رقم الترميز الدولي / ISSN (P): 2710-2653
ISSN (E): 2960-253X /
رقم الايداع الوطني / 2375 / 2019

تاريخ استلام البحث 20 / 9 / 2023
تاريخ قبول البحث 29/ 10/ 2023
تاريخ النشر 1 / 12 / 2023

الدور الدولي في تعزيز الامن السيبراني في ضوء التحديات المعاصرة

Dimensions of the Turkish water policy towards Iraq

أ. م. د. انعام عبد الرضا سلطان العگابي

Asst.Prof. Dr. Anaam abdalruda sultan aligabi

جامعة بغداد/ كلية الاعلام

University of Baghdad/College of Information

anamalkaby43@gmail.com

IRAQI Academic Scientific Journals

https://www.iasj.net/iasj/journal/393/issues

الملخص

الامن السيبراني هو الموضوع الذي يهم العالم في الوقت الراهن لأن الثورة التكنولوجية التي اجتاحت الدول والفواعل من غير الدول ادت الى ظهور تحدي كبير يواجه الدولة وافراد المجتمع , ولهذا فأن زيادة التهديدات الالكترونية التي منها السرقة والنصب والاحتلال والابتزاز الالكتروني والذي يفُترض على الدولة ان تعزز انظمتها التقنية على كافة الاصعدة ومكوناتها من اجهزة وبرمجيات وتأمين المعلومات الحساسة البالغة الأهمية للدول والمجتمعات على حداً سواء المعرضة للخطر والاختراق والاستيلاء كي تحافظ على الامن الوطني وحفظ وحماية السرية والخصوصية للبيانات والوثائق الرسمية للدول والبيانات والمعلومات الشخصية لأفراد الدولة.

الكلمات المفتاحية:"الامن السيبراني"،"التهديدات"،"الفضاء الالكتروني"،"تكنولوجيا المعلومات والاتصالات"، "الامن الوطني"

Abstract

The international role in enhancing cyber security in light of contemporary challenges

Cyber security is the topic that concerns the world at the present time because the technological revolution that swept through countries and non-state actors led to the emergence of a major challenge facing the state and members of society, and for this reason, the increase in electronic threats, including theft, fraud, occupation and electronic extortion, which the state is supposed to strengthen its technical systems At all levels and their components, including hardware and software, and securing sensitive information that is of great importance to countries and societies alike, which are exposed to danger, penetration, and seizure in order to maintain national security, preserve and protect confidentiality and privacy of data and official documents of countries, and personal data and information of state personnel.

Keywords: "cyber security" ،"threats،" cyber space"،" information and communication technology"،" national security"

المقدمة

ظهر الفضاء السيبراني كبيئة تفاعلية رقمية تضمنت مقومات مادية وغير مادية فضلا عن مجموعة من الادوات الرقمية وانظمة شبكات وبرامج لحفظ المعلومات وقدرتها على اعادة بلورة قواعد القوة الدولية والمقدرات الدولية للقوى الفاعلة في المجتمع الدولي، وما يعنيه ذلك من تهديدات على الامن القومي للدول، فتمثل الهدف الرئيس للامن السيبراني في تعزيز قدرات الدول وفي مقاومة التهديدات الكامنة من تداعيات الفضاء السيبراني حيث اصبح الامن السيبراني جزء من الامن القومي للدول ، الامر الذي دفع اغلب دول العالم وضعه في سلم اولوياتها ، عبر ظهور الحروب الالكترونية التي واجهتها عدد كبير من الدول من خلال انتشار القوة السيبرانية بين الفاعلين المؤثرين في الساحة الدولية وقدرتها على السيطرة والهيمنة في الفضاء السيبراني.

اهمية الدراسة: تكمن الاهمية العلمية للدراسة في معرفة الدولة لمدى خطورة ما يجوب في الفضاء الالكتروني من حروب وجرائم الكترونية وهجمات سيبرانية وكيفية مجابهتها وتحصين فضاءها الالكتروني وتحقيق الامن السيبراني ومعرفة مدى خطورتها على الامن المعلوماتي للدول من اجل اتخاذ اجراءات لحماية الامن المعلوماتي للدولة ضمن أطار سياسات عامة وفق منظومة امنها الوطنيي.

اشكالية الدراسة: اصبحت قضية أن الفضاء الالكتروني السيبراني الافتراضي من عمليات القرصنة والهجمات الالكترونية والتي بدورها تؤثر على أمن الدول والمجتمعات تلقي اهتماماً متصاعداً على أجندة الامن الدولي وذلك في محاولة لمواجهة تصاعد التهديدات الالكترونية ودورها في التأثير على الطابع السلمي للفضاء الالكتروني . من خلال ما سبق تتضح لنا الاشكالية الرئيسة للبحث وهي: ما هي أهم المخاطر والتهديدات التي يتعرض لها الامن المعلوماتي للدول ومجتمعاتها من اجل تجسيد الامن السيبراني وماهي الاستراتيجيات الدولية والاليات التي يجب تفعيلها من قبل الدول للحد من المساس بامن الدولة وافرادها.واندرجت عدة أسئلة فرعية تتمثل اساساً في: ماهي السيبرانية؟ ماهو مفهوم الامن السيبراني والمفاهيم المرتبطة بالامن السيبراني؟ وما هي التهديدات اللاتناظرية التي تتعرض لها السيادة الوطنية للدول؟ ماهي اهداف وابعاد وخصائص الامن السيبراني ؟ ومن هم فواعل الامن السيبراني؟ الوطنية والامن الوطني السيبراني العراقي والمخاطر التي يتعرض لها في فضاءه الالكتروني؟

فرضية الدراسة: كلما زاد التطور التكنلوجي كلما ادى الى زيادة مخاطر تعرض أمن الدول ومجتمعاتها الى الهجمات والتهديدات والجرائم السيبرانية في ميدان الفضاء الالكتروني , أي ان هناك علاقة طردية بين زيادة التطور التكنولوجي وزيادة مواجهة الدول لتحديات الامن السيبراني وتآكل السيادة الوطنية والقومية لمقومات الدولة وامن المعلومات

هيكلية الدراسة: تتضمن الدراسة البحث في المحاور التالية:

المحور الاول: الفضاء السيبراني وتطور مفهوم الامن السيبراني

اضحى التقدم في الثورة التكنولوجية للاتصال والمعلومات وبالاخص في شبكات الحواسيب , ان يكون هناك تغيير في تفسير مصطلح القوة والامن مما نتج ان يدخل المجتمع الدولي في مرحلة التصادم والتنافس في داخل منظومة الفضاء الالكتروني والذي ادى الى ان يستحوذ مفهوم القوة الاهتمام الكبير من قبل القوى العظمى او السيطرة على عناصرها الاساسية.

