دراسة الحالة.

هيكل الدراسة:

للإجابة عن الإشكالية المطروحة تم تقسيم الدراسة إلى مبحثين، المبحث الأول بعنوان الفضاء السيبراني والحروب السيبرانية، ويتكون من مطلبين، في المطلب الأول تناولنا مفهوم الفضاء السيبراني وخصائصه، أما في المطلب الثاني فقد ركزنا على مفهوم الحرب السيبرانية وعناصرها فضلاً على عرض أوجه الاختلاف بين الحرب السيبرانية والتقليدية. أما المبحث الثاني فتناول الحروب بين الولايات المتحدة الأمريكية وإيران في ظل الفضاء السيبراني، إذ تم تقسيمه إلى مطلبين، المطلب الأول بعنوان استراتيجيات الولايات المتحدة الأمريكية وإيران في مجال الحرب السيبرانية، أما المطلب الثاني فتضمن الحروب السيبرانية بين الولايات المتحدة الأمريكية وإيران.

المبحث الأول: الفضاء السيبراني والحروب السيبرانية

أصبحت القضايا المتعلقة بالفضاء السيبراني تلقى اهتماماً جلياً على السياسات والاستراتيجيات الدولية على المستويين الدولي والداخلي. وتُعد الحرب من أهم المحاور في الفضاء السيبراني. إذ أدى إلى تغيير في طبيعة الحروب وملامحها. هكذا، فالحرب السيبرانية تمثل نقلة مهمة في التطور في مجال الفضاء السيبراني. بمعنى: باتت العلاقة بين الحروب والتكنولوجيا علاقة متزايدة وطردية؛ كلما تطورت التكنولوجيا كلما زادت مخاطر شن الحروب بين الدول.

بناءً على هذا، سنقسم المبحث إلى مطلبين رئيسين، فقد تضمن المطلب الأول: مفهوم الفضاء السيبراني وخصائصه، أما المطلب الثاني فقد تناول مفهوم الحرب السيبرانية وعناصرها فضلاً على توضيح أوجه الاختلاف بين الحرب التقليدية والسيبرانية.

المطلب الأول: الفضاء السيبراني: مفهومه وخصائصه

يُعدُّ مفهوم الفضاء السيبراني في العلوم السياسية والعلاقات الدولية مفهوماً جديداً نسبياً، ولكن الثورة التكنولوجية والتطور المتسارع في وسـائط التكنولوجيا تعد مثابة نقلة نوعية حيث قادت إلى تغييرات جذرية وإلى بروز تهديدات أمنية جديدة في النظام الدولي والعلاقات الدولية مايعرف بالفضاء السيبراني. وعلى الرغم من أنّه لا يوجد تعريف موحد للفضاء السيبراني بين الباحثين والمتخصصين، ولكن يوجد لديهم نهج وتوجد لديهم مبادىء موحدة نسـبياً حول أهمية الفضـاء السـيبراني وتأثيرها المباشـر على النظام الدولي والعلاقات الدولية. إنّ المجال والتطورات موضـحة التكنولوجي وتطوراتهِ قد غيّرَ مجرى التفاعلات الدولية، وخير مثال على ذلك هو إنّ الصـراعات والحروب السـيبرانية قد حلّتْ محل الحروب التقليدية. يتناول هذا المطلب في الفرع الأول منه مفهوم الفضـاء السـيبراني، أما الفرع الثاني فيتناول خصائصه.

DOI:https://doi.org/10.26750/Vol(8).No(4).Paper14 http://journal.uor.edu.krd/index.php/JUR Vol.8. No.4,December.2021

الفرع الأول: مفهوم الفضاء السيبراني

يعُد الفضاء السيبراني من أحدث المجالات في العلاقات الدولية وبالترتيب الخامس بعد مجال البر والبحر والجو والفضاء. ومما لا شك فيه أنّ التهديدات الأمنية في الفضاء السيبراني تربك الأمن والاستقرار الدوليين. لذلك من الضروري الاشارة هنا إلى بداية ظهور مفهوم الفضاء السيبراني وتعريفاته.

تعود عبارة (السايبر Cyber) تأريخياً إلى منتصف القرن العشرين، إذ انبثق هذا المصطلح من أعمال (نوربرت واينر Norbert Weiner) في كتابه (التحكم والاتصال في الحيوان والآلة Control and communication in the animal and the machine)، مفاده أنّ بإمكان البشر التفاعل مع الآلات وأنّ النظام الناتج يمكن أن يوفر بيئة بديلة للتفاعل كما يمكن أن يوفر أساساً لمفهوم الفضاء السيبراني (Wiener, 1961). وفي ثمانينات القرن نفسه، استخدم (وليام غيبسون William Gibson) لأول مرة عبارة الفضاء السيبراني (Cyber Space)، في كتابه (نيورومانسر Neuromancer) حيث وصف الفضاء السيبراني بأنّه "هلوسة توافقية يمارسها يومياً بلايين المستخدمين والمشغلين في كل الدول ... فهو تعقيد فاق التصور"(Gibson, 1989, p. 128).

أصبح هذا المفهوم يستخدم بشكل واسع بين الباحثين والأكاديميين خصوصاً في تسعينيات القرن الماضي بسبب كثرة انتشار الانترنيت وتعميم استخدامهِ عالمياً. كما وصف (جان بيري بارلو John Perry Barlow) الفضاء السيبراني بأنّ له عالماً خاصاً بين عالمين (الواقعي والافتراضي)، ومن التحديات الحديثة التي تواجه الدول القومية لأنّه تخطى كل حدود الدول وسيادتهم (Barlow, 1996).

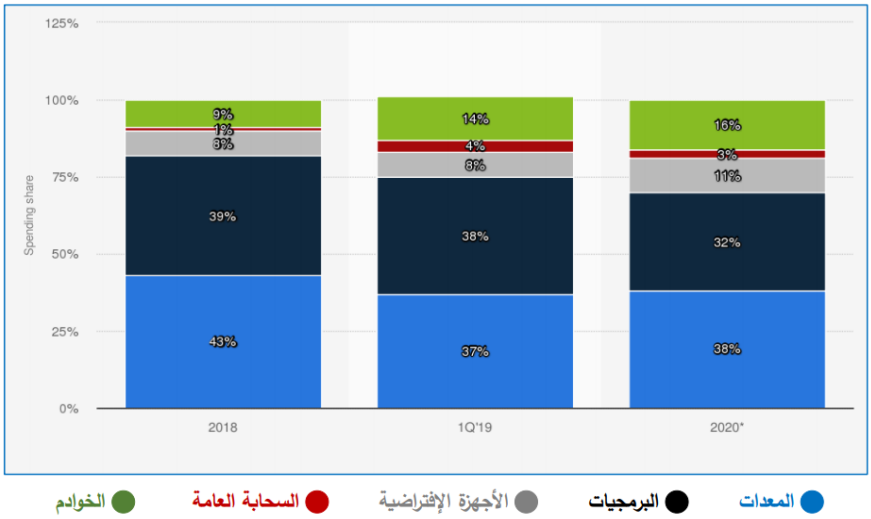
أما بالنسبة لتعريف الفضاء السيبراني في إطاره الأكاديمي والعلمي، فلم يتم الاتفاق على تعريف محدد له، ولا يوجد تعريف شامل وجامع يعالج الظاهرة، وإنما تتعدد تعاريفه بقدر المختصين والباحثين المهتمين بدراستهِ، مثل معظم المفاهيم في العلوم السياسية والعلاقات الدولية، فلهُ مفهوم غامض واجه جدلاً كبيراً بين الخبراء؛ لذلك فإنّ ايجاد إجماع على تعريف دقيق ومحدد لهذا المفهوم يعد شبه مستحيل. حيث تعرف الوكالة الفرنسية لأمن أنظمة الإعلام -التي تعد وكالة قطاعية للدولة مكلفة بالدفاع السيبراني الفرنسي- الفضاء السيبراني على أنّه "فضاء التواصل المشكل من خلال الربط البيني لمعدات المعالجة الآلية للمعطيات الرقمية" (فرحات، ٢٠١٩، ص ٩٠). أما بالنسبة لوزارة الدفاع الأمريكية فإنّ:"الفضاء السيبراني هو مجال يتميز باستخدام أجهزة الكمبيوتر والأجهزة الإلكترونية الأخرى لتخزين البيانات وتعديلها وتبادلها عبر أنظمة الشبكات والبنى التحتية المادية المرتبطة بها" (Schreier, 2015, p. 11).

وفي الجانب الواقعي والعملي، دفعت وسائل التكنولوجيا المتطورة في تحول الصراع المواجهي المباشر إلى الصراع السيبراني غير المباشر يتحكم به الإنترنيت والحواسيب ووسائل نقل المعلومات والبيانات، بناءً على ذلك، شرعت الدول والمنظمات الدولية بإنتاج آلة حربه الحديثة وابتكارها وينشرها وممارستها في الفضاء السيبراني، كذلك أصبح الفضاء السيبراني يمثل كإحدى ساحات المواجهة الدولية، مقترنة بالتكنولوجيا الحيوية (Biotechnology)، والألياف الضوئية (Digitalization) وغيرها. وبسبب أهمية الفضاء السيبراني في حياة الدول والنظام الدولي، فقد حاولت الدول التزيد في قوتها السيبرانية لحماية فضائها وأمنها السيبرانيين. فقد ظهرت حصة الإنفاق العالمي على الأمن السيبراني (٢٠١٨-٢٠٢٠)، حسب موقع (The Static) للإحصاءات من خلال نموذج للنشر للأجهزة الإلكترونية والذي يشكل الجزء الأكبر من الإنفاق على الأمن السيبراني في جميع أنحاء العالم (كما موضح في الشكل رقم ١) (العامري، ٢٠٢٠، ص ١٤٤-١٥٢).

الشكل رقم (١)

DOI:https://doi.org/10.26750/Vol(8).No(4).Paper14 http://journal.uor.edu.krd/index.php/JUR Vol.8. No.4,December.2021

حصة الأنفاق العالمي على الامن السيبراني بين عام ٢٠١٨ – ٢٠٢٠



المصـــدر: كرار محمد جواد العامري (٢٠٢٠) دور تكنولوجيا المعلومات والاتصـــالات في التفاعلات الدولية بداية الألفية الثالثة، رســـالة الماجستير، كلية العلوم السياسية - جامعة الكوفة، العراق، ص ١٥٢.

يمكننا القول أنّ تعريف الفضـــاء الســـيبراني ليس أمراً ســـهلاً، بل في الواقع إن التعاريف حول هذا الموضـــوع قيد المناقشـــة بين الباحثين والمختصين في هذا المجال. ولكن يُعد التقدم التكنولوجي من أهم مدخلات التغيير في السياسة الدولية والداخلية. كما إنّ الفضاء السيبراني قد لقي اهتماماً كبيراً في الســـياســـة الداخلية للدول إذ أصـــبح يشـــكل تحدياً كبيراً للأمن القومي للدول. ومما لا شـــك فيه فإنّ التطورات التكنولوجية والفضـــاء الســـيبراني لها الأثر البالغ في الســـياســـة الدولية بما تؤدي إلى تغيير طبيعة المواضـــيع الحســـاســـة والخطيرة المتعلقة بالسياسة الدولية كالأمن والصراع والحروب.

الفرع الثاني: خصائص الفضاء السيبراني

على الرغم من خوض المتخصـصـين نقاشـاً مثيراً بشـأن خصـائص الفضـاء السـيبراني إلاّ أنه يمكن أن نقف على أهم خصـائص الفضـاء السيبراني وأبرزها (Schreier, 2015, p. 12-13):

أولاً: تتمثل إحدى خصـائص الفضـاء السـيبراني في أنه لا يمكن أن يوجد دون القدرة على اسـتغلال الطيف الكهرومغناطيسـي الموجود بشكل طبيعي. بدون الطيف الكهرومغناطيسي، لن تتمكن الملايين من تقنيات المعلومات والاتصالات من التواصل مع بعضها البعض، بل لن تتمكن تكنولوجيا المعلومات والاتصالات نفسها من العمل.

ثانياً: إنّ الفضـاء السـيبراني يتطلب وجود تقنيات من صـنع الإنسـان، مما يجعل الفضـاء السـيبراني فريداً عند مقارنته بالمجال الأرضـي والبحري والجوي. لم يكن للفضـاء السـيبراني وجود لولا قدرة البشـر على ابتكار تقنيات قادرة على اسـتغلال الخصـائص المختلفة للطيف الكهرومغناطيسي وتصنيعها.

ثالثاً: يمكن تكرار الفضاء السيبراني باستمرار إذ يمكن أن يكون هناك العديد من الفضاءات السيبرانية التي يمكن أن يصنعها الإنسان. ولكن هناك جزء واحد مهم من المجال الجوي أو البحري أو البري: الجزء المتنازع عليه. مع الفضـــاء الســـيبراني، ومع ذلك، يمكن أن يكون هناك الكثير منه في أي وقت - بعضـها متنازع عليه والبعض الآخر غير متنازع عليه -. فضـلاً إلى ذلك، بالنسـبة للجزء الأكبر، فلا يوجد شـيء نهائي في الفضاء السيبراني. وبسبب الأجهزة غير المكلفة نسبياً والمتاحة بسهولة، يمكن إصلاح أنظمة تكنولوجيا المعلومات وشبكاتها، في حالة تلفها، وإعادة تشكيلها بسرعة.

