مجلة العلوم القانونية و الاجتماعية

Journal of legal and social studies

Issn: 2507-7333

Eissn: 2676-1742

الفضاء السيبراني وتحديات الأمن القومي للدول

Cyberspace and national security challenges for countries.

مسيكة محمد*

جامعة طاهري محمد، بشار (الجزائر)، messika.mohamed@univ-bechar.dz،

تاريخ ارسال المقال:2022/09/10	تاريخ القبول: 2022/10/15	تاريخ النشر: 2022/12/01

*المؤلف المرسل

الملخص:

في ظل موجة الذكاء الاصطناعي والثورة المعلوماتية الناجمة عن التطور التكنولوجي المتسارع، وتحول نسق الاتصال بين الأفراد والمؤسسات، واتجاه الدول نحو تحديث منظوماتها وأجهزتها تماشيا مع متطلبات العصر، وظهور تأثيرات الفضاء السيبراني الجوهرية على حياة البشرية، حيث أنه بالقدر الذي أصبح فيه بإمكان الأفراد المشاركة في رسم السياسات وصياغتها، فقد تغيرات مفاهيم الأمن بالنسبة للدولة، وانتقلت من مفهومه في صياغته التقليدية إلى مفهومه غير التقليدي، انتقال ينسحب أيضا على مجال التهديدات الأمنية التي انتقلت هي الأخرى إلى تهديدات غير تقليدية نتيجة الاستخدامات المتنوعة للثورة التكنولوجيا والاتصالات، وهذا تحول أصبح معه مفهوم الأمن السيبراني أحد العناصر الأساسية الضامنة للأمن القومي للدولة.

ولذلك تحاول هذه الدراسة الإجابة على التساؤل التالي: إلى أي مدى يمكن أن يشكل الفضاء السيبراني تهديدا للأمن القومي للدولة؟ من خلال ثلاثة محاور:

مفهوم الأمن القومي وأبعاده./تهديدات الفضاء السيبراني للأمن القومي./ الأمن السيبراني كضمان للأمن القومي.

الكلمات المفتاحية: الفضاء السيبراني؛ الأمن القومي ؛ الأمن السيبراني؛ الارهاب الالكتروني.

Abstract:

In light of the wave of artificial intelligence and the information revolution caused by the rapid technological development، shifting the mode of communication between individuals and institutions, And the trend of countries towards modernizing their systems and devices in line with the requirements of the times, The emergence of the fundamental effects of cyberspace on human life, Whereas, to the extent that individuals can participate in policy formulation and formulation, the concepts of security for the state have changed, And moved from its concept in its traditional formulation to its non-traditional concept, The transition also applies to the field of security threats, which have also moved to non-traditional threats as a result of the diverse uses of the technology and communications revolution, This is a transformation with which the concept of cyber security has become one of the basic elements that guarantee the national security of the state.

Therefore, this study attempts to answer the following question: To what extent can cyberspace pose a threat to the national security of the state? Through three axes:

The concept of national security and its dimensions./ Cyber threats to national security./ Cyber security as a guarantee of national security.

Keywords: cyber space; National Security ; cyber security; Electronic terrorism.

مقدمة:

يعيش عالم اليوم ثورة تكنولوجية غير مسبوقة يطبعها الذكاء الاصطناعي، إنترنت الأشياء، وسلاسل الكُتلة... وغيرها من التقنيات الذكيَّة، وقد أدت هذه الثورة إلى تحول ليس الأول عبر التاريخ لكنه الأقوى، حيث يتجلى ذلك من خلال تأثير الاختراعات التكنولوجية على طرق التواصل بين الأفراد والمؤسسات في اختراع الشبكات الاجتماعية وشبكة الويب.

فمع التطور الهائل الذي يشهده الفضاء الإلكتروني المتاح للأفراد والمؤسسات في تسيير أمورهم، وتستخدمه الدولة ووزاراتها في تنظيم أجهزتها تماشيا مع متطلبات العصر، فقد أصبح هذا الفضاء عنصرا حيويا مهما ذا أثر جوهري في الحياة البشرية، حتى أصبحنا نتحدث عن التجارة الإلكترونية والحكومة الإلكترونية والصحافة الإلكترونية، وبات من الواضح جليا أن من يمتلك آليات توظيف هذه البيئة الإلكترونية الجديدة، يكون الأكثر قدرة على التأثير في سلوك الفاعلين المستخدمين لهذه البيئة.