أولاً: مفهوم السيبرانية والامن السيبراني والمفاهيم ذات العلاقة:

1. مفهوم السيبرانية: في ظل التسابق الالكتروني الذي نعايشه اليوم نرى ان هناك العديد من المفاهيم الجديدة بدأت بالظهور على الساحة الالكترونية ولربما كان وجودها منذ مدة الا انها حديثاً بدأت بالانتشار والتي من ابرزها مصطلح السيبرانية الذي ارتبط بالحروب السيبرانية أو الالكترونية. اشتق اصل كلمة او تعريف سيبرانية من اللغة الانكليزية من الكلمة cyber والتي تعني شبكات الاتصال والانترنت وشبكات المعلومات والانظمة الرقمية المختلفة . ويندرج تحتها ما نسميه الفضاء السيبراني أو الالكتروني اي الفضاء الذي يضم كل ما يخص الشبكات والانترنت عموماً. واشتق من تعريف السيبرانية لاحقاً مصطلح الهجوم السيبراني وهو ما نقصد به الهجمات الالكترونية والرقمية التي تتم من خلال الانترنت على مواقع الانترنت المختلفة والحواسيب والاجهزة الرقمية وشبكات الاتصال المتنوعة(1).
2. مفهوم الأمن السيبراني : هو مجموعة من الآليات والإجراءات والوسائل والأطر التي تهدف إلى حماية البرمجيات وأجهزة الكمبيوتر من مختلف الهجمات الإختراقات (التهديدات السيبرانية) التي قد تهدد الأمن القومي للدول ، ولغرض الوصول الى تعريف اكثر دقة ووضوح ، نجد المعهد الوطني للمعايير والتقنية الأمريكي، " عرف الفضاء الالكتروني : هو شبكة متداخلة من التصنيفات التكنولوجية والفنية ، من ضمنها شبكة المعلومات الدولية ونظام الاتصالات السلكية واللاسلكية ونظم المعلومات في الحواسيب ووسائل التحكم واقراص الدمج للمعالجات الالكترونية(2) ، ويمكن ان يكون الأمن السيبراني كوسيلة عسكرية استراتيجية تستخدمها الدول والمواطنين بالشكل الذي لا يمكن اغفاله ان الحرب الافتراضية أصبحت جزء من الاستراتيجيات المعاصرة للدول وفي الصراعات المسلحة فيما بينها(3). وفي العصر الراهن لثورة تكنولوجيا المعلومات وامنها اضحى لها الوظيفة الكبرى في صد وردع إي عمل هجومي سيبراني على الدولة يهاجم انظمتها المختلفة، وكذلك حماية وسائل النظام التشغيلي ضد اي عمل استباقي بهدف الدخول والاختراق لتنفيذ اعمال غير مشروعة او غير صائبة(4). ولحماية مؤسسات الدولة جميعها من مخاطر الإختراق من قبل الدول والأفراد، ولتتم الاستفادة من الخبرات الوطنية في السيبرانية وتطوير هذه الخبرات إلى مهارات عالية الجودة للحفاظ على أمن الدولة ومواكبة التطور التكنلوجي في العالم (5).

3. الفرق بين الفضاء السيبراني والامن السيبراني: يتكون الفضاء السيبراني من انظمة واجهزة الكترونية متنوعة مندمجة بالشبكة ونظام شبكات سلكية ولاسلكية . وعدت المعلومات المتوافرة في الفضاء الخارجي واحدة من اهم مميزات وخصائص المجتمع المعاصر، وهو ما يؤدي الى تقوية امكانية وقدرة الاتصال السريع، والتحكم في قيادة مجموعة من الانظمة الموزعة ، وخزن ونقل المعلومات باعداد كبيرة (6).
4. الفرق بين أمن المعلومات والأمن السيبراني (7):-

أ. أمن المعلومات (Information Security) :يهتم بالسرية والتكاملية وتوفير البيانات
ب. الكتمان والسرية : تعني عدم معرفة أي شخص غير مسؤول او ليس لديه تخويل من الوصول لبيانات مستخدم آخر .
ج. الأئتمان وحفظ البيانات: ويعني الائتمان التكامليّة والمحافظة على البيانات من التحريف او النسخ من قبل الأشخاص غير المصرح لهم بالوصول لهذه البيانات بصورة عمدية او غير عمدية وتعديل البيانات والذي يعُد اختراقاً للائتمان وعدم القدرة في الحفاظ على المعلومات بشكل تام .
د. تتم بسرية وضرورة توافرها بصيغة مستمرة مدونة أو بصيغة الكترونية.

أذاً أمن المعلومات يضمن حماية البيانات المادية والرقمية ويختلف الامن الموظف للمعلومات عن الأمن الالكتروني والذي يسعى الى حفظ البيانات بشكل آمن أياً كان نوعها، بينما يحافظ الأمن الالكتروني على البيانات الالكترونية او الرقمية . وفي حال نريد أن نبدأ بتطوير برنامج أمان؛ فأن حفظ المعلومات وتأمينها هي اولى الخطوات ، حيث يعُد المعيار الرئيس لتأمين البيانات. وهو ايضاً يعمل على ضمان وتأمين الانظمة والبرامجيات الشبكية من الاختراق الالكتروني (8).

5-الفرق بين الأمن السيبراني وأمن الشبكات: أمن الشبكات هو فرع من فروع الأمن السيبراني؛ يحمي البيانات التي تُنقل من خلال اجهزة الشبكات لتأمين حفظ المعلومات من التغيير او الاختراق. ويتضمن وظيفة أمن الشبكة في توفير الحماية والامان للبنى التحتية والوسائل الفنية للمعلومات الحكومية والمؤسسية من الهجوم السيبراني بكل انواعه. اضافة أن اعضاء أمن الشبكات يتحمل مسؤولية حماية البرامج والآليات اللازمة لتأمين بنية شبكة الاتصالات المحلية. وباستخدام وسيلة تأمين ملائمة قادرة على إكتشاف مصادر التهديد التي تسبق عملية التسلل إلى الشبكة المحلية وتهديد بيانات الهيئات والشركات. لذا يمكن القول، يستوجب توفير الأمن للدولة والمؤسسات والهيئات توفير اسس التعاون الجماعي لأنجاز الاليات الفنية والتقنية للأمن وهي : أمن المعلومات والأمن الالكتروني او السيبراني وأمن الشبكات، فقد تحقق سوية اساس امني محترف ومتكامل (9).