DOI:https://doi.org/10.26750/Vol(8).No(4).Paper14 http://journal.uor.edu.krd/index.php/JUR Vol.8. No.4,December.2021

رابعاً: إنّ تكلفة الفضاء السيبراني رخيص نسبياً. إذ تعد الموارد والخبرات المطلوبة لدخول الفضاء السيبراني والتواجد فيه واستغلاله متواضعة مقارنةً بتلك المطلوبة لاستغلال المجالات البرية والبحرية والجوية. كما إنّ توليد تأثيرات استراتيجية في الفضاء السيبراني لا يتطلب ميزانية من المليارات، ولا أعداد كبيرة من القوى العاملة والأسلحة. بدلاً من ذلك، يمكن لتوفر النفقات المالية المتواضعة، ومجموعة صغيرة من الأفراد المتخصصين، والوصول إلى أجهزة كمبيوتر الشبكة، دخولاً إلى الفضاء السيبراني. ولهذا، فإن طبيعة الفضاء السيبراني تقتضي أن عدد الجهات الفاعلة القادرة على العمل في المجال والتي من المحتمل أن تولد تأثيراً استراتيجياً هو أسهل عند مقارنةً بالمجالات الأخرى.

خامساً: ومما يمكن أن يُعد سمة للفضاء السيبراني، في الوقت الحالي؛ إن الهجوم هو السائد، وليس الدفاع، وفي الأخص في الوقت الحاضر، ولذلك أسباب عدة منها: أولاً، يعتمد الدفاع عن أنظمة تكنولوجيا المعلومات وشبكاتها على البروتوكولات الضعيفة والبنى الفتوحة، إن الفلسفة السائدة للدفاع تؤكد على اكتشاف التهديدات، لا القضاء على نقاط الضعف. ثانياً، تحدث الهجمات في الفضاء السيبراني بسرعة كبيرة، مما يضع الدفاع تحت ضغط كبير، حيث يجب أن يكون المدافع متنبهاً وناجحاً طوال الوقت. ثالثاً، لم يعد النطاق يمثل مشكلة في الفضاء السيبراني نظراً لأنّ الهجمات يمكن أن تحدث من أي مكان في العالم. رابعاً، يُعد عزو الهجمات أمراً صعباً بشكل خاص، مما يعقد الاستجابات المحتملة. وأخيراً، يوفر اعتماد المجتمع الحديث الساحق على الفضاء السيبراني لأي مهاجم بيئة غنية بالأهداف، مما يؤدي إلى ضغوط كبيرة على المدافع للدفاع عن المجال بنجاح.

يبدو واضحاً، في ضوء ما سبق، أنّ الفضاء السيبراني مختلف تماماً عن المجالات الأخرى كالبر والبحر والجو، ومع ذلك فيمكن أن يُعُدُ ظهور الفضاء السيبراني أهم ما يُميّز القرن الواحد والعشرين عن العصور الماضية، في الأنشطة والمجالات كافة. كما إنّ اختلاف الفضاء السيبراني عن المجالات الأخرى هو السبب الرئيس لغموضه الذي يشوب مستقبل العلاقات الدولية. وليس من قبيل المبالغة القول أن الفضاء السيبراني قد أخذ دوراً كبيراً في إعادة تشكيل استراتيجيات الدول ومسار التفاعلات الدولية. كل هذه التغيرات وضعت الدول أمام تحدٍ جديدٍ، وأصبح الفضاء السيبراني ساحة جديدة تمارس فيها الأنشطة العسكرية والحربية. وأصبحت الحرب السيبرانية في ظل الفضاء السيبراني أحد أبرز الظواهر الحديثة في النظام الدولي الحالي.

المطلب الثاني: الحرب السيبرانية: مفهومها، وعناصرها، واختلافاتها مع الحرب التقليدية

الفضاء السيبراني هو متغير رئيس في السياسة الدولية، إذ ترتبط الحرب السيبرانية بشكل مباشر بالفضاء السيبراني. بناءً على ذلك، فإننا سنحاول في هذا المطلب أن نسلط الضوء على مفهوم الحرب السيبرانية وتعريفها وعناصرها في الفرع الأول؛ واوجه الاختلاف بين الحروب السيبرانية والحروب التقليدية في الفرع الثاني.

الفرع الأول: مفهوم الحرب السيبرانية وتعريفها وعناصرها

يمكن أن تُعد الحروب من أقدم الظواهر التي تعرفها الانسانية المعروفة، فتأريخها مرتبط بتأريخ ظهور المجتمع البشري على الأرض. ومن الممكن أن نُقسِم أشكال الحروب وطبيعتها إلى خمسة أجيال رئيسة: أولاً، حروب الجيل الأول هو نوع من الحروب يقوم على الحشود المتراصة التي تعتمد على استخدام الأسلحة البدائية والقوة الجسدية. ثانياً، حروب الجيل الثاني، وهو ذلك النوع من الحروب التي اعتمدت على قوة النيران التي تطورت لتتخذ شكل قنابل المتفجرات وقنابل الفيروسات ومقذوفات البارود. أما فيما يتعلق بحروب الجيل الثالث، وهي الحرب الذرية التي بدأت في تطور نوعي مع أواخر الحرب العالمية الثانية. وتتسم حروب الجيل الرابع بنوع الفواعل التي تخوضها؛ هذا النوع من الحروب تخوضها تنظيمات جهادية وفواعل من غير الدول بدلاً من الجيوش (بكر، ٢٠١٧، ص ٢٢). وحرب الجيل الخامس قد تكون أكثر

DOI:https://doi.org/10.26750/Vol(8).No(4).Paper14 http://journal.uor.edu.krd/index.php/JUR Vol.8. No.4,December.2021

أنواع الحروب حداثة، وهي حرب سيبرانية، وهذا النوع من الحروب متصل بتطور شبكات الاتصالات ومصادر المعلومات ومن أهم بوابات المخاطر الأمنية الدولية، وهذا ما سنسلط عليه الضوء في هذه الدراسة.

وعلى صعيد الدراسات والبحوث السياسية والأمنية المتعلقة بهذا الموضوع، فيعد المقال الموسوم بـــ(الحرب السيبرانية قادمة Cyber War is Coming) في عام ١٩٩٣ المكتوب من قبل (جون اركويلا John Arquila وديفيد رونفيلد David Ronfeld) أول ما كُتب في هذا المجال، كما يُعد كاتبي المقال أول من بحثا في مجال الهجمات والحروب السيبرانية في الفضاء السيبراني، إذ أشارا فيه إلى دور أنظمة الاتصال الالكتروني وتأثيرها في الصراعات والحروب المسلحة والمباشرة مستقبلاً (Arquilla and Ronfeldt, 1993, p. 25). كما إن الكاتب والمفكر الأمريكي (آلفين توفلر Alvin Toffler)، في كتابه (تحول السلطة: المعرفة والثروة والعنف Powershift: Knowledge, Wealth and Violence)، عدّ التكنولوجيا المعلومات هي المحور الأساس لصراعات المستقبل وحروبهِ (توفلر، ١٩٩٥، ص ٨).

بشكل عام، لم يتفق المتخصصون على تعريف محدد وقاطع للحرب السيبرانية. وعلى الرغم من ذلك، فقد اجتهد عدد من الأكاديميين والباحثين ضمن اختصاصاتهم في تقديم تعريف يحيط بهذا المفهوم، فعرف كل من (ريتشارد كلارك Richard Clarke وروبرت كناكي Robert Knake) الحرب السيبرانية على أنها "الإجراءات التي تتخذها دولة قومية لاختراق أجهزة الكمبيوتر أو الشبكات التابعة لدولة أخرى بغرض الإضرار بها أو تعطيلها" (Clarke and Knake, 2010, p. 115). وعرف (جوزيف ناي Joseph Nye) الحرب السيبرانية بأنّها "عمل عدائي في الفضاء الإلكتروني تؤدي التأثيرات المترتبة عليه إلى تضخيم العنف المادي أو تعادله. في العالم المادي، تفرض الحكومات ما يشبه الاحتكار على نطاق أوسع من استخدام القوة، ويتمتع المدافع بمعرفة وثيقة بالتضاريس، وتنتهي الهجمات إما بسبب الاستنزاف أو الإرهاق. وهنا تفرض عملية تدبير الموارد ونقلها تكاليف باهظة"(Nye, 2012). ويعرفها (بولو شاكريان Paulo Shakarian) بأنّها: تضمنت هجمات إلكترونية ذات دوافع سياسية ناشئة من دولة أو فاعلين من غير الدول ضد جهات أو دولة أخرى (Paulo Shakarian, Jana Shakarian, and Andrew Ruef, 2013, p. 9). وأكدت (ريفا جوجون Reva Goujon) كبيرة المحللين بمعهد ستراتفورد الأمريكي للدراسات الأمنية على أنّ في السراء والضراء، سيأتي تقدم تكنولوجيا الذكاء الاصطناعي ونشرها لتحديد ملامح هذا القرن. كما إنّ تقنيات التعلم الآلي لديها القدرة على إحداث تغيير جذري في الحياة المدنية والسياسية والعسكرية في العقود القادمة، وهذا سيؤدي إلى صراعات جديدة بين الدول (Goujon, 2018, p.18).

ووفقاً لقرار رقم (١١١٣) لمجلس الأمن الدولي (UN Security Council Resolution) في عام ٢٠١١ "فإن الحرب السيبرانية هي استخدام أجهزة الكمبيوتر أو الوسائل الرقمية من قبل حكومة أو بمعرفة صريحة أو موافقة من تلك الحكومة ضد دولة أخرى، أو الملكية الخاصة داخل دولة أخرى بما في ذلك: الوصول الدولي، اعتراض البيانات أو الأضرار التي لحقت بالبنية الرقمية والتحكم الرقمي. وإنتاج الأجهزة التي يمكن استخدامها لتقويض النشاط المحلي وتوزيعها" (Ventre, 2016, p. 80). ويشير تقرير خدمة أبحاث الكونجرس (Congressional Research Service Report) إلى أنه"يمكن استخدام الحرب السيبرانية لوصف جوانب مختلفة للدفاع والهجوم على المعلومات وشبكات الكمبيوتر في الفضاء السيبراني، فضلاً إلى إنكار قدرة الخصم على فعل الشيء نفسه" (Hildreth, 2001).

هكذا، تعرض تعريف الحرب السيبرانية لجدل أكاديمي واسع، ولكن بغض النظر عن اختلافات الرؤى واستناداً إلى التعريفات السابقة يمكن تعريف الحرب السيبرانية بأنها نوع حديث من الحرب في عالمنا الراهن أخذت طابعاً انتشاريا واسعا في العلاقات الدولية، ويعتمد هذا النوع من الحرب على التقدم التكنولوجي ومواقع التواصل الالكتروني وبات يشكل خطراً عالمياً وفي الأخص تأثيره السلبي على الأمن والاستقرار الدوليين.

أما بالنسبة لعناصر الحرب السيبرانية، فهذا النوع من الحرب له عنصران رئيسان، هما: أولاً؛ عمليات الهجوم السيبراني (Cyber Attack Operations): تنطلق هذه الهجمات من قاعدة معلوماتية تقوم عليها معظم عمليات الحروب السيبرانية في العالم، وهي العمليات

DOI:https://doi.org/10.26750/Vol(8).No(4).Paper14 http://journal.uor.edu.krd/index.php/JUR Vol.8. No.4,December.2021

المعلوماتية (Information Operations). تهدف هذه العمليات إلى السيطرة على معلومات الخصم لإلحاق الضرر المادي والمعنوي وإضعاف قدراته السيبرانية بهدف منعه من القيام بأية عمليات مسبقة، حيث يتم التركيز على ضرب معلوماته في شتى المجالات الاقتصادية والعسكرية والسياسية. وثانياً؛ عمليات الدفاع السيبراني (Cyber Defence Operations): وتشمل الإجراءات والوسائل الوقائية وحماية البيانات السيبرانية للدولة، وذلك للحد من ردة فعل الخصم المهاجم. تتلخص هذه العمليات الدفاعية بالمنع والوقاية، والتي تهدف إلى حماية الفضاء السيبراني للطرف المهاجم والخصم، وتنبيهه وتحذيره، وكشف الاختراقات الألكترونية في حال حدوثها، أو وضع الخطط الاستباقية الرامية لمنع أية اختراقات رقمية ومعلوماتية (جلعود، ٢٠١٣، ص ٨٩).

إنّ ما يمكن استنتاجه مما تقدم هو أنّ مفهوم الحرب السيبرانية قد خضع لجدل أكاديمي واسع بين المختصين والأكاديميين وليس هناك إجماع واسع على تعريف محدد ودقيق لمفهوم الحرب السيبرانية. ولكن غني عن القول: أنّ الثورة التكنولوجية قد ساهمت في ظهور الفضاء السيبراني، وفي الوقت نفسه، قد أثرت في طبيعة الحروب. الحرب السيبرانية في صميم مفاهيم أكثر حداثة من الحروب التقليدية الأخرى، وأصبح يشكل خطراً على الأمن والاستقرار الدوليين. مُضافاً إلى ذلك، فقد باتت القدرة التكنولوجية من أهم معايير القوة للدولة، إذ تحاول أن تستخدم قدراتها السيبرانية بكلا عناصرها الهجومية والدفاعية من أجل تحقيق أهدافها. ومن جانب آخر، تحاول الدولة أن تزيد قدرتها السيبرانية للوقاية من هذه الحروب والهجمات.