ومن أهم تجليات الفضاء الالكتروني أنه أدي بالمجتمعات إلى الانتقال من مرحلة تبني النموذج القائم على مركزية دور الدولة في صنع السياسات إلى مشاركة الأفراد في رسمها وصياغتها، كما أثرت هذه الثورة التكنولوجية على أشكال الحروب والصراعات البشرية، وتغير مفهوم تهديد الأمن بالنسبة للدولة من المفهوم التقليدي القائم على مجالات (البر، الجو، البحر، الفضاء)، إلى مفهوم جديد للتهديدات الأمنية غير التقليدية التي تشمل مجالا خامسا هو الفضاء السيبراني، فمن التهديدات التقليدية إلى نوع جديد من التهديدات يشمل الصراعات الإلكترونية، التي أصبحت تهدد الأمن القومي للدول، فقد غيرت من أشكال الحكومات ووظائفها أحيانا، لتلقي على الحكومات أعباء وتحديات غير تقليدية إزاء التهديدات الجديدة التي يطرحها استخدام التكنولوجيا الحديثة في الفضاء السيبراني، مثل الجرائم الإلكترونية، الإرهاب الالكتروني، وكذا الحرب الالكترونية. وكيف لهذه الدول أن تحمي أمنها القومي من مخاطر هذه التهديدات.

ومن هنا تنبع إشكالية الدراسة المتمحورة حول التساؤل التالي:

إلى أي مدى يمكن أن يشكل الفضاء السيبراني تهديدا للأمن القومي للدولة؟

وتتفرع عن هذه الإشكالية أسئلة فرعية:

- ما هو مفهوم الأمن القومي وما أبعاده ؟
- فيما تتجلى تهديدات الفضاء السيبراني لأمن القومي؟
- هل يعد الأمن السيبراني ضمانا للأمن القومي؟

وللإجابة على هذه الإشكالية وتساؤلاتها الفرعية تبنى هذه الدراسة على الفرضيات التالية:

الفرضية الأولى: يشتمل الفضاء السيبراني على تهديدات جديدة للأمن القومي للدولة.

الفرضية الثانية: يعد الأمن السيبراني من أهم ضمانات الأمن القومي غير التقليدي للدولة.

منهج الدراسة:

اعتمدت الدراسة على المنهج الوصفي التحليلي الذي يسعى وصف وتحليل، وتشخيص، الموضوع من مختلف جوانبه وأبعاده، بهدف التوصل إلى مفهوم الأمن السيبراني والأمن القومي، والوقوف على مدى أهمية الفضاء السيبراني والتهديدات التي قد تنجم عنه.

المحور الأول: مفهوم الأمن القومي وأبعاده.

أولا: مفهوم الأمن القومي.

شاع مصطلح الأمن القومي بعد الحرب العالمية الثانية، إلا أن جذوره تعود إلى القرن السابع عشر، وبخاصة بعد معاهدة وستفاليا عام 1648 التي أسست الدولة القومية أو الدولة – الأمة Nation – State وشكلت حقبة الحرب الباردة الإطار والمناخ اللذين تحركت فيهما محاولات صياغة مقاربات نظرية وأطر مؤسساتية وصولاً إلى استخدام تعبير"إستراتيجية الأمن القومي"، وسادت مصطلحات الحرب الباردة مثل الاحتواء والردع والتوازن والتعايش السلمي كعناوين بارزة في هذه المقاربات بهدف تحقيق الأمن والسلم وتجنب الحروب المدمرة التي شهدها النصف الأول من القرن العشرين[1].

لقد تطور مفهوم الأمن القومي تجاه التهديدات الجديدة غير التقليدية واتسع مجال الأمن ليمتد من الجانب العسكري لمجالات أخرى عديدة، وإذا كان الأمن القومي يعنى بالحماية وغياب التهديد لقيم المجتمع الأساسية، وغياب الخوف من خطر تعرض هذه القيم للهجوم، فإن الفضاء السيبراني قد فرض إعادة التفكير في مفهوم الأمن، وفي هذا المحور وقبل التطرق إلى مصطلح الأمن القومي سنحاول تفكيكه لمعالجة مفهوم الأمن ومن ثم القومية لنصل في محصلة المحور إلى مفهوم الأمن القومي وأبعاده.

1/ مفهوم الأمن لغة واصطلاحا:

أ/ الأمن لغة:

الأمن في اللغة هو نقيض الخوف، والفعل الثلاثي أَمِن أي حقق الأمان، قال ابن منظور: "أمنت فأنا آمن، وأمنت غيري أي ضد أخفته، فالأمن ضد الخوف، والأمانة ضد الخيانة، والإيمان ضد الكفر، والإيمان بمعنى التصديق، وضده التكذيب، فيقال آمن به قوم وكذب به قوم"[2].

وكلمة الأمن بهذا المعنى ترمي إلى معنيين رئيسيين هما سكون القلب، كما قال ابن فارس والرازي والثقة والطمأنينة كما قال الزمخشري[3].