ثانياً: خصائص الامن السيبراني:

وتُعد حروب الفضاء الخارجي واحدة من وسائل وآليات الجيل الخامس من النزاعات ، فلم تنفرد اهداف المجاميع الخاصة للقوات الامريكية في ردع اي هجوم او اعتداء من قبل الخصم في القوات السيبرانية المعادية لكن أيضاً دخلت مواقع التواصل وتطبيقات الانترنت للتنظيم الارهابي (داعش) الامر الذي ساعد على ابقاء السرية للقنوات الخاصة بهم والهادفة الى احتمالية تجنيد مزيد من الاصوليين الارهابيين . (10).

خصائص الامن السيبراني العامة: من المبادئ الشائعة والتي تُعد من اجل ان يكون البرنامج الاكثر ضرراً في تكوين اسلحة الفضاء الخارجي (11):-

1. يجب ان يكون تحت رعاية حكومية أو هيئة ناشطة غير حكومية يتم تطويعه لها.
2. ان تكون الفائدة من هذا السلاح من اجل عمل تجسسي وتوظيف قوة فاعلة في تشكيل وصياغة مشاهد تبرر فعلهم العدواني.
3. هناك قوى ترعى بناء وتشكيل السلاح السيبراني والذي يتميز عن البرامج التي تتسم بالضرر، وأن يعمل السلاح السيبراني ضد أهداف معينة حيث انه لا يستخدمه قراصنة، بل يتم استخدامه من قبل حكومات وقوى غير حكومية مثل التنظيمات الإرهابية والكيانات الفاعلة التي يتم اشراكها .
4. مراقبة النظام ومراقبة مشغليه، والمعلومات الحساسة، مثل كلمات المرور، والمفاتيح الخاصة للبرامج وسرقة البيانات والملكية الفكرية فعملية الاتلاف الالكتروني لواحداً أو أكثر يكون مما يلي(12):

أ-البيانات الموجودة في أنظمة البنى التحتية

ب-اتلاف أجهزة الكومبيوتر أو تدميرها بالكامل

5. الاستهداف: ويكون استهدافها اختياري ، قبل البدء بأي هجوم، يتم اختيار الأهداف أولاً وبالطرق المختلفة، لكن ما يستخدمه القراصنة والمحتالون لسرقة المعلومات الشخصية أو المالية، تبين إنها عشوائية، وتوزيعها واسع.
6. التميّز عن الفيروسات والبرامج الضارة الأخرى: يتميز السلاح السيبراني عن الفايروسات، ليست كل الفيروسات أسلحة سيبرانية، كما ان ليست جميع الأسلحة السيبرانية فيروسات، فالأسلحة السيبرانية المهددة للامن السيبراني هي برامج تم تصميمها للقيام بوظائف مختلفة وتشمل(13):

أ-فايروسات الحاسوب : من وظائفها ازالة البرنامج أو تعديل عيبها أو نسخها أو غير ذلك والغرض هو إلحاق الضرر بحواسيب الخصم، وفي بعض الأحيان قد تستخدم إلى تعطيل شبكة الاتصال لدولة ما ، بعد تطور الفضاء السيبراني صنعت من اجل تخريب بيانات الخصم وسرقتها او قطع شبكته، تتصف بالانتشار وصعوبة التخلص منها، لقدرتها الكبيرة على عمل التلوث والنسخ والاحتيال وبالاخص عندما يتم

استخدامها في الهجوم على المعلومات التي تركز على شبكات الاتصالات والتي تستهدف الاموال، مثل المصارف واشهر الديدان الستاكس نت التي استخدمت لتعطيل أثنين من المفاعل النووية الإيرانية [14].

ب- حصان طروادة :هي شيفرة وكذلك برنامج صغير متخفي داخل برنامج واسع ويُعد من البرامج المشهورة عالمياً، حيث يعمل على بعض الوظائف غير الظاهرة ، مثلاً يقوم بزرع فايروسات وديدان ، ولا يمكن معرفة مكان وجوده لأنه تم برمجته بدقة كبيرة ، ويخفي آثاره التي لا تتصف بأعمال تدميرية ، ويقوم بتقليل القوة الدفاعية لدى الشخص الذي تم اختراقه من اجل انتهاك خصوصية معلوماته وبياناته المثبتة في جهازه فيقوم على سبيل المثال بأرسال بيانات عن نقاط الضعف المتواجدة داخل النظام (15)

ثالثاً: ابعاد الامن السيبراني: لا بد لنا من استعراض الابعاد كما يلي(16):-

1-الابعاد العسكرية: فمن المعروف ان بدايات شبكة المعلومات الدولية قد تم تطويرها في المؤسسات العسكرية بصورة اساسية لتدخل أيضاً بعدها المؤسسة البحثية بما تقدمه من ابحاث تكون موظفة لخدمة المجال العسكري ودراسات علمية التي تميز دولة عن غيرها. ان اختراقات انظمة المنشآت النووية وخطر حروب الفضاء الخارجي المؤثرة في البنى الهيكلية التي تشمل المؤسسة الدفاعية وامدادات خدمات الكهرباء ومعظم المؤسسات الخدمية في البنى التحتية .

2-الابعاد الاجتماعية: ان معظم تطبيقات شبكة المعلومات الدولية كالمدونات ومواقع التواصل الاجتماعي منحت الفرصة لاغلب المستخدمين بأن يعبروا عن آرائهم السياسية ومتطلباتهم الاجتماعية , بالاضافة الى السمات التي يتمتع بها الانترنت من امكانات تكنولوجية هائلة في جميع الحقول الخدمية والمعلوماتية والتي تصل الى جميع بقاع الارض ولأغلب الشرائح ، والذي يمكن ان يعمل على تبادل المعلومات في اوقات الازمات الانسانية والكوارث بل تتعدى الى المحافظة على الايدولوجية المجتمعية ،وكان حرص المؤسسات والتنظيمات الدولية على بث صورة تثقيفية وتوعوية للامن في الفضاء السيبراني وضمان تفعيله وحث المجتمع الدولي على اهمية تحقيق (17).