الفرع الثاني: أوجه الاختلاف بين الحروب السيبرانية والحروب التقليدية

هناك الانفصال النوعي بين الحروب التقليدية والسيبرانية. أخذت الحروب شكلاً جديداً في طبيعتها ووسائلها وأدواتها وأهدافها، وهذا ما سيتم تناوله تباعاً.

أولاً: على الرغم من أن كلفة الحروب السيبرانية ضئيلة جداً مقارنةً بالحروب العسكرية التقليدية، وعلى عكس الحروب التقليدية التي تتطلب قدراً كبيراً من المصادر، مثل الأفراد والمعدات والأسلحة، تتطلب الحروب السيبرانية أجهزة الكمبيوتر والالكترونيات واشخاصاً لديهم خبرة ومعرفة مناسبتين في المجال السيبراني (Hruza and Cerny, 2017, p. 158).

ثانياً: إنّ الأبعاد والأولويات الأساسية للحروب السيبرانية ليست عسكرية على أرض الواقع بقدر ماهي حروب سياسية، فالهدف الرئيس منها ليس بالهزيمة التقليدية عند سقوط أحد الخصوم، أنما هي تحقيق النصر عليها سياسياً عبر أستنزاف طاقتها ومواردها وكسر إرادتها وتشويه واقعها في إدارة مفاصل الحكومة. ومن أبرز مضامين الحروب السيبرانية المتمثلة بالحروب الدعائية ونشر الإخبار غير صحيحة وترويج الأفكار المتطرفة والهدامة بغرض التأثير على الأفكار ومدركات الشعوب لإضعاف قيادة الدولة وقواتها المسلحة على المجتمع (العامري، ٢٠٢٠، ص ١٤٦، ١٦٥).

ثالثاً: خلافاً للحروب التقليدية، لم تقتصر الحروب السيبرانية على فترات المواجهة العسكرية بين الفواعل الدولية، أنما يرتبط بتداخل حالتي الحرب والسلم. بمعنى، البعد الآخر للحروب الجديدة تكمن في زيادة اللجوء لتلك الآلية لاستخدامها بصورة بارزة في أوقات السلم، وذلك بعد تراجع الخطوط الفاصلة بين حالتي -السلم والحرب-، حيث لم تعد هنالك حاجة إلى إعلان حالة حرب (العامري، ٢٠٢٠، ص ١٤٩، ١٦٥).

رابعاً: يعد مفهوم الردع الذي تم تطبيقه بشكل أساسي في الحرب التقليدية غير ذي جدوى في الحروب السيبرانية. فالردع بالعقاب والانتقام لا ينطبق على سبيل المثال على الحروب السيبرانية. فعلى عكس الحروب التقليدية حيث ينطلق الصاروخ من أماكن يتم رصدها والرد عليها، فإنه من الصعوبة بمكان بل ومن المستحيل في كثير من الأحيان تحديد الهجمات السيبرانية ذات الزخم العالي؛ كونها لا تترك أثراً ودلائل واضحة وملموسة. وفي بعض الحالات قد تتطلب وقت طويلاً لرصدها وهو ما يلغي مفعول الردع بالانتقام وكثير من الحالات لا يمكن

DOI:https://doi.org/10.26750/Vol(8).No(4).Paper14 http://journal.uor.edu.krd/index.php/JUR Vol.8. No.4,December.2021

تتبع مصدرها في المقابل (عبدالغفاري، ٢٠١٦، ص ١٢). كما أشار الكولونيل (كينيث وايت Kenneth White)، ضمن مشروعه البحثي التابع لكلية الحرب بالجيش الأمريكي بعنوان (الإرهاب السيبراني: الفوضى الحديثة Cyber-Terrorism: Modern Mayhem) في عام ١٩٩٨، أكد بأنّ غموض التهديد وتحديد هوية الفاعلين من أبرز خصائص الهجمات السيبرانية وأخطرها (White, 1998, p. 14). وفي السياق نفسهِ، صرح (كارل ليفين Carl Levin) عضو مجلس الشيوخ الأمريكي السابق ورئيس مجلس الشيوخ للخدمات المسلحة، "بأنّ الحرب السيبرانية مدمرة في تأثيرها كأسلحة الدمار الشامل، وأصعب جزء فيها هو خاصية اخفاء المهاجمين، وصعوبة اثبات هوية المنفذ وجهة التنفيذ، فمن غير الممكن تحديد الجهة المنفذة هل هي دولة، أو مجموعة، أو حتى فرد، وعليه صنفت الحروب والهجمات السيبرانية على أنها تهديدات خطيرة للأمن القومي" (غيدان والربيعي، ٢٠٢٠، ص ٢٠٣).

خامساً: في الجانب القانوني، لم تتضمن المعاهدات الدولية المنظمة نصوصاً صريحةً وواضحةً للتعامل مع الحروب والصراعات السيبرانية. ولكن أستاذ القانون الدولي (مايكل شميت Michael Schmitt)، يذهب في دراسة له بالمجلة الدولية للصليب الأحمر حول هذا الموضوع، إلى أنه حتى لو لم تواكب المعاهدات الدولية للصراعات والحروب السيبرانية، فإنها تخضع لقواعد القانون الدولي الإنساني من منظور تأثيراتها التدميرية. حيث إن استهداف الطائرات، الكهرباء، أو شبكات المياه في دولة ما بفيروس إلكتروني قد يؤدى لتعطيلها، فضلاً إلى الإضرار بالمدنيين الذين يفترض أن تشملهم حماية القوانين الدولية في الحروب العسكرية المباشرة (على، ٢٠١٧، ص ٤).

من خلال ما سبق نلخص للقول أن مع بروز الفضاء السيبراني، واجهت المفاهيم التقليدية مثل الأمن والقوة والسيادة تحديات واضحة. فوق ذلك، بروز الفضاء السيبراني تسبَبَ في تغيير طبيعة الصراع والحروب بأدوات مختلفة عن نظيراتها التقليدية. هكذا، يتم استخدام الفضاء السيبراني ساحة للصراع، مما أدى إلى تحويل الحرب التقليدية إلى حرب رقمية وافتراضية. فالصراعات والحروب، قبل بروز ذلك الفضاء السيبراني، كانت أكثر محدودية وقابلة للتنبؤ. على الرغم من أنّ الحرب السيبرانية تمتاز بسهولتها وانخفاض تكلفتها، مقابل خسائر الحروب التقليدية. ولكن لا شك أنّ الفضاء السيبراني تسبب في تهديدات سيبرانية مرعبة وساحة محفزة للعنف والصراع. لذلك، فإنّ السلاح الرقمي هو سلاح القرن الحالي، وأصبح المتغيير التكنولوجي يخلق نوعاً جديداً من السلاح، والقرن الحالي ينطلق بسباق تسلح الكتروني. فضلاً إلى ذلك، تتميز الحرب السيبرانية بصعوبة تحديد مضمونها وفواعلها بدقة.

إنّ قضية الحرب السيبرانية من القضايا المؤثرة والبارزة في العلاقات الدولية بين الولايات المتحدة الأمريكية وإيران في القرن الحالي. من خلال مراجعة العلاقات بين واشنطن وطهران طيلة مسيرة الثورة الإيرانية في ١٩٧٩ حتى يومينا هذا، مما يجعلنا نجزم بأنّ هناك عداوة تأريخية بين البلدين. كما لا يمكن التغافل عن إنّ إيران تمتلك مكانة مهمة في العديد من الملفات الإقليمية والدولية لذلك لم يعد من الممكن تجاهل دورها فاعلةً لها تأثير. ويشتهر نظام السياسة الخارجية الإيرانية بتعقيده وغموضهِ في علاقاته مع الدول الأخرى بشكل عام ومع الولايات المتحدة الأمريكية بشكل خاص.

وقد لعب التطور المتسارع في وسائط تكنولوجيا المعلومات في العلاقة بين الولايات المتحدة الأمريكية وإيران دوراً فاعلاً في لإرتفاع وتيرة التوتر والصراع بينهما، وهذا بدوره يؤثر سلباً على مستقبل العلاقة بين البلدين. وهكذا يتضح بما لا يدع مجالاً للشك، إن الفضاء السيبراني أصبح مجالاً للتفاعلات الصراعية بين الدولتين، وهذا ما سنناقشه في المبحث الثاني.

DOI:https://doi.org/10.26750/Vol(8).No(4).Paper14 http://journal.uor.edu.krd/index.php/JUR Vol.8. No.4,December.2021

المبحث الثاني: الحروب بين الولايات المتحدة الأمريكية و إيران في ظل الفضاء السيبر اني

مع ظهور العولمة زادت الخلافات والتضـاربات بين الدول، ظهرت معها أحداث وظواهر جديدة من بينها الحرب السـيبرانية. أصـبحت قضية الحروب السيبرانية قضية دولية، ففي عصرنا تمثل هذه الحروب أكثر التهديدات وأخطرها على الأمن والاستقرار الدوليين. لذلك فإنّ بيئة كهذه تتطلب اسـتراتيجيات وسـياسـات صـلبة وجدية في مواجهتها من قبل الدول، سـواء على المسـتوى الدفاعي أم الهجومي. وهذه التغييرات في العلاقات بين الدول أدت إلى تغيير جذري والعلاقة بين الولايات المتحدة الأمريكية وإيران أبرز مثال على ذلك. وقد تقوم كلا الدولتين باستخدام هجمات سيبرانية كجزء من استراتيجيتهما الهجومية ضد بعضهما البعض هذا من جهة. ومن جهة أخرى، تستخدم كلا الدولتين القدرات السيبرانية سلاحاً دفاعياً لضمان بقائهما وحفاظاً على سيادتهما وأمنهما الوطني.

قامت الولايات المتحدة الأمريكية بشن سلسلة من الهجمات السيبرانية ضد إيران بأعذار عديدة منها: أن إيران تمتلك قدرات سيبرانية هجومية، والتي يمكن لها أن تشـكل خطراً جلياً على الولايات المتحدة الأمريكية وعلى حلفائها. وفي سـياق متصـل، هاجمت الولايات المتحدة الأمريكية المنشـآت النووية الإيرانية الكترونياً بهدف تعطيل البرنامج النووي الإيراني، لأنها تعد هذا البرنامج واحداً من أخطر التهديدات الأمنية على المسـتوى الدولي. ورداً على ذلك، كشـفت إيران علناً محاولات التجسـس والهجمات السـيبرانية ضـد حكومة الولايات المتحدة الأمريكية ومؤسساتها الأكاديمية والرسمية.

لذا سـنخصـص هذا المبحث للبحث في الحروب السـيبرانية بين الولايات المتحدة الأمريكية وإيران، وذلك من خلال مطلبين، نتناول في المطلب الأول اسـتراتيجيات الولايات المتحدة الأمريكية وإيران في مجال الحرب السـيبرانية، ونبين في المطلب الثاني الحرب السـيبرانية بين الولايات المتحدة الأمريكية وإيران.

المطلب الأول: استر اتيجيات الولايات المتحدة الأمريكية و إيران في مجال الحرب السيبر انية

على الرغم من أنّ الولايات المتحدة الأمريكية هي الدولة الرائدة في مجال الإبتكار التكنولوجي، ولكن ازداد القلق في السـنوات الأخيرة بين السياسيين الأمريكين بشأن المخاطر والخوف من الحروب في الفضاء السيبراني بعد حدوث سلسلة من الهجمات المجهولة اتجاه أمن وطنهم وسـيادتهِ، خصـوصـاً بعد أحداث ١١ أيلول ٢٠٠١ إذ بدأت الولايات المتحدة الأمريكية التركيز على الفضـاء السـيبراني كتهديد أمني جديد وجدي، فعملت على تطوير قوتها الدفاعية والهجومية في مجال الفضـاء السـيبراني. أما بالنسـبة لإيران، فمن غير المرجح أن تتخلى عن تزايد قوتها السـيبرانية وذلك لأنها تعدها ركيزة رئيسـة للأمن القومي وأمن النظام، وتعدها نوعاً من القوة الأسـاس بالنسـبة إلى أمنها الخاص على المسـتوى الأقليمي والدولي. لذلك، اسـتثمرت إيران في الآونة الأخيرة في بناء قدراتها السـيبرانية -الهجومية والدفاعية- لتكون مثابة مضـاعفة لقوتها.

بناءً على ما سبق، سنتناول في هذا المطلب استراتيجيات الولايات المتحدة الأمريكية وإيران في مجال الحرب السيبرانية من خلال فرعين، سـنكرس الفرع الأول للقدرات الدفاعية والهجومية السـيبرانية للولايات المتحدة الأمريكية، وسـنفرد الفرع الثاني للقدرات الدفاعية والهجومية السيبرانية لإيران.