وقد ورد المفهوم في القرآن الكريم بقوله تعالى: "فليعبدوا رب هذا البيت الذي أطعمهم من جوع وآمنهم من خوف"[4].

ومن خلال ما تقدَّم من كلام وأقوال أهل اللغة والبيان يتَّضِح أنَّ للأمن في لغة العرب إطلاقات عِدَّة، فهو يعني: "الطمأنينة، وعدم الخوف، والثِّقة، وعدم الخيانة[5].

ب/ الأمن اصطلاحا

أما عن"الأمن" في الاصطلاح فيشير إلى شعور عام بالطمأنينة، وهذا الشعور ناجم عن اعتقاد بالقدرة على مواجهة كافة أنواع المخاطر أو التهديدات، والسيطرة على كافة الأدوات والآليات الكفيلة بمواجهة تلك المخاطر

والتهديدات، أيا كان مصدرها، سواء بالاعتماد على الموارد والقدرات الذاتية، أو على موارد وقدرات الآخرين من الحلفاء والأصدقاء، وكل الراغبين في مد يد العون والمساعدة[6].

وتتفق معظم الأدبيات التي قامت بتعريف مفهوم الأمن على أن المفهوم يشير عموماً إلى تحقيق حالة من انعدام الشعور بالخوف، وإحلال شعور الأمان ببعديه النفسي والجسدي محل الشعور بالخوف، والشعور بالأمان قيمة إنسانية كونية مرغوبة لا تقتصر على فئة اجتماعية معينة أو مرتبطة بمستوى الدخل، فالفقير مثل الغني يحتاج إلى الشعور بالأمان ويسعى إلى تحقيقه وإن اختلفت درجات المتمتع به، ونظراً لصعوبة تحقيق الأمان الكامل، فقد أصبح يُنظر للأمن على أنه مسألة نسبية مرهونة بالسعي لتعزيز أفضل الشروط لتوافره[7].

والحديث عن الأمن، يستدعي تعريف الخطر،أي التهديد الذي يتعرض له النظام إضافة إلى نقاط الضعف، أو الثغرات التي تعتريه، ومن ثم الإجراءات المفروض اتخاذها، لدفع الخطر. فالتهديد هو نوع الأعمال العدائية، التي يمكن أن تمارس ضد النظام، بينما نقاط الضعف هي مستوى الانكشاف على هذا التهديد، في سياق معين. والإجراءات التي يفترض اتخاذها، لا يمكن أن تقتصر في أي حال من الأحوال على التقنية، بل أنها تتناول بناء القدرات، والتوعية، والتدريب، ونقل الخبرات، عدا عن مجموعة من القواعد المحددة والواضحة، التي يفترض إتباعها[8].

2/ مفهوم القومية لغة واصطلاحا:

أ/ القومية لغة:

الجذر اللغوي لكلمة القومية هو (ق.و.م)، والقوم يعني الرجال دون النساء، وهو لفظ جمعي لا واحد له، وربما يدخل النساء فيه على سبيل التبع، وجمع القوم أقوام. أما الفعل الثلاثي منها قام، والرباعي أقام، ومنها يأتي معني الارتباط بالمكان[9].

ب/ اصطلاحا:

والقوم هم الجماعة التي ترتبط بمكان ما وتقيم فيه، وعندما يوجد قوم من الناس في أرض واحدة ويمارس أفراده الحياة بثقافة واحدة توجد بينهم علاقات أخرى قوية تدور حول المصلحة المشتركة والتضامن والنسب، وعلاقات اجتماعية تجعلهم يداً واحدة، وتلك الروابط هي التي توجد ما يُسمى بالقومية[10].

والقومية هي صلة اجتماعية عاطفية تنشأ من الاشتراك في الوطن والجنس واللغة والمنافع وقد تنْتهي بالتضامن والتعاون إلى الوحدة، وتعد مبدأ سياسيا اجتماعيا يُفضل معه صاحبه كل ما يتعلق بأمته على سواه مما يتعلق بغيرها، أو هي الاعتقادُ السائد لدى الشعب في أنه يشكل جماعة متميزة ذات سمات خاصة تميزه عن الآخرين، مع توفر الرغبة في حماية هذا التميز والارتقاء به ضمن حكومة ذاتية[11].

ومفهوم "القومي" في الاصطلاح يعرف على أنه الشعور بالانتماء إلى مجموعة بشرية معينة ترتبط فيما بينها بروابط مشتركة، قد تكون ناجمة عن وحدة الأصل العرقي، أو اللغة والثقافة، أو التاريخ والمصالح المشتركة، وبالتالي تشعر بأن لها هُوية خاصة تميزها عن "أقوام" أخرى مختلفة عنها في كُل ـ أو بعض ـ هذه السمات[12].