3-الابعاد السياسية: وتشمل بصورة مرتكزة وهو ان الحكومات لها احقية في حماية وضمان ديمومة بقاءها في السلطة, ولا يمكن ان نغفل عن دور تقنيات الاتصال والمعلومات في تشكيل فواعل محلية ضمن المجتمع ، فقد تحول المواطن الى فاعل ولاعب اساس قادر على ان يؤثر في تغيير وتعديل القرارات ومساعدة صانع القرار في صياغة القرارات السياسية من خلال قدرته في الحصول والوصول الى المعلومات المتوافرة من كل مصادرها المعلومة وغير المعلومة(18).

4- الابعاد الاقتصادية: هناك علاقة وثيقة بين اقتصاد المعارف التي ترتبط به وبين تكنلوجيا الاتصال والمعلومات من خلال ما تقدمه من احصائيات وبيانات محفوظة يتم استخدامها وتداولها بين جميع

الفئات الرسمية وغير الرسمية. لقد ساعدت تقنية المعلومات وتكنولوجيا الاتصال في تحقيق التنمية والتقدم الاقتصادي لعدد كبير من بلدان العالم (19).

5- الابعاد القانونية: يؤدي الدور الشخصي والنشاطات والهيئات الحكومية دوراً جداً فاعل في الفضاء الخارجي الالكتروني ويعطي حلولاً ونتائج تساعد في نزع فتيل الازمات والحروب التي تشكلت بسببها , لهذه الاسباب تستدعي الحاجة الى وضع دراسة متوازنة بين التغييرات التي اصابت المجتمع الدولي وبين تعزيز حقوق الانسان وحريته الشخصية التي دونت في القانون الدولي ومنظمات مراقبي حقوق الانسان وحقوق اخرى تم اضافتها كحق الوصول الى الانترنت والحق في انشاء مدونات الكترونية ، وضمان الملكية للمعلومات , وتوأمة القوانين مع الاقتصاد كحق الاحتفاظ بالبيانات الابلاغ عن جرائم الاختراق والابتزاز الالكترونية وجرائم تخص المحتوى ذات اثار اقتصادية سلبية لذا يجب الحفاظ على سرية البيانات والمعلومات للافراد وخصوصيتها(20).

المحور الثاني: الدور الدولي في تعزيز الامن السيبراني

بعد بيإنّ الخطوط العامة لطرق الدفاع الالكتروني نوضح في ما يلي الاستراتيجيأت التي تتبناها القوى السيبرإنّية الكبرى "Cyber Superpowers". والأكثر اعتماداً واهتماماً بالفضاء السيبرإنّي، وذلك لحماية مؤسساتها وإنّظمتها الإلكترونية وشعوبها مما قد تتعرض له من هجمات سيبرإنّية، ولقد تم اختيار نماذج من اجل استعراض استراتيجيأت الأمن السيبرإنّي وذلك لانها الأكثر اعتمادا على الفضاء السيبرإنّي والأكثر عرضة للهجمات السيبرإنّية ، والأكثر وضوحاً في الإعلإنّ عن استراتيجيأت الأمن السيبرإنّي الخاص بها(21) ,لإنّها تضفي قدراً كبيراً من السرية على إنّشطتها السيبرإنّية بشكل يعيق إلى رؤية واضحة لاستراتيجيتها السيبرإنّية في مواجهة تحديات الامن السيبراني

أولاً: الاستراتيجيات الدولية في تعزيز الامن السيبراني:

تُعد الحكومة الامريكية من مصافي الدول التي تعاملت مع موضوعة امن الفضاء السيبراني وجعلتها ضمن اولوياتها الاستراتيجية من اجل درء المخاطر التي يتعرض لها اقتصادها القومي وعلى تقنية الاتصالات والمعلومات مما فرض على الحكومة الامريكية ان تعمل على تحسين وزيادة قوة الدفاع السيبراني وزيادة الاهتمام بتوفير ضمان وتأمين كافة هياكل البنى التحتية المهمة بأتباع نهج اساس واستراتيجية شاملة عرُفت ب" الاستراتيجية الوطنية لحماية الفضاء السيبرإنّي" فتم وضع تقسيم شامل من اجل توفير الحماية لأمن الفضاء السيبرإنّي بين وكالات الامن الامريكية وولاياتها ألاتحادية، وتولت المسؤولية وزارة الأمن الداخلي باعتبارها الهيئة التي تنسق العمل مع الوكالات الاخرى, ونسبةٍ لمضمون الاستراتيجية عملت وزارة البنتاغون مع هيئة تنفيذ القانون ووكالات إنّفاذ القانون بتشكيل إنّظمة تكشف عن المخاطر والتهديدات السيبرانية من اجل تحقيق الردع والوقاية الاستباقية في الوقت