DOI:https://doi.org/10.26750/Vol(8).No(4).Paper14 http://journal.uor.edu.krd/index.php/JUR Vol.8. No.4,December.2021

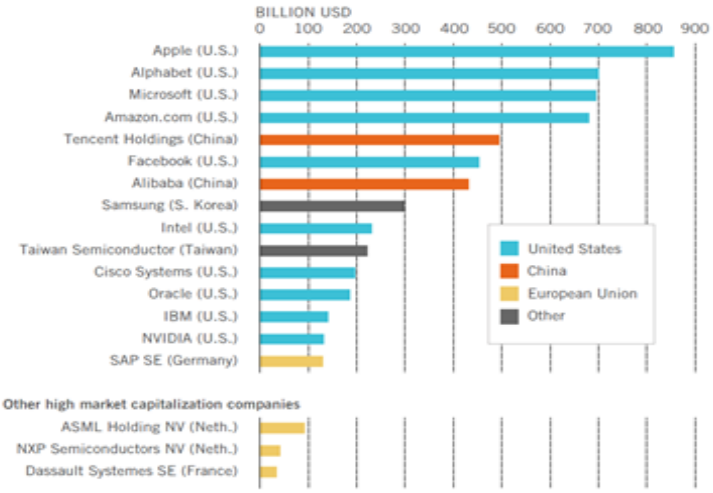
الفرع الأول: القدرات الدفاعية والهجومية السيبرانية للولايات المتحدة الأمريكية

أصبحت الهجمات السيبرانية مصدر تهديد جلى لأمن الدول، لذلك تبنت معظم دول العالم سياسات هجومية في الفضاء السيبراني عبر اتخاذ إجراءات لمهاجمة مصادر التهديد وتعقب الفاعلين في الهجوم على منشآت البنية التحتية الحيوية ويتم استخدام نظم سيبرانية متقدمة كتطوير استخدام أسلحة سيبرانية في الحرب (شلوش، ٢٠١٨، ص ٢٠٠)، والولايات المتحدة الأمريكية ليست استثناءاً من هذه القاعدة. وفي سياق متصل رفع الخبير السياسي والدبلوماسي والاستشاري الجيوسياسي الأمريكي (هنري كيسنجر Henry Kissinger) سقف القناعة حول رؤية الولايات المتحدة الأمريكية للفضاء السيبراني بقوله: "الثورة في عالم الأتصالات والمعلوماتية هي الأولى في التاريخ في إيصال هذا العدد الكبير من الأفراد والسيرورات إلى أداة التواصل نفسها وترجمة تحركاتهم وتعقبها بلغة تكنولوجية واحدة" (كيسنجر، ٢٠١٥، ص ٣٣٣).

وعلى الرغم من أنّ أكبر الشركات التكنولوجية في العالم من حيث القيمة السوقية تنتمي إلى الولايات المتحدة الأمريكية (للمزيد ينظر الشكل رقم ٢)، وأنّ أكثر من (٤٦٪) من امكانيات العالم الالكترونية مركزها أمريكا (عبد اللطيف، ٢٠١٥، ص ١٠٠). ومع ذلك دخلت الولايات المتحدة الأمريكية في المنافسة الحقيقية والشديدة داخل الفضاء السيبراني منذ عقد الستينات.

الشكل رقم (٢)

أكبر شركات التكنولوجيا من حيث القيمة السوقية



Source: Reva Goujon (2018) The global race for Al supremacy: The geopolitics of artificial intelligence competition. Bled Strategic Times, p. 19.

بعد أحداث ١١ أيلول، تتصدر الولايات المتحدة الأمريكية قائمة الإنفاق على تطوير القدرات السيبرانية الهجومية. في ٢٣ حزيران ٢٠٠٩، حيث أنشأت الولايات المتحدة الإمريكية مركز القيادة المقاتلة الموحدة للأمة في مجال الفضاء السيبراني (USCYBERCOM). يتألف المركز من القدرات العسكرية والاستخباراتية وتكنولوجيا المعلومات. وتتمثل مهمتها في توجيه عمليات الفضاء السيبراني ومزامنتها وتنسيقها وتخطيطها للدفاع عن عمليات الفضاء السيبراني للدفاع عن المصالح الوطنية وتعزيزها بالتعاون مع الشركاء المحليين والدوليين. يدافع هذا المركز عن أنظمة معلومات وزارة الدفاع (DoD-Department of Defense)، ويدعم قادة القوات المشتركة في عمليات الفضاء السيبراني، ويدافع عن الولايات المتحدة الأمريكية من الهجمات السيبرانية الكبيرة. يمثل هذا المركز أحدث تطور في سلسلة من التصاميم التنظيمية

DOI:https://doi.org/10.26750/Vol(8).No(4).Paper14 http://journal.uor.edu.krd/index.php/JUR Vol.8. No.4,December.2021

لتمكين شـبكة معلومات وزارة الدفاع (Department of Defense Information Network - DoDIN) ولتحسـين القدرات العسـكرية الأمريكية في الفضاء السيبراني (U.S. Cyber Command).

في عام ٢٠١٠، أقرت الولايات المتحدة الأمريكية استراتيجية جديدة تحضر فيها لإمكانية خوض حرب سيبرانية شاملة. في هذا السبيل، جهز البنتاغون خمس عشرة ألف شبكة حاسوب يعمل على إدارتها تسعون ألف خبير في الكمبيوتر والتكنولوجيات، مع أكثر من ألف خبير عسكري في القرصنة الالكترونية، والمهمة الرئيسة لهذا الجيش هو التصدي للهجمات السيبرانية على الولايات المتحدة الأمريكية مع تسديد الضربات الاستباقية إلى الجهات التي تحضر هجمات سيبرانية. وفي سياق نفسه، أعلن مدير وكالة الدفاع الأمريكية للتقنيات الواعدة، (ريغينا دوغانRegina Dugan)، بأنّ "جهوداً إضافية ستبذل لإنشاء سلاح إلكتروني هجومي يشكل عنصراً جوهرياً في الآلة العسكرية الأمريكية، مع ضرورة معرفة الإمكانات الإلكترونية للدول الأخرى بهدف التحصن ضدها" (عبد اللطيف، ٢٠١٥، ص ١٠٥). وقامت وزارة الدفاع الأمريكية بتصنيف الفضاء السيبراني على أنّه الميدان الرابع من ميادين الحروب بعد البر والبحر والجو، حيث تقوم وزارة الدفاع الأمريكية بإجراء مناورة سنوية تحت اسم (سايبر ستورم Cyber Storm) لاختبار جاهزيتها لمواجهة أية هجمات سيبرانية معادية ويشارك فيها أكثر من مئة واثنا عشرَ جهازاً أمنيا أمريكيا (شكر، ٢٠١٩، ص ٥).

وفي عام ٢٠١٢، خصصت الولايات المتحدة الأمريكية خمسمائة مليون دولار في ميزانيتها لمواجهة التهديدات السيبرانية، وعملت لتصنيع أدوات وأسلحة سيبرانية هجومية لمواجهة احتمال تهديدات العدو مع تطوير فيروسات سيبرانية لتخريب شبكات الخصم الحساسة. وفي العام نفسه، عملت الولايات المتحدة الأمريكية على زيادة مخصصات تمويل الأبحاث السيبرانية من مئة وعشرين مليون دولار إلى مئتين وثماني ملايين دولار (عبد الصادق، ٢٠١٦، ص ٦٧).

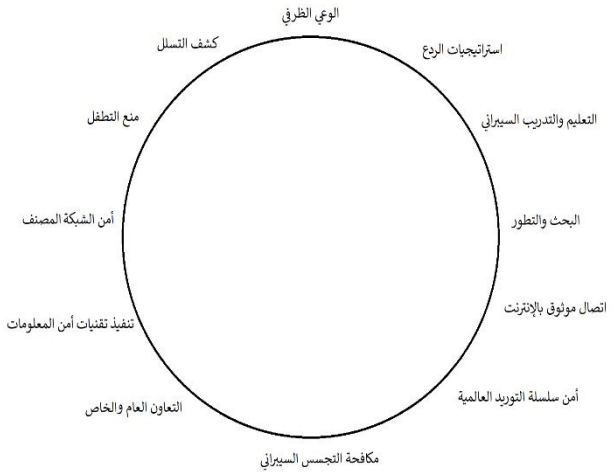
أما بالنسبة للقدرات الدفاعية السيبرانية، فعلى الرغم من أنّ الولايات المتحدة الأمريكية تبقى الدولة الأكثر امتلاكاً للقدرات الهجومية العالية المطلوبة في الفضاء السيبراني، إلا أنّه من الواضح أنّ اهتمامها انصب في السنوات الأخيرة على تعزيز القدرات والتقنيات الدفاعية وتقويتها في هذا المجال. ونظراً لأنها الدولة الأكثر اعتماداً في العالم على شبكات الإنترنيت في مختلف المجالات العسكرية والمدنية لذا فهي الأكثر اهتماماً بالجانب الدفاعي فيما يتعلق بالفضاء السيبراني بشكل عام والحروب السيبرانية بشكل خاص مقارنةً بالدول الأخرى (شكر، ٢٠١٩، ص ٣).

أما بالنسبة للعهد الرئاسي لجورج بوش الابن، فقد قام جورج بوش بمبادرة تمويل المؤسسات والجهات المتعلقة بالأمن السيبراني بشكل كبير، وعُرِف الأمن السيبراني كجزء من الاستراتيجية الوطنية الأمريكية (Andress and Winterfeld, 2011, p. 9). وفي تشرين الثاني ٢٠٠٧، دعت إدارة بوش وكالة الأمن القومي للتنسيق مع وزارة الأمن الداخلي لحماية الحكومة وشبكات الإتصالات المدنية من التهديدات الخارجية، ضمن اطار خطة تهدف إلى تعزيز "الأمن السيبراني"، وقد خصصت لهذا التوجه الاستراتيجي مئة واربعة واربعين مليون دولار من ميزانية الدفاع الأمريكي (عبد اللطيف، ٢٠١٥، ص ٩٣). وإدارة جورج بوش كانت مصممة لمعالجة مخاوف مستوى الأمن القومي السيبراني خلال آثني عشر مجالاً استراتيجياً، كما هو موضح في الشكل رقم (٣).

DOI:https://doi.org/10.26750/Vol(8).No(4).Paper14 http://journal.uor.edu.krd/index.php/JUR Vol.8. No.4,December.2021

الشكل رقم (٣)

المجالات الأثني عشر التي استثمرت فيها إدارة جورج بوش في الأمن السيبراني



Source: Jason Andress and Steve Winterfeld (2011) Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners, ELSEVIR, London, p. 9.

وفي عام ٢٠٠٨، تم التعديل على المادة (٧٠٢)، من قانون مراقبة الاستخبارات الأجنبية على بيانات المواطنين من غير الولايات المتحدة الأمريكية، وقد اعطت هذه المادة الحق لوكالة الأمن القومي الأمريكي على جمع رسائل البريد الألكتروني وتحليلها، ومراقبة مواقع التواصل الإجتماعي والمكالمات الهاتفية. وفي العام ذاته، قامت إدارة الرئيس بوش بإطلاق "مبادرة الأمن الالكتروني الأمريكي"، حيث سعت هذه المبادرة إلى إنشاء خطوط أمامية للدفاع ضد التهديدات الفورية، وجميع أنواع التهديدات السيبرانية التي تواجه الولايات المتحدة الأمريكية من خلال نشر ثقافة التعليم الالكتروني، وزيادة أمن تكنولوجيا المعلومات، وتعزيز قدرات مكافحة التجسس، وتطوير خطة حكومية قائمة على مخابرات الكترونية وزيادة أمن الشبكات السرية (غيدان والربيعي، ٢٠٢٠، ص ٢٠٥).

أما بالنسبة للعهد الرئاسي لباراك أوباما، فمع تزايد حجم الاعتمادية الأمريكية على شبكة المعلومات وتعرض الجيش الأمريكي عام ٢٠٠٨ لعدد كبير من الهجمات السيبرانية، أعلن الرئيس الأمريكي آنذاك باراك أوباما: الهجمات السيبرانية بأنّها هي من أخطر الحوادث السيبرانية حتى الآن ضد شبكاتنا العسكرية، إذ أصيبت عدة آلاف من أجهزة الكمبيوتر ببرامج ضارة. وفي الواقع، في عالم اليوم، فإن الأعمال الإرهابية ليست التهديدات الوحيدة في العالم، بل إنّ الضربات والهجمات السيبرانية تعد مثابة سلاح من أسلحة الدمار الشامل (The New York Times, 2009). لذلك، ظهرت النقلة الكبيرة في الفضاء السيبراني الأمريكي في بداية عهد الرئيس باراك أوباما، حيث قام بمضاعفة الميزانية المرصودة من مئتين وسبعة مليار دولار إلى سبع مليارات دولار، وقد تضاعف عدد العاملين من قبل الجيش الأمريكي في هذا المجال من تسعة الاف إلى اربعة آلاف شخص أيضاً. واستحدث وزير الدفاع الأمريكي السابق (روبرت غيتس Robert Gates) وحدة متخصصة مكرسة لقيادة الحرب السيبرانية (شكر، ٢٠١٩، ص ٤).

وكلف الرئيس أوباما عند تولية المنصب فريق عمل لتقييم الاستراتيجيات الخاصة بمجال الفضاء السيبراني، وانتهى الفريق بإصدار تقرير بعنوان "مراجعة سياسة الفضاء السيبراني Cyberspace Policy Review"، وقد اعتبرت الولايات المتحدة الأمريكية أن قضية الأمن السيبراني تمثل قضية أمنية وطنية مهمة (غيدان والربيعي، ٢٠٢٠، ص ٢٠٦).

