The Role Of Cyber Security In The Iranian Security Strategy

Dr Louay Sayouh*
Dr. Rami Laika **
Ramadan Al Houshi ***

(Received 30 / 7 / 2022. Accepted 30 / 10 / 2022)

□ ABSTRACT □

This study addresses the issue of the change in the concept of security threats due to developments in the field of technology, as the issue of cyber security has become one of the major challenges faced by countries at the regional and global levels, especially with the increasing volume of cyber threats that affect the information security of countries.

Today, cyber security is one of the most important concepts that countries seek to achieve, especially after technological progress and the extent of the impact of this progress on the national security of countries, which necessitated the development of defensive security strategies to repel cyber-attacks and work to develop the cyber capabilities of countries.

This study will focus on the most important concepts in cyberspace and the main actors in the practice of cyber-attacks, in addition to identifying the Iranian security strategy in the cyber field.

The study reached results and recommendations, the most important of which is that cyberspace has become a new arena for international conflict and the need to develop defensive strategies to repel and detect cyber attacks.

Keywords: cyber, cyber space, cyber-attacks, cyber security, security threats**.**

***Professor - The Department Of Economics And Planning, International Relations, Faculty Of Economics, Tishreen University, Lattakia, Syria.**

****Assistant Professor - The Department Of Economics And Planning, International Relations, Faculty Of Economics, Tishreen University, Lattakia, Syria.**

*****Postgraduate Student - The Department Of Economics And Planning, International Relations, Faculty Of Economics, Tishreen University, Lattakia, Syria.**

دور الأمن السيبراني في الإستراتيجية الأمنية الإيرانية

الدكتور لؤي صيوح*
الدكتور رامي لايقة **
رمضان الهوشي ***

(تاريخ الإيداع 30 / 7 / 2022. قُبِل للنشر في 30 / 10 / 2022)

□ ملخّص □

يعد الأمن السيبراني اليوم من أهم المفاهيم التي تسعى الدول إلى تحقيقها لاسيما بعد التقدم التكنولوجي، ومدى تأثير هذا التقدم على الأمن القومي للدول، مما استدعى إلى وضع إستراتيجيات أمنية دفاعية لصد الهجمات السيبرانية (cyber–attacks) والعمل على تطوير القدرات السيبرانية للدول.

تعالج هذه الدراسة مسألة التغير في مفهوم التهديدات الأمنية الحاصلة بسبب التطورات في مجال التكنولوجيا، حيث أصبحت قضية الأمن السيبراني(cyber security) ،من التحديات الكبرى التي توجهها الدول ،على الصعيدين الإقليمي والعالمي، لا سيما مع تزايد حجم التهديدات السيبرانية (Cyber threats) التي تصيب أمن معلومات الدول.

سيتم التركيز في هذه الدراسة على أهم المفاهيم في الفضاء السيبراني (cyber space)، والفواعل الرئيسية في ممارسة الهجمات السيبرانية، إضافة إلى التعرف على الإستراتيجية الأمنية الإيرانية في المجال السيبراني.

توصلت الدراسة إلى نتائج وتوصيات: أهمها أصبح الفضاء السيبراني ساحة جديدة للصراع الدولي، وضرورة وضع إستراتيجيات دفاعية لصد وكشف الهجمات السيبرانية.

الكلمات المفتاحية: السيبرانية، الفضاء السيبراني، الهجمات السيبرانية، الأمن السيبراني، التهديدات الأمنية.

***أستاذ – قسم الاقتصاد والتخطيط، اختصاص علاقات دولية، كلية الاقتصاد، جامعة تشرين، اللاذقية–سورية.**
****مدرس – قسم الاقتصاد والتخطيط، اختصاص علاقات دولية، كلية الاقتصاد، جامعة تشرين، اللاذقية–سورية.**
*****طالب ماجستير – قسم الاقتصاد والتخطيط، اختصاص علاقات دولية، كلية الاقتصاد، جامعة تشرين، اللاذقية–سورية.**

مقدمة:

تزايدت العلاقة بين الأمن والتكنولوجيا ومعها تزايدت إمكانية تعرض المصالح الإستراتيجية للدولة للتهديدات السيبرانية، وهددت بتحول الفضاء السيبراني لوسيط ومصدر لأدوات جديدة للصراع الدولي المتعدد الأطراف ، وأحدثت تكنولوجيا المعلومات والاتصالات ثورة شاملة في جميع نواحي الحياة ،إذ تزداد المخاطر السيبرانية في غالب الأحيان كلما زادت هيمنة تكنولوجيا المعلومات والاتصالات على النسق العام للحياة، فأصبحنا أمام جرائم حقيقية ومتكاملة الأركان تتم عن طريق شبكات الإنترنت ، و أجهزة الحاسوب بأشكال متعددة مثل: الهجمات والقرصنة السيبرانية ،باعتبارها الجرائم الأكثر شيوعاً في العالم الرقمي.

خلال العقد الأخير شهد المجتمع الدولي، بروز مجال جديد وبيئة جديدة مؤثرة في حركة التفاعلات والتحولات في العلاقات الدولية تضاف إلى البيئات الأربع السابقة (الأرض، الجو، البحر، الفضاء الخارجي)، أطلق على هذا البعد الفضاء السيبراني، والذي أصبح جزءاً أصيلاً من عمل الدول ومن بنيتها التحتية.

وتستخدم العديد من الدول القدرات التي يوفرها هذا الفضاء، لاعتبارات في مقدمتها الأمن والقوة العسكرية، نظراً لأن زيادة الاعتماد على الفضاء السيبراني، في جميع القطاعات العامة والخاصة وكذلك العمليات الحكومية.

إن العلاقة بين الأمن السيبراني والأمن القومي تزداد، كلما ازداد نقل المحتوى المعلوماتي، والعسكري، والأمني، والفكري والسياسي، والاجتماعي، والاقتصادي، والخدمي، والعلمي، والبحثي، إلى الفضاء السيبراني، خاصة مع التسارع في تبني الحكومات الإلكترونية والمدن الذكية في العديد من الدول.