3/ مفهوم الأمن القومي:

يعرف تريجر وكرننبرج الأمن القومي بأنه "ذلك الجزء من سياسة الحكومة الذي يستهدف خلق الظروف المواتية لحماية القيم الحيوية، ويعرفه هنري كيسنجر بأنه يعني "أية تصرفات يسعى المجتمع – عن طريقها – إلى حفظ حقه في البقاء، أما **روبرت ماكنمارا** فيرى أن "الأمن هو التنمية، وبدون تنمية لا يمكن أن يوجد أمن، والدول التي لا تنمو في الواقع، لا يمكن ببساطة أن تظل آمنة" [13].

وتعرف الأمانة العامة لجامعة الدول العربية، الأمن القومي بأنه قدرة الأمة على الدفاع عن أمنها، وحقوقها، وصياغة استقلالها، وسيادتها على أراضيها، وتنمية القدرات والإمكانات العربية، في مختلف المجالات، مستندة إلى القدرة العسكرية والدبلوماسية، آخذة في الاعتبار الاحتياجات الأمنية الوطنية لكل دولة، والإمكانات المتاحة، والمتغيرات الداخلية والإقليمية والدولية، التي تؤثر على الأمن القومي العربي.

ولم يعد تعريف الأمن القومي مرتبطا بالتهديدات القديمة فقط، بل هناك نوع آخر من التهديدات حددت تعريفه مثل التعريف الذي قدمه "محمد جمال مظلوم " حيث اعتبر أن هناك تهديدات غير تقليدية وظواهر جديدة تهدد الأمن هي " تهديدات ذات طابع عالمي لا تقتصر على دولة بذاتها، وهي متداخلة بحيث يمكن أن تؤدي أحد التهديدات الى تهديد آخر ، أو يفاقم من نتائجه السلبية، ولا يمكن التعامل معها بشكل نهائي وفقا لنظريات الأمن في صياغته التقليدية، إذ يُعتبر الأمن السيبراني أحد عناصر الأمن القومي غير التقليدي، وذلك لأن أحد مستخدمي الفضاء الالكتروني بإمكانه أن يوقع خسائر فادحة بالطرف الأخر [14].

ولأسباب تتعلق بالأمن القومي والرفاه الاقتصادي، تحتاج الحكومات إلى المساعدة في عملية حماية البنية التحتية لمعلوماتها الحيوية، وتعزيز هذه الحماية وضمانها لا يمكن الوصول إليه إلا من خلال وجود إستراتيجية وطنية تعنى بالأمن السيبراني، وإن إستراتيجية الأمن الوطني السيبراني بشكل عام هي :"كافة التدابير المتعلقة بسرية المعلومات والبيانات التي يتم معالجتها وتخزينها وإبلاغها عن طريق وسائل إلكترونية أو مشابهة، وحمايتها والنظم المرتبطة بها من التهديدات الخارجية أو الداخلية"، وتهدف هذه الإستراتيجية إلى تطوير وتنفيذ قدرات الأمن السيبراني [15].

وما يجدر الإشارة إليه أن مفهوم الأمن القومي في تبلور واضح مع التغيرات الحاصلة في موازين القوى، إضافة إلى تطور مفهوم دور الدولة، الذي لم يعد تقليديا قائما على حقها في اللجوء إلى استخدام القوة، في الداخل، أو للدفاع عن أراضيها، ضد التهديدات الخارجية، فمع الاعتماد على الأنظمة المعلوماتية، والأجهزة المتصلة بالشبكة العالمية للمعلومات، والعملية المعقدة لطبيعة هذه الأجهزة، من هواتف ذكية، وأجهزة كمبيوتر، وارتفاع نسبة مستخدمي الفضاء السيبراني، تزداد نسبة توقع الاعتداءات و الخروقات والجرائم المعلوماتية، وهذا ما أشار إليه تقرير صادر عن **مركز ماكينزي**، الذي توقع زيادة المعلومات الرقمية، بمعدل 44% ، خلال الأعوام الممتدة من 2009 إلى 2020 [16].

إن نسبة التقارير التي تؤكد على ارتفاع نسب اختراق الأنظمة وسرقة البيانات وتسربها، كاختراق أنظمة معلومات بعض الشركات العالمية، الذي تسبب في كشف بيانات عدد كبير من المستخدمين، كذلك الأمر عند

اختراق بيانات وزارات هامة في الدولة وتدمير أنظمة معلوماتها، فهذه كارثة أمنية حقيقية تمس بأمن الدولة القومي، ما استدعى الأمر بالدول إلى ضرورة الاهتمام بهذا المجال ووضع خطط ودراسات استراتيجية لمواجهة هذه الأخطار[17].

ثانيا: أبعاد الأمن القومي.