DOI:https://doi.org/10.26750/Vol(8).No(4).Paper14 http://journal.uor.edu.krd/index.php/JUR Vol.8. No.4,December.2021

وفي أيار ٢٠٠٩، وافق بارك أوباما على توصيات لمراجعة سياسة الفضاء السيبراني، ووجهت الحكومة الأمريكية العمل بشكل دقيق ووثيق مع جميع الفاعلين في هذا المجال، بما في ذلك القطاع الخاص وحكومات الولايات والحكومات المحلية، وذلك لضمان استجابة منظمة وموحدة للتهديدات السيبرانية في المستقبل المنظور، وتقوية الشركات الخاصة والعامة وتعزيزها لإيجاد الحلول التكنلوجية التي تضمن أمن الولايات المتحدة الأمريكية وتحافظ عليه. كذلك الاستثمار في الأبحاث الأكاديمية المتطورة والتنمية اللازمة للاكتشاف لمواجهة التحديات والتهديدات السيبرانية. والبدء بحملة لتعزيز الوعي بالأمن السيبراني (شكر، ٢٠١٩، ص ٤-٥). وفي سياق متصل لتقوية الفضاء السيبراني، خصصت الإدارة الأمريكية للأمن السيبراني نحو ستة مليار دولار من ميزانية عام ٢٠٠٩. وقامت الإدارة الأمريكية بتخطيط الإستراتيجية الجديدة للفضاء السيبراني، وكان من بين ما تضمنه هذه الإستراتيجية الجديدة توحيد نظم (القيادة والتحكم والاستخبارات والإتصالات) تحت إدارة واحدة تسمى (القيادة الفضائية الأمريكية)، التي تخضع للإشراف المباشر من قبل مساعد وزير الدفاع الأمريكي آنذاك (عبد اللطيف، ٢٠١٥، ص ٩٤).

وبهدف تطوير التكنولوجيات الدفاعية، عمل عدد كبير من الشركات الدفاعية باشراف وكالة البحوث الدفاعية المتقدمة، على تأسيس نماذج افتراضية تحت مسمى "ميادين رماية" في إطار "معارك الحرب السيبرانية". أهمية هذا النظام تكمن في أن يسمح للمختصين بمحاكاة هجمات من قبل قوى خارجية، ومن قراصنة الحواسيب داخل أمريكا. جاءتْ هذه الاستراتيجية مثابة إختبار لتطوير التكنولوجيات الدفاعية (عبد اللطيف، ٢٠١٥، ص ٩٤).

وفي أيار ٢٠١٠، قام باراك أوباما بإنشاء قيادة الإنترنت "سايبر كوم Cybercom" وعيّن مدير وكالة الاستخبارات القومية الجنرال (كيث أليكساندر Keith Alexander) قائداً عليها، مهمته الحرص على حماية الشبكات العسكرية الأمريكية على الدوام. وهذه الوكالة تضم ألف فرد من نخبة الجواسيس والقراصنة الإلكترونيين المحترفين بهدف ضمان حماية الفضاء السيبراني الأمريكي بأسرهِ (شكر، ٢٠١٩، ص ٥).

وفي عام ٢٠١٤، قدمت هيئة الدفاع الوطني الأمريكية مشروع قانون للكونجرس لتوفير ميزانية ضخمة لتطوير الأسلحة الدفاعية السيبرانية، ودعت مبادرة الأمن السيبراني لمواجهة التجارة الدولية في مجال الأسلحة السيبرانية. وقد تمت المطالبة بتخصيص ثمان وستين مليون دولار للقيادة العسكرية للفضاء السيبراني، وخمسة مليون وثمان مئة الف دولار للدفاع السيبراني، ومئة وتسع وستين مليون دولار لاستكمال إنشاء مبنى مركز العمليات في الفضاء السيبراني، وتسع عشرة مليوناً لأبحاث الأمن السيبراني، وعشرين مليون دولار لدعم الأبحاث المتقدمة في الأمن السيبراني (عبد الصادق، ٢٠١٦، ص ٧٣).

وفي عهد الرئيس دونالد ترامب، حيث زاد الاهتمام بالمجال السيبراني وبالتهديدات والجرائم المتعلقة به. فعلى سبيل المثال، في البداية عام ٢٠١٧، حددت إدارة دونالد ترامب استراتيجية واضحة بخصوص كيفية مواجهة التهديدات السيبرانية للحفاظ على الأمن الوطني الأمريكي، وهذا من خلال بناء شبكات حكومية يمكنها الدفاع ضد الهجمات السيبرانية، وتحسين تبادل الاستشعار والمعلومات، وتحديد أولويات المخاطر السيبرانية، ومحاولة ردع الفواعل السيبرانية الاجرامية وتعطيلها (دحماني، ٢٠١٨، ص ٧٥). وفي السنة نفسها، أكد دونالد ترامب على رفع القيادة السيبرانية في البنتاجون إلى وضع قيادة مقاتلة موحدة، كما قال: "إنّ قرار إنشاء قيادة سيبرانية منفصلة يظهر عزمنا المتزايد على مواجهة التهديدات السيبرانية وسيساعد في طمأنة حلفائنا وشركائنا وردع خصومنا" (دحماني، ٢٠١٨، ص ٧٦). بناءً على أهمية الفضاء السيبراني، خصصت الولايات المتحدة الأمريكية حوالي بليون وأربعة وخمسين مليون دولار من ميزانيتها لعام ٢٠١٧ للدفاع السيبراني (عبد الصادق، ٢٠١٦، ص ٧١).

لابد لنا من ذكر حقيقة مهمة هي؛ أنّه كلما تقدمت التكنولوجيا زادت احتمالية احلال الحرب والهجمات السيبرانية بين الدول. لذلك، أصبح الفضاء السيبراني أهم الأسلحة الاستراتيجية التي تستخدمها الدول للدفاع عن أمنها وسيادتها ومكانتها في النظام الدولي. وفي هذا

DOI:https://doi.org/10.26750/Vol(8).No(4).Paper14 http://journal.uor.edu.krd/index.php/JUR Vol.8. No.4,December.2021

السـياق، فإنّ الولايات المتحدة الأمريكية كأكبر قوة تكنولوجياً على المسـتوى العالم اعتمدت على التكنولوجيا لحماية أمنها ومكانتها على المسـتوى العالمي من خلال محاولة انجاز الردع التكنولوجي من جهة، ومحاولة توظيف قدراتها التكنولوجية لمواجهة الدول الأعداء وإضعافهم، وعلى رأسهم إيران، من جهة آخرى.

الفرع الثاني: القدرات الدفاعية والهجومية السيبرانية لإيران

أصبحت إيران تدرك أن الخطر في الوقت الحاضر قد يأتي من الفضاء السيبراني. لذلك فإنّه ليس من المستغرب أن علها مواجهة التهديدات السيبرانية الخارجية خصوصاً تهديدات الولايات المتحدة الأمريكية، إذ حاولت إيران توسيع نطاق قدرتها الدفاعية والهجومية، ورصدت لها ميزانيات ضخمة.

طورت إيران من قدراتها السيبرانية الدفاعية خلال إنشائها لمجموعة مؤسسات وهيئات مخصصة لهذا المجال؛ ومن أبرز وأهم تلك الهيئات هي:

أولاً: في بداية عام ٢٠٠٩ بدأت إيران بتأسيس إحدى مشاريعها الاستراتيجية السيبرانية بما عُرفت بـــ(برنامج الانترنت المنعزل Loner Internet Program) أو (الانترنت الحلال Halal Internet) الهدف الرئيس وراء هذا المشروع تقوية النظام الدفاعي السيبراني من خلال منع الاختراق الخارجي له، هذا من الجهة. ومن جهة أخرى، حاول هذا المشروع تحويل النشاط السيبراني بالدولة إلى شبكة اتصالات داخلية منعزلة عن الشبكة العالمية للإنترنت، لذلك حاولت الحكومة إحكام رقابتها وتعزيز إشرافها على محتوى الشبكة والبيانات المتاحة بها وكذلك بيانات المستخدمين (راشد، ٢٠١٦).

ثانياً: من أجل تعزيز الاجراءات الدفاعية السيبرانية اعتمدت إيران على إنشاء عدد من المؤسسات الحكومية والبرنامج السيبرانية وتشكيلها من أجل تحقيق هذا الهدف، فعلى سبيل المثال، في تشرين الأول ٢٠١١، قامت إيران بتأسيس مقر الدفاع السيبراني؛ وبهذا أصبحت ضمن الدول التي تملك منظومة دفاعية كاملة في مواجهة تهديدات الحرب السيبرانية (عبد الصادق، ٢٠١٦، ص ٦٧-٦٨). وفي آذار ٢٠١٢ أسست إيران (المجلس الأعلى للفضاء السيبراني Super Council of Cyberspace-SCC) الذي تم تشكيله بموجب أوامر خامنئي المباشرة لوضع خطة سياسة شاملة للفضاء السيبراني والاهتمام بتنسيق الجهود للدفاع السيبراني، وإعداد السياسات العامة التي يتوجب على جمع الهيئات المعنية والمتصلة بالفضاء السيبراني تنفيذها. ويضم المجلس الأعلى للفضاء السيبراني مجموعة واسعة من وسطاء السلطة الرئيسين ومسؤولين رفيعي المستوى في النظام مثل: رئيس الدولة، رئيس البرلمان، رئيس القضاة، وزراء الثقافة والاتصالات ومسؤولين من أجهزة المخابرات والأمن وغيرهم (Sabet and Safshekan, 2013, p. 18).

ثالثاً: في إطار تطوير إيران قدراتها الدفاعية السيبرانية، أسست هذه الدولة منظمة (قيادة الدفاع السيبراني) بهدف حماية البنية التحتية الإيرانية من التهديدات والهجمات السيبرانية، وتدعيم الدفاعات السيبرانية والعمل على أنظمة مؤسسات الدولة (راشد، ٢٠١٦).

رابعاً: تضع إيران أهمية قصوى لتأسيس خدمة البريد الإلكتروني الداخلي لمواطنها بدلاً من استخدام شبكة الإنترنت العالمية لتقليل التهديدات والاختراق السيبراني الخارجي. وفي هذا الخصوص، قامت الحكومة الإيرانية في أيلول ٢٠١٢ بتنفيذ مشروع شبكة المعلومات الوطنية (National Information Network -NIN). وفقاً لإيران، تسعى هذه المبادرة إلى تقييد وصول الإيرانيين إلى شبكة الإنترنيت العالمية بشدة من خلال إنشاء شبكة انترنت وطنية، وهذا بهدف تخفيف الهجمات السيبرانية على إيران خلال سرقة المعلومات المهمة. أخذت المرحلة الأولى بربط ٤٢٠٠٠ جهاز كمبيوتر حكومي حساس بشبكة المعلومات الوطنية. وفي المرحلة الثانية حاولت الحكومة الإيرانية إلزام الإيرانيين باستخدام شبكة المعلومات الوطنية بدلاً من شبكة المعلومات العالمية (Sabet and Safshekan, 2013, p. 18). وقد وفرت خدمة

DOI:https://doi.org/10.26750/Vol(8).No(4).Paper14 http://journal.uor.edu.krd/index.php/JUR Vol.8. No.4,December.2021

البريد الإلكتروني تلك حوالي ١٠٠ مليون مشترك. وقامت الحكومة الإيرانية بإغلاق بعض البرمجيات مثل (غوغل توك Google Talk) و(سكايب Skype). والهدف من تأسيس هذه الخدمة تسهيل عملية المراقبة والإشراف على جميع الاتصالات الإلكترونية (راشد، ٢٠١٦).

جنباً إلى جنب القدرات الدفاعية السيبرانية، تسعى إيران من ناحية أخرى إلى تعظيم قدراتها الهجومية السيبرانية أيضاً. وأن تُصبح إيران واحدة من أقوى الجيوش السيبرانية في العالم، ولها القدرة الكافية لصد كل الهجمات الخارجية. فأصبحت إيران، بحلول عام ٢٠١٣، واحدة من أهم اللاعبين الأساسين على ساحة الحرب السيبرانية الدولية، ومصدر تهديد للدول الكبرى عموماً، والولايات المتحدة الأمريكية خصوصاً (العامري، ٢٠٢٠، ص ١٦٢).

جنباً إلى جنب القدرات الدفاعية السيبرانية، طورت إيران من قدراتها السيبرانية الهجومية خلال إنشائها لمجموعة مؤسسات وهيئات مخصصة لهذا المجال؛ ومن أبرز تلك الهيئات وأهمها هي:

أولاً: الجيش السيبراني الإيراني (Iranian Cyber Army-ICA): بدأت العمليات الإلكترونية الإيرانية في حوالي عام ٢٠٠٤، وهي تركز بشكل أكبر على خنق المعارضة الداخلية للنظام الحاكم وفرض تكاليف على الدول الأخرى لأنشطتها المناهضة لإيران. وبعد ذلك تم تنفيذ العمليات السيبرانية الجدية في إيران من قبل الجيش السيبراني الإيراني والعديد من الوكلاء. وهذا الجيش يتكون من مجموعة تضم مختصين من ذوي مهارات عالية في تكنولوجيا المعلومات والمتسللين المحترفين الذين يتجنبون الكشف عن هويتهم. وبشكل عام، يبدو أن العمليات السيبرانية الإيرانية انتقامية بطبيعتها، وتركز على الخصوم الإقليميين والدوليين، وتسعى إلى تعظيم البنية التحتية السيبرانية الحاسمة لردع الخصوم عن التدخل في الشؤون الداخلية لإيران (Hodgson and et al, 2019, p. 23).