حيث توجهت إيران إلى وضع إستراتيجية أمنية شاملة من أجل ضمان الأمن السيبراني ، لأن الأمن السيبراني يعد ضمن الأمن الوطني الشامل، فأجهزة الأمن السيبرانية الإيرانية تدرك أن التغيرات المتسارعة في التكنولوجيا تؤدي إلى خلق تهديدات ليست بالسهلة، لذلك لابد من ضرورة العمل على ضمان أمن المعلومات وشبكات الإنترنت من خلال خطوات مهمة، تعتمد على مجموعة كبيرة من وسائل قانونية وتقنية لمقاومة الاستخدام غير الشرعي للشبكة العنكبوتية ،من أجل حماية نظم المعلومات ووسائل الاتصالات لحماية المؤسسات المدنية والعسكرية من الهجمات السيبرانية .

الدراسات السابقة:

1-دراسة (صالحي – 2021) بعنوان: القوة الذكية التنافس العالمي على قوة الفضاء الإلكتروني والقدرات السيبرانية، مقال علمي محكم منشور في مجلة دفاتر السياسة و القانون ، جامعة عباس لغرور خنشلة ، الجزائر ،هدفت هذه الدراسة إلى تسليط الضوء على تأثير تكنولوجيا الاتصالات والمعلومات، في التفاعل بين الفواعل الأساسية في السياسة الدولية (الدول)، وتأثيره في تحول القوة ، وهذا أدى إلى ظهور مبادئ جديدة في النظام الدولي (الفضاء السيبراني) ،وأشكال جديدة من أشكال القوة (القوة السيبرانية)، ونوع جديد من التهديدات (التهديدات السيبرانية) ،واستخدمت الدراسة المنهج الوصفي التحليلي.

توصلت الدراسة إلى أن ثورة المعلومات والاعتماد على التقنيات المتطورة ساهم في تغير العديد من المفاهيم التقليدية المتعلقة بالعلاقات الدولية، بدأً من وحدات التفاعل في العلاقات الدولية، حيث لم تعد الدولة الفاعل الوحيد في ظل قدرات فواعل أخرى، وسعي الدول إلى تنمية القدرات السيبرانية ، ووضع إستراتيجيات لمواجهة التهديدات السيبرانية في المستقبل.

2-دراسة (العوفي ،2021) بعنوان: الحرب السيبرانية في عصر الذكاء الاصطناعي ورهاناتها على الأمن الدولي، مقال علمي منشور في مجلة الحكمة للدراسات السياسية، جامعة الجزائر.

هدف البحث إلى معالجة موضوع الحروب السيبرانية، التي فرضت نفسها كبديل عن الحروب التقليدية، وأثر الذكاء الاصطناعي على الحرب السيبرانية، واستخدمت الدراسة المنهج الوصفي التحليلي.

توصلت الدراسة إلى نتائج أهمها: أصبح الفضاء السيبراني جزء مهم من التفاعلات الدولية، ظهور تحالفات دولية جديدة في مجال القوة السيبرانية.

3-دراسة (رشاد ،2022) بعنوان: التهديدات الهجينة في العلاقات الدولية (السيبرانية والذكاء الاصطناعي)، بحث علمي منشور في مجلة وادي النيل للدراسات والبحوث الإنسانية، جامعة 6أكتوبر.

هدفت الدراسة إلى دراسة التهديدات الأمنية، في العلاقات الدولية طبيعتها وخصائصها، إضافة إلى مفهوم السيبرانية والذكاء الاصطناعي، وانعكاساتها على العلاقات الدولية، واعتمدت الدراسة على المنهج الوصفي التحليلي.

توصلت الدراسة إلى نتائج أهمها: إن التقدم التكنولوجي والتقنيات الحديثة فرض وسائل جديدة على العمليات العسكرية وبالتالي زيادة التهديدات على الأمن القومي للدول.

تتميز الدراسة الحالية عن الدراسات السابقة في أن ستقدم جانب تطبيقي مع ذكر الإستراتيجية الإيرانية في مجال الفضاء السيبراني ومعرفة أهم الهجمات السيبرانية التي لها إيران.

مشكلة البحث:

تكمن مشكلة البحث في انعكاس التطورات والمتغيرات التكنولوجية، على شكل التهديدات الأمنية، وظهور أشكال جديد من التهديدات المتمثلة بالهجمات السيبرانية، مما أدى إلى تعزيز دور الأمن السيبراني في وضع استراتيجيات في مجال الفضاء السيبراني. استناداً لما سبق يمكن صياغة مشكلة البحث في السؤال الرئيسي:

كيف وظفت إيران تقدمها في مجال الأمن السيبراني في وضع إستراتيجية أمنية لصد الهجمات السيبرانية؟

يتفرع عن السؤال الرئيسي عدة أسئلة فرعية:

1-ما هو مفهوم السيبرانية؟

2-ماهي مظاهر التهديدات السيبرانية وما علاقتها بالأمن القومي للدول؟

3-ماهي أهم الاستراتيجيات الأمنية الإيرانية في مجال الأمن السيبراني ؟

أهمية البحث وأهدافه:

تأتي أهمية الدراسة من كونها تناقش قضية حديثة على الساحة الدولية، وهي قضية الأمن السيبراني، وأثرها على الإستراتيجية الأمنية للدول، إضافة إلى دراسة المفاهيم الأساسية المرتبطة بالفضاء السيبيراني.

إن هذه الدراسة لها أهمية عملية تتمثل في تزايد تأثير التهديدات والهجمات السيبرانية على الأمن القومي للدول، وخاصة إيران.

وتكمن أهداف البحث:

1-يهدف البحث إلى دراسة المفاهيم الأساسية المرتبطة بالأمن والفضاء السيبراني، وتوضيح العلاقة بين الأمن السيبراني والأمن القومي للدول.

2-التعرف على الظاهرة واقعياً بدراسة حالة إيران، ومحاولة فهم وإبراز أهم الهجمات التي تعرضت لها، والتعرف على الإستراتيجية الأمنية السيبرانية الإيرانية، ودور الأمن السيبراني في وضع هذه الإستراتيجية.

فرضيات البحث:

1- هنالك علاقة ذات دلالة معنوية بين التقدم الذي حققته إيران في المجال التقني ومواجهها للهجمات السيبرانية .

2- هنالك علاقة طردية بين زيادة الأمن السيبراني وقدرة الدولة على التقليل من المخاطر السيبرانية .

حدود الدراسة:

الحدود الزمانية: الفترة من 2010 إلى 2021.

الحدود المكانية: إيران.

منهجية البحث:

يعتمد البحث على المنهجين:

المنهج الوصفي التحليلي: يقوم المنهج الوصفي التحليلي، على وصف وتحليل ماهية الأمن السيبراني بتحليل واقعي، والتعرف على الإستراتيجية الإيرانية في مجال الأمن السيبراني، للوصول إلى النتائج واقتراح التوصيات.