المطلوب، بينما تقوم وزارة الخارجية بتأطير قضايا التعاون في اغلب موضوعات الأمن السيبرانّي في المجتمع الدولي (22)،لذلك تم تشكيل نظام يستعرض فيه استراتيجية الفضاء السيبراني الامريكي ليس الهدف منه تحليل انظمته ولكن تشكيل خطة تعمل على توفير سياسة دفاع وردع الكتروني مناسبة للقدرات العسكرية الامريكية تتوائم مع مبادرة الامن السيبراني القومي والتي تم تقويمها وتعديلها باعتبارها من اهم المشاكل التي تواجه امن الفضاء الالكتروني ومن ثم القيام بتوزيع المهام والادارات بين اهم الاجهزة الامنية وبين الولايات الفيدرالية من اجل تطوير النظام الامني وتنسيقه مع سياسة واستراتيجية الامن السيبراني الحكومي الذي تم تسميته بالملك السيبراني(23) . لكن الاهتمام البارز والمركزي كان في في تأطير التعاون الدولي بشأن موضوعات الامن السيبراني ووضع استراتيجية دولية للفضاء السيبراني وتشكيل وظيفة منسق عالي المسؤولية على شبكة المعلومات الدولية في بناء القدرات برعاية وزارة الخارجية الامريكية من أجل تقديم المعونة للبلدان النامية وتوفير الامكانات والمقومات اللازمة بما فيها تصميم استراتيجيات متعددة لتعزيز الامن السيبراني الوطني(24). ان استراتيجية الامن السيبراني الجديدة اصبحت موضع مشهد مستقبلي لسياسة العقود القادمة والتي تعمل على تشكيل رؤية في انها سوف تكون بمثابة تهديد خارجي لمبادي حرية الانسان وتعزيز الديمقراطية ، وبناء وصناعة السلام باستخدام القوة ، وكذلك توفير الحماية لنظم المعلومات بما فيها المواقع التي تتسم بالسرية والحساسة تُعد من الاهداف الرئيسة في الاستراتيجية الجديدة ، فكلما تم تحديث هذه القطاعات كلما كانت عرضة لمواجهة المخاطر والتهديدات السيبرانية (25). وكذلك تمتلك روسيا قيادة إلكترونية مركزية كبيرة ومجهزة تجهيزاً جيدًا حتى اتهمت من قبل الحكومة الأمريكية بما فيها وزارة الخارجية ووزارة الدفاع والبيت الأبيض ،إن المتسللين الذين تسللوا على الحكومة الأمريكية ترعاهم الحكومة الروسية. إن روسيا لديها تجهيز ألكتروني جيد، في عام (2007)، قامت روسيا بشن هجمات الحرمان من الخدمة الموزعة على إستونيا مما ادى الى تحطيم البنية التحتية للتكنولوجيا الحيوية في إستونيا ، وفي عام (2009)، تم الإبلاغ عن قيام روسيا والصين بمحاولات لاختراق شبكة الطاقة الأمريكية ، باستخدام برامج لرسم خريطة للبنية التحتية للولايات المتحدة وإمكانية تعطيل النظام ، وتم اكتشاف عدة برامج ضارة على الشبكات الأوكرانّية في مايو (2014) فضلا عن ذلك هناك اختراق للانتخابات الأمريكية التي أتُهمت بها روسيا أيضاً(26) . وهناك الاستراتيجية الصينية التي اتبعتها بشأن تحصين امنها السيبراني والتي كانت فاعلة ولا تزال متقدمة للغاية في مجال السيبرانّية منذ فترة (27)، لا سيما فيما يتعلق بالتجسس الاقتصادي ضد الشركات الأمريكية على الرغم من إنّهم يستخدمون غالبًا أدوات الإنّترنت القوية (مثل الماسحات الضوئية للشبكات والفيروسات والروبوتات) للوصول إلى الأهداف. قد تتهم التدخلات المتعددة التي تقوم بها الصين إلى الشبكة الذكية بشكل أكبر إلى سرقة الملكية الفكرية وجمع المعلومات الاستخباراتية لتعزيز بنيتها التحتية(28).

أما بالنسبة للتحدي السيبراني الإيرانّي فتستخدم إيران برنامجها الإلكتروني كأداة ضد الأعداء السياسيين وجمع المعلومات الاستخباراتية ، وقد أثبتت إنّها ذات دوافع عالية ، على الرغم من إنّها أقل فاعلية إلى حد ما بالمقارنة مع روسيا والصين. ففي عام (2016) قامت الولايات المتحدة اتهام إيران بحادثة (2013)التي شملت عدة عمليات اقتحام عن بعد لجهاز تحكم لسد بومان في راي ،في نيويورك فرق أمن الكومبيوتر الخاصة العاملة نيابة عن الحرس الثوري الإسلامي في إيران وفي عامي (2012ـ2013) ضربت إيران الولايات المتحدة الأمريكية عبر الإنترنت بهجمات مؤثرة بشكل عام، وأخذت إيران تتواصل مع المنظمات الإلكترونية التي ترعاها الحكومة في جميع انحاء البلاد لتوسيع نطاق قدرتها على شن هجوم سيبراني كبير(29). واخيراً هناك التحدي السيبراني من كوريا الشمالية فعلى الرغم إنّها أقل تطوراً أثبتت جمهورية كوريا الشعبية الديمقراطية DPRK عزمها على شن هجمات إلكترونية لا يمكن التنبؤ بها إلى حد ما. تركز جمهورية كوريا الديمقراطية الشعبية في المقام الأول على عملياتها السيبرانية على جمع المعلومات الاستخباراتية بدلاً من التدمير، الموجهة بشكل رئيس إلى كوريا الجنوبية. على الأقل، فإنّ كوريا الديمقراطية لديها اهتمام واضح بالحرب السيبرانّية كوسيلة لمواجهة قدرات كوريا الجنوبية والولايات المتحدة(30).

ثانياً : الاستراتيجيات الوطنية للامن السيبراني

تتعدد اساليب وآليات حماية الامن السيبراني والتي تتمثل بجهود الانظمة السياسية لضمان توفير الحماية لفضاءها الالكتروني ونجدها بوسائل كثيرة اهمها(31):

1- تشكيل قوات عسكرية سيبرانية بمثابة جيوش ورصد نفقات من اجل تحديثها لاغراض شن الهجمات وتشكيل الدفاعات وحمايتها ، فنجد الولايات المتحدة الامريكية تقع في المرتبة الاولى في اقامة وتأسيس الجيوش الالكترونية عبر رصدها لميزانية خاصة لهذا المجال.

2-بناء مؤسسات وطنية للامن السيبراني فالحروب السيبرانية لا تميز بين مواطن وهيئات مدنية أو مؤسسات عسكرية وبالتالي هذه المؤسسات تكون وظيفتها الاساسية تشكيل الوعي ورفع مستواه فيما يخص بالأمن السيبراني واعداد استراتيجية ورسم معايير وسياسات وطنية لتشفير المعلومات والبيانات الخاصة بهذا الشأن, وضرورة تشريع القوانين الوطنية في مكافحة الجرائم الالكترونية (32).

3- وضع آليات ووسائل تقنية: ومثل هذه الاليات بناء جدران نارية للحماية حي تُعد من اهم الاليات التقنية للمواجهة التهديدات والهجمات السيبرانية, ووظيفتها الاساسية هي التمييز بين الاجزاء الموثوق بها عن الاماكن غير الموثوق بها في شبكات المعلومات الدولية ،وهناك اليات اخرى تسمى الفيروسات المضادة تستعمل من اجل أكتشاف البرمجيات التي تتصف بالمؤذية والضارة للحيلولة دون ان تلحق اضرار في اجهزة الحواسيب او ان تستحوذ على بيانات ومعلومات شخصية والتصدي لعمليات التجسس الالكتروني (33).

4-تفعيل الاجراءات للاجهزة المؤسسية : والتي تعمل على انشاء مؤسسات خاصة في اعمال امن المعلومات ورسم المعايير المسؤولة عن وظيفة التداول الالكتروني للمعلومات والبيانات وتشفيرها ويتم حفظها من اجل منعها من عملية الاندثا (34).