ثانياً: فريق الأمن الرقمي آشيانه (Ashiyane Digital Security Team): تأسست هذه المجموعة برعاية النظام الإيراني تشجيعهِ في عام ٢٠٠٥، وهذه المجموعة مستقلة عن الجيش الإيراني أو الأجهزة الأمنية، وهدفها الرئيس هي تقديم أدوات قرصنة ودروس تعليمية مجانية بخصوص الهجمات السيبرانية، بينما يستخدم أيضاً معارف ومهارات أعضائه للدفاع عن المواقع الإلكترونية (Hodgson and et al, 2019, p. 23).

ثالثاً: قوات الباسيج شبه العسكرية (Basij Paramilitary Force): فضلاً عن الجيش السيبراني الإيراني، هناك وحدات أخرى -أقل احترافية- في مؤسسات النظام الإيراني لعمليات السيبراني. إحدى هذه المؤسسات هي الباسيج التي قامت باستثمارات كبيرة لمثل هذه العمليات. وتجدر الإشارة إلى أنّه بعد إعادة تنظيمه في عام ٢٠٠٧، أصبحت الوحدات المسلحة من الباسيج الآن أعضاء في القوات البرية للحرس الثوري الإيراني بينما تتحمل وحداته غير العسكرية -التي تشكل غالبية وحدات الباسيج- مسؤولية الحرب (وهم مسؤولون بشكل خاص عن الحرب السيبرانية مع أعداء النظام الإيراني). وأهم الأنشطة السيبرانية التي حدثت بالفعل في هذه القوة شبه العسكرية هي توفير مهارات في مجال الإنترنت والكمبيوتر، مع توفير عشرات الآلاف من الدروس المجانية وتم إنشاء الآلاف من مدونات الويب للعمل فيها (The BBC Persian, 2010). فضلاً عن ذلك، تشير تقارير إلى أنّ إيران باتت في المراحل النهائية لشن هجمات سيبرانية محتملة، وخاصة بعد أن أعدت قوات الحرس الثوري الإيراني جيشا من القراصنة السيبرانيين، وقوامه عدة آلاف من المختصين في مجال الحرب السيبرانية، وهو جزء من خطة إستراتيجية جديدة لتطوير شعبة الجيش السيبراني التي أنشات في العام ٢٠١٠، وقد تم تقسيم الشعبة على ثلاث مجموعات: المجموعة الأولى؛ مهمتها دفاعية، تقوم على أساس مراقبة هوية المهاجمين في الفضاء السيبراني وتحديدهم، وصد الهجومات السيبرانية المحتملة على إيران. المجموعة الثانية؛ مهمتها هجومية عبر شن هجمات سيبرانية على مراكز التحكم في البنى التحتية لشبكات الطاقة في المناطق التي تعد معادية لإيران. المجموعة الثالثة؛ تختص بإختراق الشفرة السيبرانية الخاصة بنقل المعلومات وتحليلها (عبد اللطيف، ٢٠١٥، ص ٩٨).

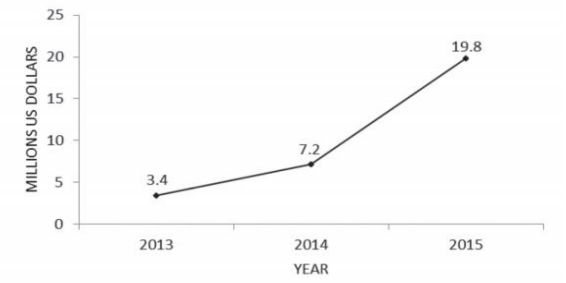
DOI:https://doi.org/10.26750/Vol(8).No(4).Paper14 http://journal.uor.edu.krd/index.php/JUR Vol.8. No.4,December.2021

رابعاً: استثمرت إيران بكثافة في قواتها الهجوم السيبراني منذ عام ٢٠١١، كما استثمرت أكثر من مليار دولار في بنيتها التحتية السيبرانية وتعظيم قدراتها في هذا المجال، فضلاً عن استقدام خبراء من الخارج لتطوير قدراتها السيبرانية وتعظيمها (راشد، ٢٠١٤). تتلقى إيران مساعدات خارجية ودولية كبيرة لتطوير فضائها السيبراني. حسب تقارير مركز التحليلات البحرية للأبحاث (Centre for Naval Analyses - CAN) أنّ إيران تنسق مع القراصنة الأجانب الذين تشاركهم أهدافاً إيديولوجية، بما في ذلك مجموعات القراصنة الشيعية الإسلاميين، والجيش الإلكتروني السوري، وحزب الله اللبناني. وفي أيلول ٢٠١٢، وقعت إيران وكوريا الشمالية اتفاقية للتعاون التقني تسمح بالتعاون في مجموعة متنوعة من المجالات، بما في ذلك تكنولوجيا المعلومات والأمن (Hodgson and et al, 2019, p. 24) . وفي إطار سعي إيران لحماية أمنها المعلوماتية ومؤسساتها الحساسة من التهديدات والهجمات السيبرانية، قامت بتخصيص أكثر من بليون دولار لتحسين قدراتها في مجالي الدفاع والهجوم في القدرات السيبرانية في عام ٢٠١٢ (عبد الصادق، ٢٠١٦، ص ٧٢).

ومع وصول حسن روحاني للمنصب الرئاسي عام ٢٠١٣، زادت الميزانية السنوية المخصصة للحرس الثوري فيما يتعلق بتطوير القدرات الهجومية السيبرانية، والتي تصل إلى حوالي ٢٠ مليون دولار (راشد، ٢٠١٦). وقامت إيران بزيادة ميزانية الأمن السيبراني بشكل ملحوظ بين عامي ٢٠١٣-٢٠١٥، كما نلاحظ في الشكل رقم (٤). وتقرير شبكة الاستخبارات نورس (Norse Intelligence Network) أشار إلى ازدياد تحريض إيران على تطوير قدراتها الهجومية السيبرانية واستخدام فضائها السيبراني سلاحاً هجومياً لمواجهة المخاطر والتهديدات الخارجية بشكل ملحوظ. وأكد التقرير على أنّ في المدة من كانون الثاني ٢٠١٤ إلى آذار ٢٠١٥ زادت الهجمات الإيرانية المنطلقة من أنظمة التحكم الإيرانية بنسبة ١٢٨٪، كما ارتفع عدد أجهزة الاستشعار المتضررة من الهجمات الإيرانية بنسبة ٢٢٩٪، في حين زاد عدد البرامج المتكاملة المستخدمة لتنفيذ مثل تلك الهجمات بنسبة ٥٠٨٪ (راشد، ٢٠١٦).

الشكل رقم (٤)

ميزانية إيران للأمن السيبراني



Source: Anthony Craig and Dr. Brandon Valeriano, Conceptualising Cyber Arms Races, 2016, NATO CCD COE Publications, Tallinn, p. 149.

بناءً على كل المحاولات الجدية للحكومة الإيرانية لتطوير قدراتها الهجومية السيبرانية، صنف المسؤول السابق في مجلس الأمن القومي الأمريكي (ريتشارد كلارك Richard Clarke) إيران على أنها تقع في المرتبة الثانية بعد الصين من حيث امتلاكها للقدرات الهجومية السيبرانية، كما أشار إليه في الجدول رقم (٥)(Clark and Knake, 2010, p.148) .

DOI:https://doi.org/10.26750/Vol(8).No(4).Paper14 http://journal.uor.edu.krd/index.php/JUR Vol.8. No.4,December.2021

الجدول رقم (٥)

القوة الشاملة للحرب السيبرانية في عام ٢٠١٠

الدول	الهجمات السيبرانية	الدفاعات السيبرانية	مجموع
الولايات المتحدة الأمريكية	٨	١	٩
الصين	٥	٦	١١
إيران	٤	٣	٧

Source: Clarke, R. A. and Knake, K. (2010) Cyber War: The Next Threat to National Security and What to do about it. New York: HarperCollins, p. 148.

على الرغم من صعوبة إنكار حقيقة قدرة إيران السيبرانية في كلا المجالين الدفاعية والهجومية إلاّ أنّها ليست على قدم المساواة مع قدرات السيبرانية للولايات المتحدة الأمريكية، ولكن هذا لا يعني أنّ إيران متوقفة عن تطوير قدراتها السيبرانية. بل إنّ المسؤولين الإيرانيين والجهات المختصة يقومون باستمرار بتعزيز الفضاء السيبراني عبر توفير الميزانيات المخصصة لهذا المجال. وإذ قامت إيران بإنشاء وحدات وجهات مختصة بالمجال السيبراني داخل قواتها العسكرية.

المطلب الثاني: الحروب السيبرانية بين الولايات المتحدة الأمريكية و إيران

إنّ التقدم التكنولوجي جعل الدول المتنافسة بشكل عام، وإيران والولايات المتحدة بشكل خاص تدخل في مضمار سباق تسلح وهو سباق تسلح الفضاء السيبراني. وعلى الرغم من أنّ الحرب العسكرية المباشرة بين الولايات المتحدة الأمريكية وإيران لم تبدأ حتى يومنا هذا على الإطلاق، ولكن الحروب والصراعات غير المباشرة والخفية كالحرب السيبرانية بين الدولتين لها تأريخ طويل وعميق. كما تعد إيران واحدة من الدول المستهدفة التي تتعرض للهجمات السيبرانية من قبل الولايات المتحدة الأمريكية وهذا بسبب برنامجها النووي. وفي المقابل، تنظر إيران إلى الولايات المتحدة الأمريكية كعدو دائم لها، وحرصت إيران على وضع استراتيجيات تتعلق بأمنها السيبراني. وقد أكد عدد كبير من السياسين والخبراء بأنّ إيران تستمر في خوض الحروب السيبرانية مع الولايات المتحدة الأمريكية.

لذا سيتم تقسيم هذا المطلب إلى فرعين، يتناول الأول الهجمات السيبرانية للولايات المتحدة الأمريكية تجاه إيران، أما الثاني فيتناول الهجمات السيبرانية الإيرانية تجاه الولايات المتحدة الأمريكية.

DOI:https://doi.org/10.26750/Vol(8).No(4).Paper14 http://journal.uor.edu.krd/index.php/JUR Vol.8. No.4,December.2021

الفرع الأول: الهجمات السيبرانية للولايات المتحدة الأمريكية تجاه إيران

بدأت الولايات المتحدة الأمريكية بسلسلة من الهجمات والحروب السيبرانية تجاه إيران بهدف تعطيل أجهزة الطرد المركزي لهذه الدولة ذات الصلة بالمنشآت النووية.

منذ عام ٢٠٠٦ قامت الولايات المتحدة الأمريكية بمهاجمة المواقع الحساسة والمهمة، المختصة بالبرامج النووية الإيرانية، من خلال نظام رئيس يسمى (اللهب Flame) للتأثير في نشاط اليورانيوم وأجهزة الطرد المركزي والمرافق التابعة له في منشأة (نطنز) النووية بالذات (الفتلاوي، ٢٠١٦، ص ٦٢٥-٦٢٦).

وفي حزيران عام ٢٠١٠ قامت الولايات المتحدة الأمريكية بإرسال فيروس أو دودة افتراضية سميت بـ"ستكسنت Stuxnet" لمهاجمة المنشآت الحساسة والأجهزة المرتبطة بتخصيب اليورانيوم الإيرانية، التي أغلقت برنامج إيران النووي بشكل مؤقت. تم تصميم الفيروس بطريقة يمكنها أن تنتشر بسرعة من جهاز كمبيوتر إلى آخر مع أو بدون الإنترنت على عكس فيروسات الكمبيوتر المتعارف عليها. وصُنعت هذا الفيروس بطريقة تجعل من المستحيل التنبؤ به أو توقيفه (Rao, 2014). وتسبب بعطل في أكثر من ٣٠ ألف حاسوب شمل حواسيب مفاعل (نطنز)، وقد أصاب الفيروس ودمّر حوالي ١٠٠ جهاز طرد مركزي ودمرها (بكر، ٢٠١٧، ص ٢٣). وفي هذا الصدد، أعلنت الإستخبارات الإيرانية في تشرين الثاني ٢٠١٠، بأنّ الهجمات الفيروسية تسري أصابتها جنباً إلى جنب من أصابات البعد الإلكتروني والمعلوماتي، كذلك أصابة المكون المادي، لأنّه أصاب ستة عشر آلالف جهاز كمبيوتر، وتعطيل الأف إجهزة الطرد المركزية تدميرها، ولهذا لم تتمكن إيران في آب ٢٠١٠ أفتتاح المفاعل النووي (العامري، ٢٠٢٠، ص ١٥٨).