اسلوب دراسة الحالة: وقد استخدم في الدراسة من خلال اعتماد إيران كنموذج، لنوضح من خلاله مدى تأثير الأمن السيبراني في الإستراتيجية الأمنية، ومعرفة الهجمات السيبرانية التي تعرضت لها.

النتائج المناقشة:

1- مفهوم السيبرانية:

أُطلق العديد من المصطلحات والمفاهيم على الهجمات السيبرانية، فقد أطلق مصطلح الحرب الافتراضية، أو الحرب السيبرانية، أو الحرب الإلكترونية على الهجمات السيبرانية، التي تتم من خلالها قيام القراصنة بمهاجمة الملفات والمواقع التي تخص الآخرين، كمهاجمة المواقع الإلكترونية للمنشآت المهمّة، أو مهاجمة الحواسيب التابعة للوحدات العسكرية، أو الوحدات الاقتصادية لدول معيّنة بقصد تدميرها والسيطرة عليها والإضرار بها. [1]ترتبط نشأة الهجمات السيبرانية بحدثين مهمين هما:[2]

الأول: استخدام أجهزة الكمبيوتر قي منتصف خمسينيات القرن الماضي، كأداة لحفظ المعلومات رقمياً، حيث أصبح للحاسب دور أساسي في عمل الشركات والأفراد.

الثاني: ظهور الشبكة العنكبوتية والتي أحدثت انقلاباً في حياة الأفراد، من خلال التواصل وسرعة نقل المعلومات.

1-1-تعريف السيبرانية لغةً:

لم تشر أغلب معاجم اللغة الحديثة إلى مصدر كلمة السيبرانية، ويتضح من ذلك أن السيبرانية، هي مصطلح يوناني، الأصل وترجع إلى مصطلح(kybemetes) ،الذي ورد في مؤلفات الخيال العلمي ويعني القيادة والتحكم عن بُعد ،فقد ورد في قاموس المورد تعريف السببرانية حيث عرّفها بأنها: علم الضبط. [1]

مصدرها(Cybernetics) وهو مصدر يتطابق مع مفهوم الهجمات السيبرانية أي ضبط الأشياء عن بعد والسيطرة عليها، بينما قاموس مصطلح الأمن المعلوماتي فقد عرف السيبرانية بقوله بأنها: هجوم عبر الفضاء السيبراني يهدف إلى السيطرة على المواقع الإلكترونية، أو البنى المحميّة إلكترونياً لتعطيلها، أو تدميرها أو، الإضرار بها. [1]

1-2-تعريف الهجمات السيبرانية اصطلاحاً:

تعددت التعريفات التي تناولت مصطلح الهجمات السيبرانية، على ضوء الاجتهادات الفقهية والممارسات العملية الدولية، فالهجمات السيبرانية مصطلح يُستخدم من قبل فئات عديدة من الناس، للإشارة إلى أشياء مختلفة كالإشارة إلى وسائل القتال وأساليبه تلك التي تتألف من عمليات في الفضاء السيبراني .[1].

تعرف الهجمات السيبرانية بأنها: مجموعة من الإجراءات التي تتخذها الدولة للهجوم، على نظم المعلومات بهدف التأثير والإضرار بها، وفي الوقت نفسه الدفاع عن نظم المعلومات الخاصة بالدولة المُهاجمة، بينما هناك من أشار إلى أن المقصود بها هو :هجوم عبر الإنترنت يقوم على التسلل إلى مواقع إلكترونية غير مرخص الدخول إليها، بهدف تعطيل البيانات المتوفرة فيها، أو إتلافها، أو الاستحواذ عليها، وهي عبارة عن سلسلة هجمات سيبرانية تقوم بها دولة ضد أخرى. [1]

2-مفاهيم في الفضاء السيبراني :

2-1-مفهوم الحرب السيبرانية:

كانت حرب الفضاء غير واضحة المعالم في تسعينيات القرن الماضي، لأنها كانت مختلطة مع الحروب النفسية والدعائية، وكانت مقصورة على عمليات التشويش على أنظمة الرادار وأجهزة الإنذار، في حين أن اتساع شبكة الإنترنت فتح أفاق كبيرة للأجهزة المخابراتية، لاستغلال هذه الشبكة في حروبها الدولية، والتغلغل في أي شبكة من شبكات الإنترنت، والسيطرة على هذه الشبكة وتعطيلها، أو تغيير البيانات عليها، أو إتلافها، أو التحكم فيها من خلال الضغط على بضعة أزرار. [3]

يمكن تعريف الحرب السيبرانية (cyber war)على أنها: هجوم متعمد بغرض تعطيل عمل، أو خداع، أو إضعاف أو تدمير أنظمة الكمبيوتر وشبكات الاتصالات والمعلومات والبرامج الموجودة في تلك الأنظمة، أو الشبكات التي تمر من خلالها. [4]

2-2-مفهوم الفضاء السيبراني:

فرضت الثورة التكنولوجية مجموعة من التحديات والتهديدات الأمنية الجديدة، وبرز في النظام الدولي ما يعرف بالفضاء السيبراني، الذي أثر بدوره على التفاعلات السياسية والدولية الحاصلة بين مختلف الفاعلين في العلاقات الدولية المعاصرة، وحتى على المستوى الوطني.[5]

تم تعريف الفضاء السيبراني بأنه مجال عالمي داخل بيئة المعلومات يتكون من شبكة مترابطة من البنى التحتية لتكنولوجيا المعلومات، بما في ذلك الإنترنت وشبكات الاتصالات وأنظمة الكمبيوتر والمعالجات ووحدات التحكم المضمنة، كما يشار إليه بوصفه مكاناً مادياً، فهو مصطلح مختصر يشير إلى البيئة التي يتم إنشاؤها عن طريق التقاء الشبكات التعاونية من أجهزة الكمبيوتر وأنظمة المعلومات والبنى التحتية للاتصالات التي يشار إليها عادة باسم شبكة الويب العالمية. [6]

2-3-مفهوم الأمن السيبراني:

يعرف الأمن السيبراني: بأنه أمن الشبكات والأنظمة المعلوماتية، والبيانات، والمعلومات، والأجهزة المتصلة بالإنترنت، وعليه فهو المجال الذي يتعلق بإجراءات، ومقاييس، ومعايير الحماية المفروض اتخاذها، أو الالتزام بها، لمواجهة التهديدات، ومنع التعديات أو على الأقل الحد من أثارها. [7]