هناك العديد من الأبعاد التي انطوت تحت مظلة الأمن وتعددت هذه الأبعاد التي يجب على الدولة حمايتها إلى خمسة أبعاد كالتالي:

أولاً: البُعد السياسي: ويتمثل في الحفاظ على الكيان السياسي للدولة وهو ذو شقين داخلي وخارجي، ويتعلق البعد الداخلي بتماسك الجبهة الداخلية والسلام الاجتماعي والوحدة الوطنية، بينما يتمثل البعد الخارجي في أطماع الدول الأخرى في مقدرات الدولة ومواردها ومدى تطابق تلك الدول مع الدولة المقصودة سياسياً واقتصاديا واجتماعيا وتحكمه مجموعة من المبادئ الإستراتيجية التي تُحدد أولويات المصالح الأمنية وأسبقياتها[18].

ثانياً: البُعد الاقتصادي: يهدف هذا البُعد إلى توفير المناخ المناسب للوفاء باحتياجات الشعب وتوفير سُبل التقدم والرفاهية للشعب؛ فمجال الأمن القومي هو الإستراتيجية العليا الوطنية التي تهتم بتنمية واستخدام كافة موارد الدولة المتاحة لتحقيق أهدافها السياسية بل أن النمو الاقتصادي والتطور التكنولوجي هما الوسيلتان الرئيسيتان لتحقيق المصالح الأمنية للدولة وبناء قوة الردع الإستراتيجية وتنمية التبادل التجاري وتصدير العمالة إلى غير ذلك من المؤشرات المهمة التي تدل على اندماج الجانب الاقتصادي بالأمن القومي[19].

ثالثاً: البُعد الاجتماعي: يهدف الأمن الاجتماعي إلى تحقيق الأمن و الاستقرار و الاطمئنان للمجتمع سواء أفرادا أو مجموعات وتنمية الشعور بالانتماء والولاء،كما يستلزم الأمن الاجتماعي تأمين الخدمات الأساسية للإنسان، فلا يشعر بالعوز والفقر والمرض و يشمل الخدمات المدرسية و الثقافية و الرعاية الإنسانية و التأمينات الاجتماعية و على مواجهة الظروف الطارئة . حتى لا يتعرض الأمن القومي للخطر فبتحقيق العدالة يكون هناك تعزيز للوحدة الوطنية والتفاف الشعب حول القيادة السياسية وعلى العكس يؤدي الظلم الاجتماعي لطبقات معينة أو تزايد نسبة المواطنين تحت خط الفقر إلى تهديد داخلي حقيقي للأمن القومي يصعب السيطرة عليه وخاصة في ظل تفاقم مشاكل البطالة والصحة والتعليم[20].

رابعاً: البُعد العسكري: تتحقق مطالب الأمن والدفاع من خلال بناء قوة عسكرية تكون قادرة على تلبية احتياجات التوازن الإستراتيجي العسكري والردع الدفاعي على المستوى الإقليمي لحماية الدولة من العدوان الخارجي وذلك من خلال الاحتفاظ بالقوة العسكرية في حالة استعداد قتالي دائم وكفاءة قتالية عالية للدفاع عن حدود الدولة وعمقها والقوة العسكرية هي الأداة الرئيسية في تأييد السياسة الخارجية للدولة وصياغة دورها القيادي على المستوى الإقليمي والدولي[21].

خامساً: البُعد الثقافي: يُحافظ البعد الثقافي على الأمن القومي من خلال حماية الفكر والمعتقدات والعادات والتقاليد والقيم وهو الذي يعزز انطلاق مصادر القوة الوطنية في كافة الميادين في مواجهة التهديدات الخارجية والتحديات الداخلية، فالدور الثقافي بالغ الأهمية في تحصين الوطن من الأطروحات الثقافية للعولمة وصراع الحضارات إذا أخذناه بمفهومه الشامل متضمناً الفكر والثقافة والتعليم والإعلام والفنون والأدب؛ إذاً فالأمن القومي يعني " تمكين الشعب من ممارسة منظومة القيم الخاصة به على أرضه المستقلة "[22].

المحور الثاني: تهديدات الفضاء السيبراني للأمن القومي.

يعطى الأمن تعريفات عديدة، تنطلق من الإمكانات العسكرية، مرورا بالحفاظ على استقرار النظام، وصولا إلى حماية القيم الجوهرية لمجتمع ما، وهو الخشية التي تبديها معظم الدول حاليا، من تعرض أمنها القومي للاعتداءات التي قد تنجم عن الفضاء السيبراني، ويلامس الأمن السيبراني الأمن القومي، بشكل وثيق، فالتقنيات التي وسعت الآفاق، وسمحت للثقافة المحلية بالامتداد إلى المجال العالمي، حيث بات وقوع هذه الاعتداءات يهدد الهوية الوطنية والقومية، مع تأثر الأجيال الصاعدة بما يصلها وبما تصل إليه عبر الإنترنت، حيث تبدو الهوية وكأنها خاضعة لعملية إعادة تشكيل، من خلال تكنولوجيا المعلومات، وحرص الغالبية العظمى من الناس، على استخدامها في تكوين مجتمعهم الخاص، وبيئتهم المميزة[23].