وفي ١٧ شباط ٢٠١٢، أعلنت الاستخبارات الإيرانية أن فيروس (ستكسنت) قد أصاب ما يقدر بستة عشر ألف جهاز كمبيوتر (عبد الصادق، ٢٠١٦، ص ٤٦). ففي دراسة لها، أشارت شركة (سيمناتيك) التي تعمل في مجال برامج الأمن السيبراني والبرامج المضادة للفيروسات أنّ إيران تأتي في طليعة الدول المستهدفة من ناحية الإصابات التي حققها برنامج "ستكسنت" وأنّ ما يقارب ٦٠٪ من أجهزة الكمبيوتر التي تعرضت لهجوم من هذا التطبيق الخبيث كانت في إيران. فضلاً عن ذلك، ذهبت العديد من المصادر إلى التخمين بأنّ مفاعل بوشهر الإيراني قد يكون الهدف الأساس الذي يبحث البرنامج عنه لتدميره (شكر، ٢٠١٩، ص ١١). وأكدت الحكومة الإيرانية رسمياً في نيسان ٢٠١١، أن نشر فيروس "ستكسنت" مثابة سلاح سيبراني ضد برنامجها النووي الذي أُنشئ من قبل الولايات المتحدة الأمريكية بالتعاون مع إسرائيل (Rao, 2014). وتم تطوير فيروس ستكسنت بصورة تسمح للمهاجمين عن بعد بسرقة ملفات ومعلومات من أجهزة الكمبيوتر المصابة بالفيروس ومراقبة رسائل البريد الإلكتروني والرسائل الفورية (عبد اللطيف، ٢٠١٥، ص ٩٢). بناءً على كل ذلك، كشفت صحيفة (نيويورك تايمز The New York Times) أنّ الولايات المتحدة الأمريكية كانت اللاعب الرئيس في الهجوم السيبراني ضد إيران، وذلك ضمن حملة تستهدف تدمير برنامجها النووي، وأشارت الصحيفة إلى أن الرئيس الأمريكي السابق باراك أوباما يهتم شخصياً بتسريع وتيرة استخدام الفيروسات الإلكترونية في الهجوم على برنامج تخصيب اليورانيوم الإيراني (عبد اللطيف، ٢٠١٥، ص ١٠١).

وفي ٢٠١٢، استخدمت الولايات المتحدة الأمريكية واسرائيل (فيروس فليمر Flamer virus) ضد المنشآت النووية الإيرانية وألحقت بها أضراراً بالغة. ونجح الفيروس في سرقة كم هائل من المعلومات المهمة والسرية بخصوص المفاعل النووي الإيراني (عبد اللطيف، ٢٠١٥، ص ١٠١).

وفي شباط ٢٠١٨، اتهمت الحكومة الأمريكية إيران بشن هجمات سيبرانية على وطنهم وسرقة بيانات الملكية واختراق أنظمة الكمبيوتر؛ لذلك فرضت وزارة الخزانة الأمريكية عقوبات على ٩ من الشركات وكبار القادة التابعة لمجموعة معهد (مبنا) التابع للحرس الثوري الإيراني لهذا السبب. وأكد مكتب التحقيقات الفيدرالي الأمريكي إن: "ضحايا المجموعة قد شملت نحو ١٤٤ جامعة أمريكية، واثنتين من المنظمات غير الحكومية الدولية وخمس وكالات فيدرالية في الولايات المتحدة الأمريكية، و١١ شركة أجنبية خاصة" (رجب، ٢٠١٩).

DOI:https://doi.org/10.26750/Vol(8).No(4).Paper14 http://journal.uor.edu.krd/index.php/JUR Vol.8. No.4,December.2021

وبناءً على ما تقدم؛ يمكن القول بأنّ الولايات المتحدة الأمريكية هي القوة الابرز في اقتحام الفضاء السيبراني والسَّباقة في شن الهجمات السيبرانية. وتستخدم الولايات المتحدة الأمريكية أسلحة الفضاء السيبراني في صراعها مع إيران بشكل بارز. على الرغم من ذلك، تحاول إيران التعامل مع الهجمات السيبرانية الأمريكية باستخفاف شديد وتحاول التقليل من قيمتها وأهميتها. ولكن من الواضح أنّ الحرب السيبرانية ستكون مهيمنة على العلاقة بين الولايات المتحدة الأمريكية وإيران في القرن الحالي وفي المستقبل.

الفرع الثاني: الهجمات السيبرانية الإيرانية تجاه الولايات المتحدة الأمريكية

من الواضح بأنّ معدل التهديدات السيبرانية على إيران مرتفع بنسبة عالية مقارنةً بمعظم دول العالم، وهذا يعود بنسبة كبيرة إلى محاولات هذه الدولة وإصرارها لتحقيق برنامجها النووي. وفي المقابل، قامت إيران بتطوير برامجها السيبرانية لحماية برنامجها النووي، وللتدليل على ذلك، يبدو أنّ عمل الإيرانيين لا يقتصر على الدفاع فقط، وإنّما يشمل تنفيذ الهجمات أيضاً، خصوصاً ضد الولايات المتحدة الأمريكية. كما تفسر (كريج جريثهاوس Graig Greathouse) الحرب السيبرانية بأنّها تشكل فرصة مهمة لإيران، لأنها نموذج للحرب غير المتكافئة (Asymmetric warfare)، فهي شبيهة إلى حد كبير بعنف حرب العصابات والعمليات الإرهابية. وهذا النوع من الحروب مثابة الحرب المثالية للنظام الإيراني لأنه قد يستخدمه بوصفه أداة فعالة للهجوم على خصمه دون الجوء إلى الحرب العسكرية المباشرة (Greathouse, 2013, p. 22).

تلجأ إيران إلى قدراتها الدفاعية والهجومية السيبرانية كأداة مهمة للحفاظ على أمنها الوطني ووسيلة لردع أية هجمة سيبرانية على برنامجها النووي من ناحية، ورداً على العقوبات التي تفرض عليها من قبل الولايات المتحدة الأمريكية من ناحية أخرى. وقد انعكست تلك التطورات السيبرانية الملحوظة في سلسلة من الهجمات التي وقعت بين عامي ٢٠١٢-٢٠١٣. في أيلول ٢٠١٢ بدأت الجماعات الإيرانية الهجوم على المواقع الإلكترونية للمؤسسات المالية والبنوك الرئيسة في الولايات المتحدة الأمريكية من خلال شبكات مراكز المعلومات الرئيسة التي مكنتهم من الدخول إلى مواقع تلك البنوك والمؤسسات (راشد، ٢٠١٦)، استهدف قراصنة إيرانيون البنوك الكبرى مثل (جيه بي مورجان تشيس JPMorgan Chase)، و(بنك أوف أمريكا Bank of America)، و(ويلز فارجو Wells Fargo) بهجمات كبيرة لتعطيل الخدمة، ما جعل من الصعب على العملاء تسجيل الدخول إلى حساباتهم والوصول إلى أموالهم، ما أدى لانهيار مواقع البنوك على شبكة الإنترنت (Perlroth, 2012)، حتى إن خبراء الأمن السيبراني أكدوا أنّ هذه الهجمات غير مسبوقة في فاعليتها ونطاقها (راشد، ٢٠١٤). وفي السنة نفسها، هجمت الدولة الإيرانية على الشبكة الداخلية لسلاح مشاة البحرية الأمريكية عن طريق القرصنة الإلكترونية (راشد، ٢٠١٦). ويوضح المهندس سامر سفاريني لموقع "روسيا اليوم"، أنّه على الرغم من التفاوت بين قدرات إيران والولايات المتحدة الأمريكية فإنّ"جمع جيش سيبراني وأسلحة رقمية ليس بالأمر الصعب في حال توافرت الرغبة والامكانات المادية" (عبد اللطيف، ٢٠١٥، ص ١٠٥).

وفي أوائل عام ٢٠١٣، بدأت موجة أخرى من الهجمات السيبرانية الإيرانية على شركات الطاقة والبنية الأساسية الأمريكية. فعلى سبيل المثال، حاولت إيران السيطرة على الأنظمة الهكربائية وخطوط الغاز والبترول الأمريكية. لذلك، تنبأ بعض المسؤولين الرسميين والخبراء فضاء السيبراني إلى أن أية محاولة لتصعيد العقوبات وتشديدها ضد سوق البترول الإيراني من قبل الولايات المتحدة الأمريكية سيدفع إيران لشن هجمات سيبرانية على الولايات المتحدة الأمريكية (راشد، ٢٠١٤).

وفي عام ٢٠١٤، استخدمت الحكومة الإيرانية نوعاً من البرمجيات الخبيثة (Wiper Malware) ضد الشبكات المنتشرة في (لاس فيجاس Las Vegas)، ووصلت خسائر هذه الهجمات إلى حوالي ١٤ مليار دولار (راشد، ٢٠١٦).

DOI:https://doi.org/10.26750/Vol(8).No(4).Paper14 http://journal.uor.edu.krd/index.php/JUR Vol.8. No.4,December.2021

وفي عام ٢٠١٥ ، تزامن توقيت انتهاء الهجمات السيبرانية الإيرانية على البنوك والوكالات الحكومية الأمريكية مع توقيع خطة العمل الشاملة المشتركة (Joint Comprehensive Plan of Action-JCPOA). ولكن قبل الصفقة من السنة نفسها قامت إيران بهجمات متكررة ضد ست وأربعين مؤسسة وشركة مالية أمريكية (Hodgson and et al, 2019, p. 27).

وزادت حدة التوتر بين الولايات المتحدة الأمريكية وإيران بعد اغتيال قائد فيلق القدس في الحرس الثوري الإيراني قاسم سليماني مع نائب قائد مليشيا "الحشد الشعبي" العراقي (أبو مهدي المهندس) في ٣ كانون الثاني ٢٠٢٠ في ضربة جوية أمريكية قرب مطار بغداد الدولي. قال (كيرستين تود Christine Todd)، العضو المنتدب لمعهد الجاهزية الإلكترونية: "قتل سليماني أحرز تقدما كبيرا في الصراع الأمريكي الإيراني. لأن الإيرانيين سيحاولون بالتأكيد الانتقام، في المنطقة وسيقومون أيضا بدراسة الخيارات في وطننا. ومن بين الخيارات المتاحة لهم، الفضاء الإلكتروني الأكثر إلحاحا" (هاشم، ٢٠٢٠).

بجانب الهجمات السيبرانية الإيرانية ضد الولايات المتحدة الأمريكية، فهذه الدولة لها تاريخ طويل في الهجمات السيبرانية على دول إقليمها أو حتى الدول خارج نطاق إقليمها، السعودية العربية أبرز مثال على ذلك، ففي عام ٢٠١٢ هجمت إيران على شركة النفط السعودية (أرامكو Aramco) بفيروس (شامون Shamoon). وفي السنة نفسها، هجمت إيران على شركة الطاقة القطرية (راس غاز Ras Gas). وفي عام ٢٠١٤ أستخدمت إيران الهجمات السيبرانية ضد إسرائيل. وفي ٢٠١٧ للمرة الثانية هاجمت إيران شركة النفط السعودية أرامكو باستخدام قدراتها السيبرانية.

مما تقدم يتبين أنّ الفضاء السيبراني ذو طبيعة غامضة ومعقدة، وإنّ الهجمات السيبرانية الإيرانية المتكررة تجاه الولايات المتحدة الأمريكية مثابة محاولة اثبات أن الفضاء السيبراني سيكون مجال المنافسة الأمنية القادمة بين الدولتين. وتعد إيران منافساً نظيراً للولايات المتحدة الأمريكية، ومن المرجّح بأنّ إيران ستلعب دوراً كبيراً في هذا النوع من الحروب.

الخاتمة والاستنتاجات:

التطورات المتسارعة في المجال التكنولوجي فرضت نفسها على شتى المجالات كالاجتماع والإقتصاد والأمن والسياسة. والتطورات هذه، تشمل مجالي النظام الدولي والعلاقات الدولية بشكل واضح، مما أدى إلى المطالبة بإعادة التفكير في مفهوم العلاقات الدولية والنظام الدولي ومصطلحاتها منها الحرب السيبرانية. تشكل ظاهرة الحرب السيبرانية إحدى أبرز الظواهر التي نتجت عن اتساع العالم الالكتروني والفضاء السيبراني. ولكن بسبب غموض الفضاء السيبراني وتعقيده كان من الصعب أن نجد تعريفاً عالمياً مقبولاً، يتعلق به، كالحرب السيبرانية.

ترسم التطورات التكنولوجية معظم ملامح العلاقات بين الدول، العلاقة الأمريكية-الإيرانية أبرز مثال على ذلك. وتعد الحرب السيبرانية جزءا أساسا لهذه العلاقة بين الدولتين. وهذا ما أقحم العلاقات الأمريكية-الإيرانية في مرحلة جديدة من التوترات بصورة مكثفة.

في هذه الدراسة، تناولنا في المبحث الأول منها توصيفاً عاماً لمفهوم الفضاء السيبراني وتعريفه؛ والحرب السيبرانية أهم هذه الظواهر وأبرزها، وسلطنا الضوء على أوجه الاختلاف بين الحروب التقليدية والسيبرانية. وحاولنا في المبحث الثاني أن نفسر العلاقة بين الولايات المتحدة الأمريكية وإيران في ظل الفضاء السيبراني.

DOI:https://doi.org/10.26750/Vol(8).No(4).Paper14 http://journal.uor.edu.krd/index.php/JUR Vol.8. No.4,December.2021

وقد توصلت الدراسة إلى عدد من الاستنتاجات التي نلخص أهمها كما يأتي:

١. أصبح من الصعب تهميش دور الفضاء السيبراني وتأثيره في مجال السياسية والعلاقات الدولية، وما يميز الفضاء السيبراني أنه عابر لحدود الدول. هكذا، ارتفعت وتيرة الصراع والمنافسة بين الدول شأنه شأن التقدم التكنولوجي وتقدم وسائل الاتصال الإلكتروني. ويتميز الفضاء السيبراني بالتغييرات السريعة والمفاجيئة لأن الابتكار والتطور في هذا الفضاء أسرع من تفاعلات الحياة الواقعية لذلك فإن التهديدات والتحديات من المفترض أن تكون أخطر مقارنةً بالتفاعلات الواقعية.