3-الفواعل الأساسية في الفضاء السيبراني:

يمكن تقسيم الفواعل في الفضاء السيبراني ومن لديهم القدرة على الفعل السيبراني، أو شن الهجمات السيبرانية إلى ما يلي:

A. **الدول:** والتي لديها قدرة كبيرة على تنفيذ هجمات سيبرانية، وتطوير البنية التحتية، وممارسة السلطات داخل حدودها.[7]

B. **الفاعلون من غير الدول:** ويستخدم هؤلاء الفاعلون القوة السيبرانية لأغراض هجومية بالأساس، إلا أن قدرتهم على تنفيذ أي هجوم سيبراني مؤثر تتطلب مشاركة ومساعدة أجهزة استخباراتية متطورة، ولكن يمكنهم اختراق المواقع الإلكترونية واستهداف الانظمة الدفاعية ومنهم.

C. **الأفراد :**

الأفراد هم الذين يملكون معرفة إلكترونية ويستطيعون توظيفها، ولكن تصعب ملاحقتهم والكشف عن هويتهم، حيث أصبح الفرد بفضل الفضاء السيبراني فاعلاً مؤثراً في العلاقات الدولية، كما أن هناك أفراد مختصون في أعمال القرصنة، أو الجرائم السيبرانية وسرقة المعلومات والبيانات الشخصية والتلاعب فيها، أو استغلالها لتحقيق مصالحهم. [8]

D–**المنظمات الإرهابية والإرهاب السيبراني:**

تعد المنظمات الإرهابية من أبرز الفواعل الدولية، خاصة بعد أحداث 11 أيلول عام 2001حيث تستغل الفضاء السيبراني في عمليات التجنيد، والتعبئة، والدعاية، وجمع الأموال، والمتطوعين، كما تحاول جمع المعلومات حول الأهداف العسكرية وكيفية التعامل مع الأسلحة وتدريب المجندين الجدد عن بعد، رغم أنها لم تصل بعد إلى مرحلة القيام بهجوم سيبراني حقيقي على منشآت البنية التحتية للدول. [8]

E–**المجموعات الافتراضية:** وهي المجموعات التي تعرف بالقراصنة المجهولون، وهم جماعات احتجاجية منتشرة حول العالم داخل الفضاء السيبراني، لهم أهداف سياسية، من أبرز وظائفهم توزيع المعلومات السرية، وتشويه المواقع وتوليد احتجاجات حول القضايا السياسية ،وهم نمط جديد من الفاعلين السياسيين الذين يعتمدون على إخفاء الهوية والقيام بهجمات سيبرانية ضد أهداف مادية وحيوية من أجل تشجيع التغيير السياسي. [3]

F–**الشركات متعددة الجنسيات:** تمتلك بعض شركات التكنولوجيا موارد للقوة تفوق قدرة بعض الدول، ولا تنقصها سوى شرعية ممارسة القوة التي مازالت حكراً على الدول. [7]

4–التهديدات الأمنية السيبرانية:

إن تحديد مفهوم التهديد من الناحية اللغوية يعبر عن نية إلحاق الاذى والضرر للغير، ومصطلح التهديد في مفهومه الإستراتيجي، هو بلوغ تعارض المصالح والغايات القومية مرحلة يتعذر معها إيجاد حل سلمي يوفر للدول الحد الأدنى من أمنها السياسي، والاقتصادي، والاجتماعي، والعسكري، مقابل قصور قدراتها لموازنة الضغوط الخارجية الأمر الذي قد يضطر الأطراف المتصارعة إلى اللجوء إلى استخدام القوة العسكرية معرضة الأمن القومي للخطر. [9]

إن العلاقة بين مفهومي (الأمن والتهديد) علاقة تأثير متبادل، وأي محاولة لتفسير الأمن لابد أن تبدأ بتحديد مصادر التهديد، وقد ركزت الدراسات الأمنية في السابق على خطر الغزو العسكري باعتباره أهم مصادر تهديد الأمن، بيد أن الدراسات الحديثة ذهبت إلى وجود مصادر أخرى للتهديد، تتمثل في التهديدات السياسية، والاقتصادية، والاجتماعية، والسيبرانية، والبيئية ببعديها الداخلي والخارجي. [10]

تتعدد أشكال التهديدات السيبرانية وتختلف من حيث الطبيعة، والمصادر، والأهداف، كالتجسس، وسرقة المعلومات، وشن الحروب، وبالتالي بات العديد من الفواعل الدوليين يلجئون إلى آليات إلكترونية لتحقيقها ومنها:

A. التجسس السيبراني: هو ذلك التجسس الذي يعتمد على استخدام التقنيات الإلكترونية، في الحصول على معلومات، ويختلف التجسس السيبراني من حيث النوع فهناك التجسس عن طريق الأفراد، ومن خلال الشبكات السلكية، أو التجسس من خلال الأقمار الصناعية. [11]

B. القرصنة السيبرانية: تتمثل في عملية نسخ البرمجيات غير المصرح بها، أو إعادة إنتاجها، أو استخدامها، أو تصنيع نسخ بطريقة غير شرعية، أو نشر وتوزيع المنتج البرمجي، أو استغلاله على نحو مادي، أو تقليدها أو محاكاتها والانتفاع بها على نحو يخل بحقوق الدول والمؤسسات بدون الحصول على إذن تفويض. [12]

C. إتلاف المعلومات أو تعديلها :يقصد بها الوصول إلى معلومات الضحية عبر شبكة الإنترنت، أو الشبكات الخاصة، والقيام بعملية تعديل البيانات الهامة دون أن يكتشف الضحية ذلك، فالبيانات تبقى موجودة لكنها مضللة قد تؤدي إلى نتائج كارثية خاصةً إذا كانت خطط عسكرية، أو مواعيد، أو خرائط سرية.[7]

D. الإرهاب السيبراني: المقصود بالإرهاب السيبراني هو ذلك الاستخدام للموارد المعلوماتية المتمثلة في الإعلام، وأجهزة الحاسوب وشبكة الإنترنت، والفضائيات من أجل أغراض التخويف، أو الإرغام لأغراض متعددة. [11]

5-تأثير التهديدات السيبرانية على الأمن القومي للدول:

لم يعد مبدأ السيادة يقتصر على الأبعاد السياسية فحسب كما كان الحال عليه في القرنين الماضيين، بل تعداه اليوم ليشمل بعداً تقنياً جديداً يضاف إلى معناه الأصلي المتعارف عليه، كما أن العولمة تؤثر على ثقافات دول العالم المختلفة فظهور التقنيات الحديثة، أدى إلى سهولة النفاذ إلى حدود الدولة، واختراق سيادتها وخاصة بالنسبة للدول النامية. [13]

كغيرها من الظواهر الجديدة فرضت الثورة المعلوماتية مجموعة من التهديدات على الأمن القومي للدول بسبب التنامي السريع لمعطيات هذه الثورة، والتدفق السريع والحر للمعلومات، وسواءً تعلق هذا التهديد بتطور التكنولوجي فإنه يمكننا القول إن اتساع قضية الأمن السيبراني، على هذا النحو الخطير عالمياً وعربياً يعود إلى أمرين هما:[14]

الأول: أن أغلب دول العالم ترفع شعار التحول إلى مجتمع المعلومات والمعرفة والرقمنة.

الثاني: أن تشييد بنية معلوماتية قوية واسعة المجال وتبني التوجه نحو مجتمع المعلومات، يحتم على الدولة مواجهة التحديات الشاملة واسعة النطاق في مجال السايبر.

أصبحت الهجمات السيبرانية مصدر قلق للأمن القومي، وأداة جديدة قي السياسة الخارجية تستلزم التكيف السريع معها، عبر تطوير القدرات العسكرية ،والاستخباراتية السيبرانية وتماشياً مع هذا الوضع الجيوسياسي قامت القوى الكبرى بتكيف إستراتيجياتها العسكرية مع خصائص البيئة السيبرانية ،وباتت الدول في خضم سباق تسلح سيبراني متسارع، سباق له العديد من الأثار السياسية والإستراتيجية التي تفرض الحاجة إلى إيجاد إجابات سياسية على وجه التحديد لفهم الفضاء السيبراني كمجال سياسي وأمني جديد .[15]

وبالتالي تواجه الدول تحديات عديدة أمام اعتماد سيادتها السيبرانية أهمها.[16]

1. الاعتراف بالفضاء السيبراني كمجال سيادي، وكون الدول تمارس سلطة عليه فوجوده يتطلب هندسة مادية وبحاجة إلى قانون لكي يعمل بفاعلية.

2. خلق نظام قادر على تحديد اللاعبين في الفضاء السيبراني بدقة، وهو مهمة شاقة نظراً لعدم القدرة على إسناد مسؤولية الهجمات السيبرانية إلى طرف محدد بنسبة صحيحة، لذلك يبدو أن الدول مترددة في قبول المسؤولية عن الأنشطة السيبرانية الناشئة من أراضيها.

3. رسم حدود الفضاء السيبراني بشكل تستطيع الدولة مراقبته والتحكم فيه، فعدم التمكن من القيام بهذه الوظيفة يفرغ الفضاء السيبراني من مضمونه.

6-دور الأمن السيبراني في الإستراتيجية الأمنية الإيرانية:

لقد وضعت إيران الأمن السيبراني أحد أولوياتها على غرار باقي دول العالم، التي سارعت إلى مراجعة سياساتها الأمنية، وإدراجها آليات جديدة تعني بهذه المسائل، بالمؤازرة مع تطوير البنيات الأساسية المتعلقة بتكنولوجيات العالم الرقمي، لقد أصبح الأمن السيبراني ركن أساسي ضمن العقيدة الأمنية الإيرانية المعاصرة، ولهذا فإن السلطات الإيرانية ملزمة باتخاذ الاحتياطات الأمنية اللازمة لتفادي أي نوع من الجرائم والهجمات السيبرانية.[17]

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

أ- البعد العسكري: تكمن الميزة النسبية للقوة السيبرانية في قدرتها على ربط الوحدات العسكرية ببعضها البعض، عبر الشبكات العسكرية في الفضاء السيبراني، بما يسمح بسهولة تبادل المعلومات وتدفقها، ، والقدرة على إيصال الأهداف عن بعد وتدميرها. [11]

ب-البعد الاقتصادي: يرتبط الأمن السيبراني ارتباطاً وثيقاً بالاقتصاد، لقد أصبح الفضاء السيبراني جاذباً لقطاعات المجتمع كافة، وباتت المعرفة محرك الإنتاج والنمو الاقتصادي، لذلك تركز الدول على التكنولوجيا الحديثة لنهوض بالاقتصاد. [8]

ج-البعد الاجتماعي: يفوق مستخدمي الانترنت 4 مليارات شخص في العالم، منهم أكثر من 2.6 مليار يستخدمون مواقع التواصل، مما يجعلها أكبر تجمع للتفاعل البشري، ويفتح الباب واسعاً لتبادل الأفكار والخبرات الجيدة، لكن في المقابل يعرض أخلاقيات المجتمع للخطر، نظراً لصعوبة مراقبة محتوى الإنترنت، كما يعرض البيانات لعمليات اختراق خارجي. [7]

د-البعد السياسي: هناك أمثلة كثيرة تدفع نحو الاهتمام بالبعد السياسي للأمن السيبراني، كالتسريبات المختلفة للوثائق الحساسة التي تؤدي إلى مشكلات معقدة على المستوى الخارجي والدولي، علماً أنه لا ينكر أحد الدور الفعال للشبكات التواصل الاجتماعي على المستوى السياسي كحملات انتخابية، تظاهرات افتراضية، حركات احتجاجية إلكترونية. ... كما يتم استغلال هذه المواقع من طرف العديد من الحكومات لتحقيق أهداف سياسية. [8]

هـ-البعد القانوني: إن التطورات التكنولوجية المتسارعة تفرض مواكبة التشريعات القانونية لها، من خلال وضع أطر وتشريعات للأعمال القانونية وغير القانونية في الفضاء السيبراني، فالملاحظ أن الجريمة السيبرانية تفتقد في معظم البلدان إلى الأطر القانونية الصارمة للتعامل معها، إضافة إلى ضرورة تفعيل التعاون الدولي المشترك لمكافحتها. [7]

حيث إن إيران عملت على توظيف تقدمها في مجال الأمن السيبراني في وضع استراتيجية أمنية في المجال السيبراني هدفها كشف وصد الهجمات السيبرانية ،وسعت إيران لبناء قدرات للحرب السيبرانية والاستطلاعية لتحييد القدرات التقنيّة العالية لمنافسيها في المنطقة والعالم، بالاستفادة من الثورة التقنية قليلة الكلفة والتي يمكن الحصول عليها واستعمال تلك القدرات في صد الهجمات السيبرانية، وقد تبنت إيران إستراتيجية تم التجهيز لها منذ عدةَ سنوات وتم بناؤها وإعداد هيكلتها وتطويرها في إطار مؤسسي وفق رؤيةٍ وأهدافٍ وضعتها النخبة الحاكمة. [17]

خاصةً بعد تعرضها لهجوم سيبراني استهدف أحد مواقع الطاقة، وتم الاستهداف بفيروس ستكسنت Stuxnet أدى إلى الحاق الضرر بعدد من وحدات الطرد المركزي.