ثالثاً: استرتيجية الامن السيبراني العراقي:

تهدف هذه الاستراتيجية هو توفير خارطة طريق متماسكة ومبادرات والآليات للتنفيذ ولتحقيق الرؤية الوطنية بشأن الامن السيبراني. حيث يوفر الفضاء الالكتروني منصات وفرصاً ممتازة لتأمين وتنمية اقتصاد البلاد. وسيصبح الفضاء الالكتروني هو الاتجاه السائد لتحقيق التكامل الوطني وتمكين الاقتصاد الرقمي , وهو فضاء مدعوم بالمعرفة مع قدرة هائلة في غلق الثغرات والفراغات جراء عمليات التجارة والنقل والتعليم وكل هياكل البنى التحتية للدولة وكذلك مكافحة الفقر وتحقيق التنمية الاقتصادية . ومن الطبيعي ان تتواجد في كل دولة ثلاث مجالات وهي البر والبحر والجو ، وهنا يجب ان يعتبر العراق ان الفضاء الالكتروني هو المجال الرابع نظراً لتأثيره الهائل والفعال في قيادة المهام الوطنية الحرجة مثل تحقيق التنمية الاقتصادية و وتطوير حقل التجارة والمعاملات المالية والنقدية، اضافة الى دوره الواضح في المؤسسة العسكرية وحماية الامن القومي العراقي (35).

1- انعكاسات مخاطر الفضاء السيبراني على مجال الامن القومي وحقل الاقتصاد

ان النمو الاقتصادي المتقدم للبلد يعتمد بشكل اساس على الاسس المتطورة والرقمية للبنية التحتية. وفي الفضاء السيبراني، فهناك علاقات تأثير متبادلة مع جهات فاعلة ودول اخرى تتعاون فيما بينها في هذا المجال عبر استخدام شبكات متداخلة للمعلومات والبيانات تتعلق بالبنى التحتية، فبالتالي نجد ان الدولة معرضة للتهديدات والمخاطر التي يمكن معرفتها أو التنبوء بها أو تكون بالعكس غير متعرف عليها. داخل الشبكة العالمية للشبكات، توجد عيوب هيكلية حرجة يمكن استغلالها لأغراض خبيثة ونوايا جنائية ضد البلد من أجل المساس بسرية المعلومات القومية وانظمة المعلومات للبنى التحتية الاساسية وسلامتها وسبل توفرها او القدرة في الوصول اليها والتي تحمل تداعيات واثار سلبية على الفرد والامن الوطني للدولة (36).

هناك العديد من الثغرات في الفضاء السيبراني التي بالامكان استخدامها من قبل الخصم أو الاطراف العدائية لأستغلال المقومات الاقتصادية الوطنية والتي تعُد تهديدا لأمن الدولة القومي .فمثلاً التخريب والدمار الذي اصاب عدد من المؤسسات الحكومية ، وتصاعد معدل الجرائم الالكترونية بشكل متزايد بالاضافة الى عمليات الابتزاز الالكتروني والنصب والاحتيال التي تستهدف فئات عمرية محددة مثل فئة الشباب ، وتسيس او استغلال بعض وسائل الاعلام لشن حملات تخريبية ضد الدولة واشاعة الفوضى والعنف بتوظيف وسائل الاعلام الجديد. وهناك عمليات التجسس الالكتروني المنسق والتدخل

الخبيث في أنظمة الكمبيوتر والاجهزة الرقمية الاخرى, كذلك القرصنة الالكترونية, سرقة الاصول الفكرية الارهاب الالكتروني, الجرائم المالية عبر الانترنت(37).

2- الامن السيبراني في سياق استراتيجية الامن القومي:

توفير الامن لهياكل البنى التحتية الفعالة للمعلومات وغيرها من العناصر الاساسية في انظمة البيانات والمعلومات في ظل التحديات المعاصرة هو يُعد مسؤولية وطنية حساسة ، فمن اجل ان يكون هناك امن وطني فعال لابد من توافر اطار متماسك وقوي للامن السيبراني وتهيئة استراتيجية شاملة حيال المشهد او الوضع الامني الراهن أو حيال التصورات المستقبلية ، ان الامن الوطني وموارد الاقتصاد الوطني يتماشى مع المتغيرات العالمية المتسارعة المتجهة الى التطور الرقمي في مجالات الحياة كافة . فهناك بعض الاطراف الحكومية الفاعلة نتيجة لطبيعة الاختلاف في الرؤى والاتجاهات وكذلك الجهات غير الحكومية يتم توظيفها في القيام بعدد من الجرائم الالكترونية والتي يتم تجهيزها بوسائل وادوات تقنية متطورة تؤدي الى الاضرار في اغلب هياكل وقطاعات الدولة ، لكن الحكومة العراقية عملت على ايجاد عدد من المعالجات الفعالة في مواجهة هذه التهديدات الامنية ومعالجة مواطن الضعف التي تعاني منها البلاد في المجال التكنولوجيا الرقمية بأن ادرجت قضايا الامن السيبراني في مجال الفضاء الالكتروني ، بالاضافة الى تطوير القدرات التكنولوجية والاليات الرقمية من اجل الاستعداد والاستجابة السريعة في تهيئة وتوفير برامج وتدابير مضادة بالتعاون مع جهات حيوية وفاعلة سواء كانت مشروعة حكومية ام غير حكومية (38). والذي يمكن اعتباره المبادئ الاساسية لنهج السياسة الوطنية للامن السيبراني والاسس التي يتم الاعتماد عليها في توضيح وفهم استراتيجية الامن السيبراني العراقي لغرض الاستعداد للامن القومي.

3-فهم التعرض الوطني للمخاطر السيبرانية

بالتوافق مع الاوضاع والتحديات الراهنة التي تحتم على الدولة تزايد اليات الاهتمام من اجل الولوج الى المجال الرابع وهو الفضاء السيبراني العالمي ، ان هذا الدخول والتواجد الوطني سوف يُعرض الدولة الى تحديات وابعاد جديدة من المخاطر. ولذلك، يتم تطوير استراتيجية الامن السيبراني العراقي من فحص التعرض لمخاطر الامن في البلد بأسره(39). ان الاخطار السيبرانية بامكانها توظيف واستثمار مواطن الضعف الحالية والمتوافرة مما يؤثر سلباً على سلامة وضمان امن المعلومات للانظمة والشبكات او هياكل البنية التحتية. ويمكن تقسيم مكونات المخاطر السيبرانية الوطنية الى مكونين اساسيين : التهديدات الالكترونية والثغرات الموجودة في شبكات ونظم المعلومات و المدى الذي نكون فيه معرضين للهجمات السيبرانية (40).