أولا: مفهوم الفضاء السيبراني.

يقصد بالفضاء السيبراني ذلك الوسط الذي تتواجد فيه شبكات الحاسوب ويحصل من خلالها التواصل الإلكتروني. وبمفهوم أشمل يعرف بأنه مجال مركّب مادي وغير مادي يشمل مجموعة من العناصر هي: أجهزة الكمبيوتر، أنظمة الشبكات والبرمجيات، حوسبة المعلومات، نقل وتخزين البيانات، ومستخدمي كل هذه العناصر.

يأتي أصل الكلمة اشتقاقا من اللغة اليونانية القديمة (kybernētēs) والتي تعني "مساعد التوجيه" أو "الحاكم" أو "الرائد" أو "الدفة"، استخدم مصطلح الفضاء الإلكتروني للمرة الأولى **ويليام غيبسون** (William Gibson) وهو كاتب في الخيال العلمي، ثم أشتهر المصطلح في التسعينيات بعدما أصبحت استخدامات الإنترنت والشبكات والاتصال الرقمي تنمو بشكل كبير وأصبح مصطلح الفضاء الإلكتروني قادرًا على تمثيل العديد من الأفكار والظواهر الجديدة التي ظهرت[24].

ويعرفه **فريدريك مايور** بأنه بيئة إنسانية وتكنولوجية جديدة للتعبير والمعلومات والتبادل، وهو يتكون أساسا من الأشخاص الذين ينتمون لكل الأقطار والثقافات واللغات والأعمار والمهن المرتبطة ببعضها بعضا عن طريق البنية التحتية الاتصالية، التي تسمح بتبادل المعلومات، ونقلها بطريقة رقمية، وعليه تستخدم كلمة Cyberمقترنة بكلمة Space لتشير إلى أشهر تعبير في عصر المعلومات، وأصبح هذا المفهوم أشمل وأوسع من انترنت ليضم كل الاتصالات والشبكات وقواعد البيانات، ويشير كذلك إلى مجموعة المعلومات المتوفرة إلكترونيا ويتم تبادلها وتشكيلها في مجموعات بناء على استخدامها، ويعمل الفضاء الالكتروني تحت ظروف مادية غير تقليدية حيث يكون وسيطا عبر العمل من خلال أجهزة الكمبيوتر وشبكات الاتصال[25].

ثانيا: التهديدات السيبرانية.

تعددت مصادر تهديد الأمن القومي، فهناك تهديدات مباشرة ذات تأثير عال واحتمالية حدوث عالية، ومنها "الهجمات السيبرانية " Cyber Attacks التي قد تأخذ عدة أشكال أكثر تطورا من مجرد هجمات، وذلك مثل الحروب السيبرانية ، Cyber warfare التي تأتي أيضا في إطار عدم الاستقرار السياسي، والإرهاب السيبراني، حيث تمثل هذه المجموعة مصادر للتهديد المباشر للأمن القومي للدول.

1: الهجمات السيبرانية.

أصبحت الهجمات السيبرانية من أخطر مصادر تهديد الأمن القومي، وهي تلك الهجمات التي تتم عبر شبكة الإنترنت بهدف التدمير أو التجسس أو التزييف، سواء كانت عبر أجهزة كمبيوتر، أو هواتف ذكية... بل يتعدى الأمر ذلك ليشمل أيضا الأجهزة غير المتصلة بالإنترنت مثل المولدات والمحركات، والتي يمكن تدميرها عبر فيروسات الكمبيوتر، وتكون الخسائر في هذه الحالة فادحة، خاصة إذا استهدفت البنية التحتية للدولة، وحدد إيهاب خليفة أنواع الهجمات السيبرانية وفقا لمعايير معينة وضحها كما يلي[26]:

معايير تصنيف الهجمات السيبرانية:

تتعدد أنواع الهجمات السيبرانية وفقا لعدة معايير، فقد يكون المعيار هو أسلوب تنفيذ الهجمة نفسها، أو قطاع الجمهور المستهدف منها، أو الهدف النهائي المرجو تحقيقه منها، أو الفواعل المشاركون فيها.