ويعد هجوم ستكسنت من أبرز الهجمات التي شنتها الولايات المتحدة والكيان الصهيوني ضد إيران، وقد هدف ستكسنت إلى تخريب برنامج إيران النووي، حيث تم إنزال فيروس على برنامج التشغيل الإلكتروني الذي يدير عملية تخصيب اليورانيوم في موقع (نطانز)النووي في عدد كبير من وحدات الطرد المركزي، وقد كان هذا الهجوم متطوراً بالنظر لقدرته على اتخاذ قرارات مستقلة في البيئة المستهدفة بدون التواصل مع الطرف منفذ الهجوم. [4]

وهناك من يرى أن وكالتي الاستخبارات الأمريكية والإسرائيلية استطاعتا تصميم هذا الفيروس، والذي عمل على اختراق وتعطيل المنشآت النووية الإيرانية، كما أن هناك من يرى أن "إسرائيل" قامت لوحدها بشن هذا الهجوم السيبراني، حيث إن الهجوم كان دقيقاً إلى درجة تحديد عدد أجهزة الطرد المركزي، وقد احتاج تفعيل هذا الهجوم مجرد تشغيل أجهزة الكمبيوتر في المنشآت الإيرانية، وبمجرد أن تسلل الفيروس إلى الأجهزة أخفى وجوده واستطاع تعطيل أجهزة الطرد المركزي بمهارة فائقة، حيث عمل على تغيير الضغط داخل أجهزة الطرد المركزي، وجعل سرعة الدورات داخل الأجهزة متفاوتة، مما أدى إلى انهيارها . [18]

فيروس ستكسنت Stuxnet وهو عبارة عن برنامج كمبيوتر خبيث يهاجم أنظمة التحكم الصناعية المستخدمة على نطاق واسع في مراقبة الوحدات التي تعمل آلياً. [18]

وقد خصّصت إيران جزءاً كبيراً من ميزانيتها لتطوير قدراتها السيبرانية، إذ ارتفعت ميزانية الأمن السيبراني الإيراني خلال الأعوام (2013 –2017م) بنسبة 90%ويقول عن ذلك مدير أمن السايبر ونائب رئيس جامعة جورج واشنطن في العام 2017م إن إيران خصّصت خلال السنوات الأخيرة الكثير من الأموال لبناء قدرات سيبرانية، هذا ما جعل إيران واحدة من القوى السيبرانية الكبرى، وكذلك دمجت إيران عمليات السايبر في إستراتيجيتها وعقيدتها العسكرية. [17]

بدأت الهجمات السيبرانية الايرانية ضد الولايات المتحدة الامريكية في عام 2009عندما قام الجيش السيبراني الإيراني بتشويه صفحة تويتر الرئيسية رداً على احتجاجات التي حدثت في إيران.[19]

6-1- الإستراتيجية الأمنية الإيرانية في المجال السيبراني :

وفق هذه الإستراتيجية تقود مؤسسة الحرس الثوري وقوات الباسيج التابعة لها مجموعات من الفصائل الرقمية، التي إما أنها تنتمي إليها بشكلٍ مباشر، أو تدين لها بالولاء، حيث تأسس كياناً افتراضياً منذ العام 2005م وأطلق عليه (جيش فضاء إيران الإلكتروني) الذي يُعد أحد الأذرع الرقمية التي تستخدمها إيران لصد هجماتٍ سيبرانية، التي تقف عائقاً أمام البرنامج النووي الإيراني وتطويره، أوفي المجالات الاستخبارية وجمع المعلومات، حيث رأت إيران في هذا المجال ميداناً جديداً ونشطاً لتنمية قدراتها العسكرية. [17]

في ضوء التطور التكنولوجي المتسارع وتنامي دور الفاعلين من النشطاء والجيوش السيبرانية والفواعل من دون الدول في المجال السيبراني، زادت التهديدات السيبرانية. [20]

وإلى حد الأن لا زال عدم الاتفاق حول الإستراتيجية الدفاعية الفعالة التي يجب تنفيذها لمواجهة هذه الحرب السيبرانية، ونظراً لكونها نوعاً من الحروب الخاطفة سيتطلب معرفة متقدمة بالبرامج الضارة التي يتم تطويرها في أنظمة يحتمل أن تكون معادية إضافة إلى الاستجابة التلقائية وإجراء رد فعل وقائي لنزع سلاح الهجوم، ولكي يكون الدفاع النشط فعالاً يجب تفويض السلطة بإجراء العمليات المناسبة.[21]

تتضمن منظومة القدرات السيبرانية الإيرانية قدرات بشرية مدربة في مجالات تقنية المعلومات، والاختراق السيبراني ، وفق تنظيم إداري يصل إلى المستويات العليا من الدولة للتنظيم والإشراف على الجهات المعنيّة بالحرب السيبرانية على النحو الآتي:[17]

أ–المجلس الأعلى للسايبر: تم تشكيله بأمر من المرشد الإيراني علي خامنئي عام 2012م، ويضم في عضويته المسؤولين في الجهات الحكومية الرئيسة برئاسة رئيس الجمهورية، ويتولى المجلس الإشراف على جميع الجهات التي لها علاقة بالسايبر ويُحدد السياسات ومجالات العمل.

ب–قيادة دفاع السايبر: مُهمّتها دفاعية تهدف لحماية المنشآت الوطنيّة ضدّ أي هجوم سيبراني.

ج–الجيش السيبراني الإيراني: يهتم بالجانب الهجومي من السايبر، ويتبع لقيادة الحرس الثوري (القوات السيبرانية)، ويضم خبرات عالية في مجال تقنية المعلومات، والهاكرز المحترفين ويسانده عدد من الوحدات الفنية.