4- مصادر التهديد السيبراني العراقي

في السياسات الامن السيبراني الدولي فان هنالك (خمسة تهديدات سيبرانية رئيسية) وهي الدول الاجنبية والنقابات الجنائية المنظمة والارهابيين والجماعات المنظمة والهاكرز والشركات, وتعتبر على أنها مخالفة لأستراتيجية الامن الوطني للدولة. ولهذه التهديدات قدرة كبيرة على إحداث أضرار جسيمة لسلامة اقتصاد البلد تتمثل الايديولوجية الاساسية لهذه الاستراتيجية الوطنية للامن السيبراني في تقديم الاطر والآليات الاستراتيجية ذات العلاقة من اجل ايجاد حلول ومعالجات اساسية لمواجهة التهديدات السيبرانية وضمان تأمين الامن في مجابهة مخاطر التهديدات السيبرانية(41).

5- تقييم مواطن الضعف الوطنية

مواطن الضعف هي الثغرات التي تتسم بالضعف الهيكلي لانظمة الاتصالات والمعلومات الحيوية في البلاد وهياكل البنية التحتية الهامة للمعلومات التي تقف بين الثغرات التقنية، واجراءات التدبيرية التي لم تخضع مسبقاً للدراسة ، والاهمال من قبل الاطراف المعنية . تتطلب الاستراتيجية الوطنية للامن السيبراني إجراء عمليات تقييم تشمل جميع مؤسسات الدولة ، وتقديم سلسلة من الحلول في كيفية معالجة البيانات والتي تساعد في معرفة القدرة ام عدمها وفي تقدير مستوى الاستعداد(42), ان الغرض الرئيس من بناء هذه الاستراتيجية هو ايجاد آليات واجراءات مضادة تساعد في رفع قدرة البلد على ايجاد مزيد من الحلول لسد الثغرات الهائلة في مواطن الضعف القائمة بين شبكات نظم المعلومات، والبنى التحتية الاساسية للمعلومات، وضمان توفير الحماية لوجود الدولة المستقبلي في الفضاء السيبراني , فهناك جهود مبذولة تهدف إلى مواجهة بعض هذه التحديات ومعالجتها على مستوى الهيئات الوزارية عبر الاستعانة بفريق الاستجابة للحوادث الالكترونية العراقي. ومع ذلك، تسعى استراتيجية الامن السيبراني العراقي على ضرورة تأسيس آلية وبرنامج فعال من اجل تنسيق العمل لمعايير النظام البيئي السيبراني للبلاد مع وضع نهج مؤطر وموحد للأمن السيبراني.

الخاتمة :

وفي خلاصة القول نجد ان التطور الحاصل في تقنية الاتصال والمعلومات هو يمكن استخدامه من قبل الدول بشكل مزدوج اي هو سلاح ذو حدين ، فهو بالامكان ان يتم استخدامه في تحسين البيئة الامنية والمجال الرقمي في جميع القطاعات ، مما يمكنها ان تضحى قوة تكنولوجية هائلة وقادرة على حماية امنها السيبراني دون الحاجة الى الاستعانة بقدرات الغير، ومن جانب آخر قد يمكن الدول من الاستحواذ على قدرة تكنولوجية دون الاستخدام الامثل، حيث يمكن ان تستخدمها في توجيه تهديدات وهجمات سيبرانية ضد الخصوم، أو حتى القيام باختراق المنظومة الامنية للمعلومات والبيانات الحساسة للدول الاخرى واخضاعها للابتزاز الالكتروني أو فرض الاذعان لمطالب الدولة التي شنت الهجمات

السيبرانية ، مما قد يؤدي الى تحول كبير في مفهوم الامن والقوة السيبرانية , والتي لم تعد تقتصر على بعُد واحد في تطوير البيئة السيبرانية بل على ابعاد متعددة في مجال الاقتصاد والمال والقوة العسكرية والتكنولوجية من اجل حماية فضاءها الالكتروني الذي يُعد في مقدمة اولويات استراتيجية الامن الوطني بهدف الحفاظ على امنها القومي بكل الوسائل والاليات المشروعة وغير المشروعة مستغلة الضعف الدولي في تفعيل تشريعات واتفاقيات تعاونية في ردع الخروقات التي تهدف الامن السيبراني.

النتائج والتوصيات: من النتائج التي تم التوصل اليها في هذه الدراسة هي:

1-ان الفضاء الالكتروني قد ارغم المجتمع الدولي بضرورة الاعتراف به كمتغير استراتيجي مؤثر وبُعد جديد في ادارة الصراعات الدولية وذلك للخصائص والسمات التي يتسم بها هذا المتغير.

2- ان التطور الهائل في مجال تكنولوجيا الاتصال والمعلومات قد تم توظيفه واستثماره من قبل فواعل دولية وغير دولية تسببت بتهديد واختراق الامن السيبراني للعديد من الدول.

3-الكثير من الدول تتصف بضعف القدرة والامكانات على ضمان امنها السيبراني او حتى توفير الحماية اللازمة لفضائها الالكتروني بشكل مطلق ، وذلك بسبب الخصائص التي تتسم بها طبيعة الهجمات والتهديدات السيبرانية بكونها مجهولة المصدر، ومتعددة في طبيعة استهداف الخصم ، بالاضافة الى انها تتسم بمحاكاتها للتطور الحاصل في مجال تكنولوجيا الفضاء السيبراني.

التوصيات:

1- لابد للمجتمع الدولي ان يسعى الى مزيد من عمليات الفهم والادراك لطبيعة الفضاء السيبراني ، وعده عاملاً وعنصراً رئيساً في تعزيز الامن القومي السيبراني لما له من علاقة وثيقة بتحسين قضايا وموضوعات التنمية السياسية وتحقيق الرفاهية والازدهار الاقتصادي

2-ضرورة تفعيل التشريعات والقوانين التي تنظم الفضاء الالكتروني منها قوانين الامن الالكتروني

3- الحث على نشر التوعية بخطورة تهديد الامن السيبراني للدولة والهدف منه حتى يكون هناك فهم وادراك لدور الافراد في بناء الامن.

4- تعزيز مجالات واليات التعاون الدولي والاقليمي في حقل مكافحة المخاطر والتهديدات التي يتعرض لها الامن السيبراني الوطني وحق الدول في فرض هيمنتها على فضاءها الالكتروني.