٢. أثر الفضاء الألكتروني الذي رافق تطور التكنولوجيا على النظام الدولي وعلى الحرب بمفهومهِ التقليدي. ولكن هذا لا يعني أنّ الحرب السيبرانية أقل خطراً من الحرب التقليدية؛ بل من الممكن أن تتحول الحرب السيبرانية إلى حرب تقليدية مباشرة بين الدول.

٣. مع انخفاض وقوع الحروب التقليدية العالمية أصبحت الحروب السيبرانية المهدد الأول للأمن والاستقرار الدوليين. كما إنّ ما يُعد خطيراً في عالم الانترنت عدم معرفة مكان الهجمات السيبرانية أو زمانها، أو مصدرها، أو هوية الفاعل الحقيقي لهذه العملية، أو حتى التكهن بهذه المجالات، ولهذا فإنّ المعلومات غير واضحة في معظم الأحيان.

٤. أصبح الفضاء السيبراني يحتل أهمية كبيرة في استراتيجة الدول. لذلك، ربطت الدول وظائفها وبنيتها التحتية بشبكات الفضاء السيبراني. من هذا المنطلق، تطورت القدرات الهجومية والدفاعية السيبرانية واخذن حيزاً كبيراً في سياسات إيران واستراتيجياتها لمواجهة الهجمات السيبرانية من قبل الولايات المتحدة الأمريكية. والآن، يشار إلى إيران على أنها نموذج لدولة متطورة سيبرانياً على المستويين الدولي والإقليمي.

٥. عززت الولايات المتحدة الأمريكية حضورها المتزايد في الفضاء السيبراني يوماً بعد يوم، ووضعت الأمن السيبراني على قمة أولوياتها الأمنية والاستراتيجية. وأصبح للولايات المتحدة الأمريكية قدرة عملية عالية على تنفيذ تهديدات سيبرانية وهجمات على جميع الدول في العالم، ولكن أكثر الهجمات تستهدف إيران بدرجة أولى.

٦. تصاعد التوتر بين الولايات المتحدة الأمريكية وإيران بشكل خطير، خصوصاً بعد الهجوم السيبراني الأخير الذي وقع في بداية عام ٢٠٢٠ وقتل قاسم سليماني من المرجح أنّ السنوات القادمة ستشهد حروباً فريدة في الفضاء السيبراني، وأكثر تشدداً بين البلدين. ومن المتوقع أنّ الحرب السيبرانية بين الولايات المتحدة الأمريكية وإيران ستتحول إلى صراعات مدمرة.

٧. ومن المتوقع أن يتيح تولي إبراهيم الرئيسي، رئيساً للبلاد الفرصة لتغيير العلاقة بين البلدين (الولايات المتحدة الأمريكية وإيران) في مجال الفضاء والحروب السيبرانية. وفي ظل التوقعات يرى بعض من المختصين إنّ مدة رئاسته ستكون مجرد امتداد لواقع معهود بين البلدين، بل أكثر من ذلك من الممكن أن تجلب المزيد من التحديات والصراعات للعلاقة بينهما. بينما يرى آخرون أنّ هدف إبراهيم رئيسي الأساس سيكون تحسين العلاقة المستقبلية بين بلاده والولايات المتحدة الأمريكية وتهدءتها بشكل عام، ونرى أنّ هذا الموضوع ذو أهمية بالغة يمكن دراسته من قبل باحثين آخرين.

DOI:https://doi.org/10.26750/Vol(8).No(4).Paper14 http://journal.uor.edu.krd/index.php/JUR Vol.8. No.4,December.2021

The Effect of Cyber Warfare on Raising the Level of Conflict Between the United States of America and Iran

Bakhan Ako Najmaddin
Department of Politics and International Relations, College of Political Sciences, University of Sulaimani, Sulaimani, Kurdistan Region, Iraq.
E-mail: bakhan.najmadin@univsul.edu.iq

Abstract:

Modern technologies and communication systems are tools to make human life easier, and they have started a revolution in the fields of international securities and international relations. However, modern technologies and cyberspace have to be considered as causes of serious damages, dangers, and represent a serious risk in international security. Cyberspace is accounted as the fifth sphere for the conduct of combat besides land, water, air and space. Cyberspace has occurred in a very new and unique type of war, which is called cyber war. Nowadays, protecting cyberspace becomes a vital part of the national level strategies because cyber war under the shadow of cyberspace is a real phenomenon in international relations, and the United States and Iran's cyber war is the obvious example. Both countries attempt to attack the infrastructure of the other side's information technology and network communication systems in order to cause serious damage financially, economically, politically and militarily. Consequently, cyber war is likely to become the most characterized in the twenty-first century and future military operations.

Keywords: Cyber War, the United States, Iran, Cyberspace, Conflict.

المصادر:

بكر، ياسر (٢٠١٧) حرب المعلومات، دار الكتب المصرية، القاهرة، الطبعة الثانية.

توفلر، آلفين (١٩٩٥) تحوّل السّلطة: المعرفة والثروة والعنف على أعتاب القرن الحادي والعشرين، ترجمة: لبنى الريدى، الهيئة المصرية العامة للكتاب، القاهرة.

جلعود، وليد غسان سعيد (٢٠١٣) دور الحرب الإلكترونية في الصراع العربي الإسرائيلي، رسالة ماجستير، جامعة النجاح الوطنية، فلسطين. متاح على الرابط: https://scholar.najah.edu/sites/default/files/وليد%٢٠جلعود.pdf (تاريخ الزيارة: ٢٧-٣-٢٠٢٠).

دحماني، سليم (٢٠١٨) أثر التهديدات "السيبرانية" على الأمن القومي الولايات المتحدة الأمريكية -أنموذجا- (٢٠٠١-٢٠١٧)، رسالة ماجستير، جامعة محمد بوضياف - المسيلة، كلية الحقوق والعلوم السياسة. متاح على الرابط: سليم دحماني - أثر التهديدات السيبرانية على الأمن القومي(univ-msila.dz).pdf (تاريخ الزيارة: ٤-٤-٢٠٢٠).

راشد، باسم (٢٠١٦) نمو متصاعد للقدرات الإيرانية في مجال الحرب الإلكترونية، المعهد الدولي للدراسات الإيرانية. متاح على الرابط: https://rasanah-iiis.org/مركز-الدراسات-و-البحوث/نمو-متصاعد-القدرات-الإيرانية-في-مجال-ا/ (تاريخ الزيارة: ٣٠-٣-٢٠٢٠).

راشد، باسم (٢٠١٤) بين الدفاع والهجوم: التطورات الإيرانية في مجال الحرب الإلكترونية، مركز المستقبل للأبحاث والدراسات المتقدمة. متاح على الرابط: https://futureuae.com/ar/Mainpage/Item/783/بين-الدفاع-والهجوم-التطورات-الإيرانية-في-مجال-الحرب-الإلكترونية (تاريخ الزيارة: ٥-٤-٢٠٢٠).

رجب، على (٢٠١٩) صراع "الكيبورد" .. كيف تدير أمريكا الحرب الإلكترونية ضد إيران؟، مركز المرجع لدراسات وأبحاث استشرافية حول الإسلام الحركي. متاح على الرابط: https://www.almarjie-paris.com/9314 (تاريخ الزيارة: ٦-٤-٢٠٢٠).

شكر، عمر حامد (٢٠١٩) المجال الخامس - الفضاء الإلكتروني، المعهد المصري للدراسات.

شلوش، نورة (٢٠١٨) القرصنة الالكترونية في الفضاء السيبراني "التهديد المتصاعد لأمن الدول"، مجلة مركز بابل للدراسات الانسانية، المجلد ٨، العدد ٢.

العامري، كرار محمد جواد (٢٠٢٠) دور تكنولوجيا المعلومات والاتصالات في التفاعلات الدولية بداية الألفية الثالثة، رسالة الماجستير، كلية العلوم السياسية، جامعة الكوفة، العراق.

عبد الصادق، عادل (٢٠١٦) أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني، مكتبة الإسكندرية، الإسكندرية.

عبد اللطيف، سامر مؤيد (٢٠١٥) الحرب في الفضاء الرقمي رؤية مستقبلية، مجلة رسالة الحقوق، العدد الثاني، السنة السابعة.

على، خالد حنفى (نيسان ٢٠١٧) إشكاليات تداخل الصراعات السيبرانية والتقليدية، مجلة السياسة الدولية، العدد ٢٠٨، المجلد ٥٢، مؤسسة الاهرام.

غيدان، سرى غضبان والربيعي، محمد منذر جلال (كانون الأول ٢٠٢٠) الامن السيبراني وسياسات المواجهة الدولية، مجلة الدراسات الاستراتيجية والعسكرية، العدد ٩، المجلد ٢، المركز الديمقراطي العربي - برلين.

الفتلاوي، أحمد عبيس نعمة (٢٠١٦) الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مجلة المحقق الحلي للعلوم القانونية والسياسية، العدد ٤، السنة الثامنة.

فرحات، علاء الدين (كانون الأول ٢٠١٩) الفضاء السيبراني: تشكيل ساحة المعركة في القرن الحادي والعشرين، مجلة العلوم القانونية والسياسية، المجلد ١٠، العدد ٣.

كيسنجر، هنري (٢٠١٥) النظام العالمي: تأملات حول طلائع الأمم ومسار التاريخ، ترجمة: د. فاضل جتكر، دار الكتاب العربي، بيروت.

هاشم، أحمد (٢٠٢٠) هل تهاجم إيران أمريكا إلكترونيا ردا على مقتل سليماني؟. متاح على الرابط: هل تهاجم إيران أمريكا إلكترونيا ردا على مقتل سليماني؟(al-ain.com) تأريخ الزيارة (٢٠-٥-٢٠٢١).

Andress, Jason and Winterfeld, Steve (2011) Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners, ELSEVIER, London.

Arquilla, John and Ronfeldt, David (Spring 1993) Cyberwar is Coming!, Comparative Strategy, Vol. 12, No. 2.

Barlow, John Perry (1996) A Declaration of the Independence of Cyberspace. Available at: A Declaration of the Independence of Cyberspace | Electronic Frontier Foundation (eff.org) (Accessed: 17-5-2021).

Clarke, Richard, A. and Knake, Robert. (2010) Cyber War: The Next Threat to National Security and What to Do About It, HarperCollins, New York.

DOI:https://doi.org/10.26750/Vol(8).No(4).Paper14 http://journal.uor.edu.krd/index.php/JUR Vol.8. No.4,December.2021

Craig, Anthony and Valeriano, Brandon (2016) Conceptualising Cyber Arms Races, NATO CCD COE Publications, Tallinn.

Greathouse, Craig B. (2013) Cyber War and Strategic Thought: Do the Classic Theorists Still Matter?. Cyberspace and International Relations, Springer, Berlin.

Gibson, William (1989) Neuromancer, Berkley Publishing Group, New York.

Goujon, Reva. (2018) The global race for Al supremacy: The geopolitics of artificial intelligence competition. Bled Strategic Times. Available at: BSF-Bled-Strategic-Times_2018.pdf (bledstrategicforum.org) (Accessed: 18-5-2021).

Hildreth, Steven A. (2001) Cyberwarfare, CRS Report for Congress. Available at: https://fas.org/sgp/crs/intel/RL30735.pdf (Accessed: 10-4-2020).

Hodgson, Quentin E., Ma, Logan, Marcinek, Krystyna and Schwindt, Karen (2019) Fighting Shadows in the Dark: Understanding and Countering Coercion in Cyberspace, RAND, California.

Hruza, Petr and Cerny, Jiri (June 2017) Cyberwarfare, International Conference KNOWLEDGE-BASED ORGANIZATION, Vol. 23, No. 1.

Paulo Shakarian, Jana Shakarian, and Andrew Ruef (2013) Introduction to Cyber-warfare: A Multidisciplinary Approach, Newnes, Waltham.

Perlroth, Nicole. (2012) Attacks on 6 Banks Frustrate Customers. The New York Times. Available at: Cyberattacks on 6 American Banks Frustrate Customers - The New York Times (nytimes.com) (Accessed: 20-5-2021).

Rao, Siddharth Prakash Rao (2014) Stuxnet, A new Cyberwar Weapon: Analysis from a technical point of view. Available at: https://www.researchgate.net/publication/267156195_Stuxnet_A_new_Cyberwar_weapon_Analysis_from_a_technical_point_of_view (Accessed: 10-4-2020).

Sabet, Farzan and Safshekan, Roozbeh (2013) Soft War: A new episode in the old conflict between Iran and the United States, Pennsylvania, University of Pennsylvania.

Schreier, Fred (2015) Geneva Centre for the Democratic Control of Armed Forces, No. 7.

The BBC Persian (2010) Structure of Iran's Cyber Warfare. Available at: https://nligf.nl/v1/upload/pdf/Structure_of_Irans_Cyber_Operations.pdf (Accessed: 30-3-2020).

The New York Times (2009) Text: Obama's Remarks on Cyber-Security. Available at: Text: Obama's Remarks on Cyber-Security - The New York Times (nytimes.com) (Accessed: 19-5-2021).

U.S. Cyber Command. Available at: Command History (cybercom.mil) (Accessed: 3-5-2021).

Ventre, Daniel (2016) Information Warfare, 2nd edition, 2016, WILEY, London.

White, Colonel Kenneth C. (1998) Cyber-Terrorism: Modern Mayhem, USAWC Strategy Research Project, Pennsylvania.

Wiener Norbert (1961) Cybernetics or control and communication in the animal and the machine, The M.I.T. Press, Cambridge, 2nd edition.