وأخذت عقيدة الأمن السيبراني تفرض نفسها في إطار استراتيجية الأمن القومي الإيراني بشكل عام، وإن هذه العقيدة تستند على ركيزتين مهمتين:[19]

- الركيزة الأولى: تتمثل بحماية الأمن القومي الإيراني من خلال بناء بنية تحتية علمية تكنولوجية تستند على استراتيجية وقائية في الدفاع واستراتيجية استباقية في الهجوم في المجال السيبراني .
- الركيزة الثانية: تتمثل بتطوير العديد من المفاهيم والتقاليد القتالية السيبرانية عن طريق شبكة معقدة من الجيوش السيبرانية القادرة على شن هجمات سيبرانية متعددة على اهداف محددة في آن واحد.

وفي عام 2019 كشفت المحكمة الموثقة أن مكتب التحقيقات الفدرالي الأمريكي تعقب فاعلين إيرانيين سيبرانيين انتهكوا شركات تكنولوجيا الأقمار الصناعية الامريكية.[19]

أصبحت إيران ذات هجمات سيبرانية فعالة خاصة بعد الهجوم السيبراني عليها من قبل الولايات المتحدة الامريكية والكيان الإسرائيلي، حيث تحسنت تلك القدرات السيبرانية بشكل مطرد ،واعتبرت إيران قوة سيبرانية من الدرجة الثالثة كونها قادرة على شن هجمات أكثر تعقيداً وتدميراً خاصة ضد الولايات المتحدة الامريكية، وفي الإستراتيجية الايرانية تعمل القدرات السيبرانية كركيزة فعالة خاصة بما تسمى (عقدة الردع) ، و تهدف القدرات السيبرانية الإيرانية إلى معاقبة السلوك غير المرغوب فيه للخصوم ،وردع الجهات التي تنوي القيام بتلك الهجمات. [19]

في عام 2012م مسح فيروس (شمعون) ثلاثة أرباع البيانات الموجودة على أجهزة الحاسب لشركة أرامكو السعودية، واستبدل البيانات بصورة علم الولايات المتحدة الامريكية، وإن هذا الهجوم موجه للولايات المتحدة الامريكية.[19]

وفي عام 2020 م أعلنت شركة مايكروسوفت، أن مجموعة من القراصنة المرتبطين بإيران شنوا هجمات سيبرانية ، استهدفت حسابات صحافيين أميركيين وشخصيات حكومية رسمية وحسابات مرتبطة بالحملة للانتخابات الرئاسية بهدف التأثير عليها.[22]

وتضمنت جهود إيران الرامية لحشد القدرات الوطنية الإيرانية في مجال السايبر، واستغلالها لخدمة أهداف إيران، والتضليل بشأن مصادر الهجمات وإخلاء مسؤولية إيران عنها، وترك المجال مفتوح ، أمام قراصنة المعلومات الإيرانيين، وغض الطرف عن مزاولتهم القرصنة السيبرانية بصورة انفرادية، أو ضمن مجموعات القرصنة التي عملت وراء أسماء مستعارة، أو تحت أسماء شركات مختصة ، الأمر الذي أسهم في عدم وجود دلائل أكيدة لدى مراكز الدراسات الغربية حول طبيعة الهجمات وجعل الإدارة الحكومية في إيران بمنأى عن اتهامات المباشرة بالإعداد أو تنفيذ هجمات سيبرانية على مواقع للدول المناهضة لسياساتها .[17]

وعلى صعيد آخر، وفي حزيران من العام 2021، وبعد قيام إيران بإسقاط طائرة استطلاع أميركية قرب مضيق هرمز، أفادت وسائل إعلام أميركية، أن الولايات المتحدة الأمريكية شنت هجمات سيبرانية استهدفت أنظمة حاسوبية إيرانية تستخدم لإطلاق الصواريخ. وجاء بعدها إعلان إيران عن التصدي لهجمتين سيبرانيتين خلال أسبوع واحد، كانتا قد استهدفتا منظومة الاتصالات الدفاعية. [22]

ورغم تعرض ايران للهجمات السيبرانية استطاعت ايران أن تصد تلك الهجمات والكشف عنها وعدم التأثير على مجريات الاحداث بشكل عام،واشتد التصعيد الأمريكي الإسرائيلي وبعض الدول الأوروبية منها لكن استطاعتْ ايران أن تقوض تلك الاحداث خدمة لمصالحها العليا وسترد على اي هجمات ضدها سواءً كانت سيبرانية أو تقليدية برد سيبراني أو تقليدي ضمن ما تراه مناسباً .[19].

نستنتج من كل ما تقدم أن الحرب السيبرانية هي احدى أدوات الجيل الخامس من الحروب، التي ميدان صراعها وعملها هو الفضاء السيبراني، إذ تستخدم عبر هذا الفضاء الأسلحة السيبرانية من برمجيات وفيروسات ذات قدرة تدميرية ضد الجهة المستهدفة ، لذلك سعت الدول ذات القدرات السيبراينة إلى تفعيل ذلك وخاصة الولايات المتحدة الامريكية وايران، حيث إن الولايات المتحدة الامريكية استخدمت الفضاء السيبراني في شن هجمات ضد ايران، واستمرت بتلك الهجمات عبر استراتيجية سيبرانية خاصة لها عبر الإدارات الامريكية المتعاقبة، وحتى وقتنا الحاضر ساعية من ذلك لتدمير وإنهاك وابطاء القدرات الحيوية لإيران والبنى التحتية خاصة في اطار قدراتها النووية متمثلاً بالبرنامج النووي الإيراني وصولاً لما مخطط له ضمن استراتيجيتها الخارجية، مع رد إيراني استراتيجي سيبراني ضد الولايات المتحدة الامريكية واستمر حتى وقتنا الحاضر ،عبر استراتيجية سيبرانية خاصة هدفها الحاق أكبر ضرر داخل المواقع الحيوية والبنى التحتية للولايات المتحدة الامريكية لإثبات أن ايران لها القدرة السيبرانية على الرد والهجوم الاستباقي أيضاً.

الاستنتاجات و التوصيات :

من خلال هذه الدراسة تم التوصل إلى عدد من النتائج وهي:

1-أصبح الفضاء السيبراني ساحة جديدة للصراع الدولي بمختلف أشكاله.