الهوامش:

1) منى الاشقر, الامن السيبراني : التحديات ومستلزمات المواجهة, المركز العربي للبحوث القانونية والقضائية, جامعة الدول العربية, 2012, ص89.
2) المصدر نفسه, ص92.
3) نورة شلوش, القراصنة الالكترونية في الفضاء السيبراني" التهديد المتصاعد لأمن الدول, مجلة مركز بابل للدراسات الانسانية, المجلد 8 , العدد 2, ص156.
4) أيهاب خليفة ،حروب مواقع التواصل الاجتماعي ،العربي للنشر والتوزيع ، 2016 , ص58
5) ايهاب خليفة, مجتمع ما بعد المعلومات: تأثير الثورة الصناعية الرابعة على الأمن القومي، ابو ضبي: العربي للنشر والتوزيع، 2014, ص85
6) أيهاب خليفة، القوة الالكترونية: كيف تدير الدول شؤونها في عصر الانترنيت "الولايات المتحدة الامريكية نموذجاً"، القاهرة: العربي للنشر والتوزيع، ط1، 2017, ص98
7) ايهاب خليفة، حروب مواقع التواصل الاجتماعي ، مصدر سبق ذكره , ص47
8) المصدر نفسه, ص45.
9) ذياب موسى البداينة، الأمن وحروب المعلومات، دار الشروق للنشر والتوزيع، 2002, ص67
10) سين إس كوستجان، الأمن السيبراني منهج مرجعي عام، نشر: مركز جورج كاتليت مارشال الأوروبي للدراسات الأمنية، منظمة حلف شمال الأطلسي أكتوبر، 2012, ص86
11) المصدر نفسه, ص90
12) عادل عبد الرزاق، الفضاء الالكتروني والعلاقات الدولية: دراسة في النظرية والتطبيق, القاهرة: المكتبة الاكاديمية، 2016, ص68
13) المصدر نفسه, ص70
14) عادل عبد الصادق، الارهاب الالكتروني القوة في العلاقات الدولية نمط جديد وتحديات مختلفة ،الطبعة الاولى مركز الاهرام للدراسات السياسية والاستراتيجية , القاهرة , 2009, ص99
15) سين اس كوستجان , مصدر سبق ذكره, ص90.
16) منى الاشقر جبور, السيبرانية هاجس العصر، جامعة الدول العربية–المركز العربي للبحوث القانونية والقضائية، بيروت, 2016, ص62.
17) المصدر نفسه, ص57.
18) ماري آيكن , التأثير السيبراني (كيف يغير الإنترنيت سلوك البشر), الدار العربية للعلوم ناشرون , بيروت :لبنان، 2018, ص56
19) مجدي كامل، حروب الجيل الرابع، (الحرب بالوكالة)، دار الكتاب العربي،2016, ص67
20) منى الاشقر جيور, السيبرانية هاجس العصر, مصدر سبق ذكره, ص79.
21) أحمد عبد الغني محمد ، السيبرانية كمدخل لتحول مفهوم التصوير الى فن ما بعد الحداثة للقرن الحادى والعشرين، كلية التربية الفنية, 2000, ص98
22) إريك غارتسك ، "أسطورة الحرب الإلكترونية: إعادة الحرب في الفضاء السيبراني إلى الأرض" ، الأمن الدولي ، 2013 , ص88
23) المصدر نفسه, ص90.

24)جيمس روزنو ، ثورة المعلومات قوية ومحايدة معا: كتاب توماس كوبلاند ، ثورة المعلومات والأمن القومي ، دراسات دولية ، 46 ، ط1 ، 2003 , ص54

25)اسماعيل صبري مقلد ، ثورة المعلومات وحروب المستقبل المحتملة ، مجلـة آفاق المستقبل، ابوظبي، 2010 , ص87

26)ديفيد جومبرت ، الحرية والقوة في عصر المعلومات ، " دراسات عالمية : الدور المتغير للمعلومات في الحرب ، تحليل (زلمي خليل زاد وجون واين) ، " ابو ظبي : مركز الامارات للدراسات والبحوث الاستراتيجية ، 2004 , ص54

27)المصدر نفسه, ص59.

28)شادي عبد الوهاب منصور, حرب الجيل الخامس , اساليب تفجير من الداخل على الساحة الدولية , ط1 , المستقبل للابحاث والدراسات المتقدمة , القاهرة , 2019, ص77

29)علي زياد العلي , الصراع والامن الجيوسيبراني في الساحة الدولية : دراسة في استراتيجيات الاشتباك الرقمي, دار أمجد للنشر والتوزيع, ط1, الاردن, 2019, ص45

30)جيمس روزنو, مصدر سبق ذكره, ص60

31)جون باسيت, حروب الفضاء الالكتروني واساليب الدفاع الجديدة , من كتاب الحروب المستقبلية في القرن الحادي والعشرين ,مركز الامارات للدراسات والبحوث الاستراتيجية, ط1, 2014, ص59

32)اماني عصام محمد, استخدام روسيا للقوة السيبرانية في ادارة تفاعلاتها الدولية, مجلة كلية الاقتصاد والعلوم السياسية, جامعة حلوان, العدد 4, مصر, 2021, ص50-54

33)المصدر نفسه, ص60

34)باسم علي خريسان, الامن السيبراني في العراق قراءة في مؤشر الامن السيبراني العالمي 2020, مركز البيان للدراسات والتخطيط, العراق, 2021, ص45

35)المصدر نفسه, ص47

36)تغريد صفاء ولبنى خميس, أثر السيبرانية في تطور القوة, جامعة النهرين, كلية العلوم السياسية , مجلة حمورابي, العدد 33-34, السنة الثامنة, 2020, ص120.

37)عبد الفتاح علي الرشدان, تطور مفهوم الامن العالمي في عالم متغير , دراسات , الجامعة الاردنية , كلية العلوم الانسانية والاجتماعية, العدد 3, 2019, ص75.

38)تغريد صفاء ولبنى خميس, مصدر سبق ذكره, ص123

39)محمد ميسر, استراتيجية مكافحة الارهاب السيبراني, المجلة العلمية لجهاز مكافحة الارهاب, العدد 2, العراق, 2021, ص79.

40)محمد وائل القيسي, مستقبل الامن الاستراتيجي العالمي في ظل التحديات التكنو- معلوماتية والفضاء السيبراني , مجلة دراسات اقليمية, العدد 44, الجامعة اللبنانية –الفرنسية , اربيل , العراق, 2020, ص96.

41)باسم علي خريسان, مصدر سبق ذكره, ص60

42)محمد ميسر، مصدر سبق ذكره،ص81.