أ/ **حسب الأسلوب المستخدم:** تتعدد هذه الأساليب لتنفيذ الهجمات السيبرانية، ومنها :

- **هجمات التصيد Phishing**: يعتمد هذا الأسلوب على الهندسة الاجتماعية Engineering Social من خال تحفيز الضحية لفتح رابط يحتوي على برمجية خبيثة تصيب الجهاز.
- **هجمات وقف الخدمة DDOS** : وإغراق الضحية بالآلاف من الرسائل والطلبات التي تؤدي في النهاية إلى انقطاع الخدمة ووقفها، سواء كان ذلك موقع إنترنت، أو خدمة إلكترونية خاصة، أو حكومية.
- **الأبواب الخلفية Backdoors**: ثغرات مقصودة توضع على أجهزة الضحايا بهدف التجسس والمراقبة أو جمع المعلومات.

ب/ حسب القطاع المستهدف:

قد يكونون أفرادا عاديين يتم اختراقهم بهدف الابتزاز، أو شركات خاصة لسرقة حقوق الملكية الفكرية وبراءات الاختراع، أو القطاع المالي والمصرفي بهدف الإضرار باقتصاد الدولة أو سرقة الأموال، أو خدمات حكومية، أو أجهزة أمنية بهدف سرقة معلومات استخباراتية أو خطط عسكرية أو تصميمات أسلحة، أو مؤسسات إعلامية.

ج– حسب الهدف من الهجمة:

فقد يكون الهدف "مالي" من خال اختراق الحسابات البنكية، أو هدف"عسكري"، مثل اختراق النظم العسكرية، أو هدف "سياسي" للتعبير عن الغضب من قرارات أو تصرفات سياسية، أو هدف "إنسان" للتعبير عن التعاطف مع قضية إنسانية.

د– حسب الفواعل المشاركة:

قد يقوم بهذه الهجمات "قوات مسلحة" وجيوش إلكترونية في إطار الصراعات العسكرية والسياسية بين الدول، أو"مجموعات إجرامية"وعصابات منظمة من أجل السرقة وغسيل الأموال، أو"جماعات إرهابية" كأحد أنواع ممارسة الإرهاب الإلكتروني...

2: الإرهاب السيبراني.

يعتبر الإرهاب السيبراني تهديدا واضحا للأمن القومي للدول والذي يتضح من خطورة توظيف التقنيات الذكية في تنفيذ هجمات إرهابية سيبرانية، سواء عبر الفضاء السيبراني أو استخدام الربوتات وطائرات دون طيار في شن تلك الهجمات أو استخدام الطابعات ثلاثية الأبعاد في تصنيع الأسلحة.

وكان " **باري كولين** Barry Collin" من أوائل الذين استخدموا مصطلح الإرهاب السيبراني (Cyber terrorism) في ثمانينات القرن الماضي والتي خلص فيها إلى صعوبة وضع تعريف شامل للإرهاب التكنولوجي، ولكنه تبنى تعريفاً للإرهاب السيبراني بأنه : " هجمة إلكترونية غرضها تهديد الحكومات أو العدوان عليها سعياً لتحقيق أهداف سياسية أو دينية أو أيديولوجية، وأن الهجمة يجب أن تكون ذات أثر مدمر وتخريبي مكافئ للأفعال المادية للإرهاب"[27].

فقد أضحت الأسلحة السيبرانية من أهم أدوات حروب الجيلين الرابع والخامس، وهي ليست حكرا على الدول فقط، إذ تقوم التنظيمات المتطرفة باستخدام بعض آلياتها، فهي مجرد فيروسات وبرمجيات خبيثة يتم تصميمها عبر برامج كمبيوتر، لشن هجمات إلكترونية على أهداف عسكرية أو مدنية، تؤدي إلى تدمير النظم والبرمجيات أو مكوناتها المادية أو إلحاق خلل وظيفي أو فني بها، بما قد يؤدي في النهاية إلى تدمير البنية التحتية للدول أو اختراق الأنظمة العسكرية والتجسس على الأفراد والمعلومات وأنظمة الاتصالات، وغيرها من الأعمال التخريبية التي تهدد أمن الدول[28].

ووفقاً لوزارة الدفاع الأمريكية "البنتاغون" فإنها تعرف الإرهاب الألكتروني بأنه :" عمل إجرامي يتم الإعداد له باستخدام الحاسبات ووسائل الاتصالات ينتج عنها عنف وتدمير أو بث الخوف تجاه تلقي الخدمات بما يسبب الارتباك وعدم اليقين وذلك بهدف التأثير على الحكومة أو أو السكان لكي تمتثل لأجندة سياسية أو اجتماعية أو فكرية معينة"[29]، وتتعدد استخدامات التنظيمات الإرهابية للتكنولوجيا ومخرجاتها، سواء لأغراض التجنيد والدعاية الدينية المتطرفة، أو للتمويل من مصادر خفية يصعب تعقبها، أو في صناعة الأسلحة وتنفيذ العمليات الإرهابية.