2-تعدد الفواعل التي تستخدم وتمارس الهجمات السيبرانية (الدول، الأفراد، شركات دولية، جماعات مسلحة)

3-لا يمكن تجاهل مكانة الأمن السيبراني وارتباطاته في حماية أبعاد الأمن القومي للدول سواءً العسكرية أو الثقافية أو الاقتصادية، حيث يعتبر الأمن السيبراني شريك قوي في حماية مقومات الدولة.

4-تسعى إيران إلى توسيع نطاق سيادتها السيبرانية وتخصص من أجل ذلك موارد هائلة خاصة في ميدان الصناعة التكنولوجية والذكاء الاصطناعي وتتعدد دوافعها لامتلاك القوة السيبرانية من دوافع سياسية، اقتصادية، عسكرية.

5-تمثل الحروب السيبرانية مدخلاً جديداً على نطاق الصراع الذي يمتد عبر أشكال سياسية واقتصادية واجتماعية وقانونية.

6-إن هناك سباقاً للتسلح السيبراني والالكتروني بين الدول وذلك لرغبة الدول المتزايدة في تعزيز دفاعاتها ضد خطر التعرض للهجمات السيبرانية.

التوصيات:

بناء على نتائج البحث يوصي الباحث بالتوصيات التالية:

1. ضرورة إنشاء تشكيلات ووحدات خاصة بالأمن السيبراني داخل الإطار الحكومي تكون مهمتها تطوير الأمن السيبراني ورسم سياسة الدفاع والهجوم السيبراني وحماية المعلومات والاهتمام بتقنيات الذكاء الاصطناعي.
2. يجب على الدول أن تتبنى وضع إستراتيجيات سواءً كانت قريبة أو متوسطة أو بعيدة المدى وذلك لحماية البنية التحتية الإلكترونية والمرافق الحيوية.
3. انشاء مراكز تدريب خاصة بمكافحة الهجمات السيبرانية والاهتمام بتقنيات الذكاء الاصطناعي.
4. انشاء شراكات بين القطاع العام والخاص والشركات المتخصصة بالأمن السيبراني على المستوى الوطني والدولي لمكافحة الهجمات السيبرانية.

References:

1- Al-Issa, Talal; Jujube, Uday. International responsibility arising from cyber attacks in light of international law, Zarqa Journal for Research and Human Studies. Jordan, Vol. 19, No. 1, 2019, 82-95.
2- Farhat, Aladdin. Cyberspace Shaping the Battlefield of the Twenty-First Century, Journal of Legal and Political Science. Algeria, Vol. 10, No. 3, 2019, 88-107.
3- Al-Aboudi, Ali. Obsessed with cyber warfare on international peace and security, Journal of Political Issues. University of Baghdad, Volume 23, Issue 17, 2019, 89-118.
4- Mansour, Shadi. Fifth Generation Wars, first edition, Al-Araby for Publishing and Distribution, Cairo, 2019, 241.
5- Hussein, Hayat. Cyberspace and global security challenges, Journal of Legal and Political Sciences. Blida University, Algeria, Vol. 12, No. 1, 2021, pp. 1066-1089.
6- Farhat, Aladdin; Amrous, building. Cyberspace and the Erosion of the Concept of National Sovereignty, Algerian Journal of Political Studies. Algeria, Vol. 8, No. 1, 2021, pp. 162-183.
7- Zaruka, Ismail. Cyberspace and the shift in the concepts of power and conflict, Journal of Legal and Political Sciences. Algeria, Vol. 10, No. 1, 2018, 1016-1031.
8- Talah, Lamia. Cyber Threats and Crimes, Maalem Journal for Legal and Political Studies. Algeria, Vol. 4, No. 2, 2020, 56-69.
9- Belhaj, Selim. Asymmetric security threats and their repercussions on Algerian national security. PhD thesis in political science, University of Batna 1, Algeria. 2021.
10- Dahmani, Salim. The impact of cyber threats on the national security of America as a model. Master's Thesis in International Relations, Faculty of Law and Political Science, University of Mohamed Boudiaf M'sila, Algeria, 2018.
11- Attia, Idris. The status of cybersecurity in the Algerian security system, Algerian Journal of Human Security. Algeria, Vol. 7, No. 1, 2021, 100-121.
12- Abdel-Gawad, Amira. Cyber risks and ways to confront them in public international law, Journal of Sharia and Law. Al-Azhar University, Part III, Issue 35, 2020, 363-541.

13- Ahmed, Shuhairat; Murad, Qurebeez. Internet Challenges for State Sovereignty Digital Sovereignty, Journal of Legal and Economic Research. University of Laghouat, Algeria, Vol. 5, No. 1, 2022, pp. 302-322.
14- Abu Saud, Hani Matar; Tahir, Mayasa. Links of information security to national security, Journal of Human Rights Studies. Algeria, Vol. 7, No. 2, 2020, pp. 204-221.
15- Farhat, Aladdin. From Nuclear Deterrence to Cyber Deterrence: A Study of the Extent to Realize the Principle of Deterrence in Cyberspace, The Thinker Magazine. Algeria, Vol. 16, No. 1, 2021, 263-285.
16- Bayram, Fatima. National Sovereignty in the Shadow of Cyberspace and Digital Transformations: China as a Model, Algerian Journal of Human Security. University of Constantine 3, Algeria, Vol. 5, No. 1, 2019, pp. 789-816.
17- Al-Maimouni, Ahmed bin Ali. The Active Front: Implications of the Cyber Confrontation between Iran and Israel, Journal of Iranian Studies. International Institute for Iranian Studies, Issue 12, Fourth Year, 2020, 67-86.
18- Hakim, Gharib; Sabrina, Sharqi. The repercussions of electronic warfare on international relations, Journal of Policy and Law Notebooks. Algeria, Vol. 12, No. 2020, 2, 92-107.
19- Faraj, Karrar Abbas. Cyber war A study of the strategy of cyber attacks between the United States of America and Iran, Hammurabi Journal of Studies. Issue 40, Year 2021, 10, 195-223.
20- Khalifa, Ihab. Post-information society, the impact of the fourth industrial revolution on national security, first edition, Al-Araby for Publishing and Distribution, Cairo, 2019, 180.
21- Shanouf, Zainab. Cyber warfare in the digital age, post-Clwervitch wars, Algerian Journal of Security and Development. Algeria, Vol. 9, No. 2, 2020, pp. 89-103.
-22Abdel Wahed, Salah Haider. Cyberspace wars, a study in their concept, characteristics, and ways to confront them. Master's thesis in political science, College of Arts and Sciences, Middle East University, Jordan. 2021.