3: الحروب السيبرانية.

عرفت على أنها توظيف القدرات السيبرانية وذلك بهدف تحقيق غرض أساسي، يتمثل في تحقيق الأهداف أو الآثار العسكرية في الفضاء الإلكتروني أو من خلاله، وبالتالي يُمكن تلخيص مفهوم الحروب السيبرانية في معناها الإجرائي بأنها: هي الهجمات التي تشنها بعض الدول ويكون مسرحها هو الفضاء الإلكتروني بغرض إلحاق الضرر بالمنشآت والبنى التحتية والأهداف العسكرية للدولة التي تعرضت للهجوم، وتتميز حروب الفضاء الإلكتروني بأنها يُمكن أن تكون من فاعلين غير الدول فيكون هناك صعوبة في تحديد العدو والجهة المهاجمة[30].

وعند تعريف حروب الفضاء الإلكتروني لابد من الإشارة إلى الجهود الفكرية لعدد من المعنيين بدراسة الحروب الإلكترونية مثل "**جون أركويلا**" و"**ديفيد رون**" اللذان عرفا حروب الفضاء الإلكتروني بأنها " إجراء أو استعداد لإجراء عمليات عسكرية بالاعتماد على المبادئ والآليات المعلوماتية، ما يعني تعطيل أو تدمير نظم المعلومات والاتصالات في دولة العدو المستهدفة"، ويُمكن تعريف الحروب الإلكترونية من النظرة القانونية بأنها نظام قائم على الرعب المنتشر في الشبكة العنكبوتية تهدف إلى تنفيذ العديد من الأعمال لترويع أمن الأفراد والجماعات

والمؤسسات والدول وإرهاقهم اقتصاديا وإدخالهم في أزمات نفسية واجتماعية ناتجة عما يعرف بالإرهاب الصامت، وينطلق هذا المفهوم من الواقع الغربي، وهي حرب ناعمة صامتة تأخذ أشكالاً عدة كشكل الاتصالات بين الجيوش وقاداتها وإضعاف شبكات النقل والإمدادات اللوجستية وضرب المعلومات الاقتصادية وإحراج الساسة والعبث بالمحتوى الفني والتقني[31].

والدولة هي الفاعل الرئيسي في الحروب السيبرانية بالأساس، حيث بدأت بعض الدول الاستعداد لهذا النوع من الحروب، سواء من خال إنشاء جيوش سيبرانية داخل صفوف القوات المسلحة للدول، أو من خال إبرام الاتفاقات السياسية والعسكرية،بعدم شن أي هجمة سيبرانية، مثل الاتفاقية المبرمة بين الولايات المتحدة الأمريكية والصين في عام 2015.

مؤشرات الحروب السيبرانية:

من أمثلة حروب الفضاء الإلكتروني، ما حدث بين أمريكا وإيران سنة 2009، ولهذا طغى مفهوم الأمن السيبراني على إستراتيجية الأمن القومي الأمريكي والبريطاني منذ عام 2010. وقد تحدث الحرب السيبرانية ليس لأسباب عسكرية محضة، بل لمجرد الخلاف السياسي، أو بهدف سرقة المعلومات الإستراتيجية لمعرفة فيما يفكر العدو، والأسلحة التي يتم استخدامها في هذه الحرب متنوعة ومتعددة، منها على سبيل المثال برامج كمبيوتر تمثل فيروسات وبرمجيات خبيثة، والتي تعتبر أحد أهم عناصر إدارة الحروب السيبرانية، وتتسم الأسلحة السيبرانية بعدد من المميزات هي[32]:

- منخفضة التكاليف .
- تستهدف مرافق حيوية وحرجة للدولة
- يتم تطويرها بواسطة دول أو فواعل من دون الدول.
- تسعى إما الى التجسس وسرقة المعلومات أو للتدمير.
- هي إحدى أهم أدوات حروب الجيل الرابع.
- يصعب تعقبها.

المحور الثالث: الأمن السيبراني كضمان للأمن القومي.

إن معالجة قضايا الأمن السيبراني على مستوى العالم يحتاج إلى عمل وتعاون جماعي ودولي . ورغم الإقرار بصعوبة تحقيق مثل هذا التعاون، فإن الرغبة في حماية المصالح الخاصة، وامتلاك قدر من الثقة فيما بين الحكومات، قد يمهد لتعاون دولي يعمل على تحجيم التهديدات السيبرانية المستقبلية

أولا: مفهوم الأمن السيبراني.

إن مصطلح الأمن السيبراني أو الإلكتروني ظهر حديثاً وهو يعني مجمل القوانين السياسية، الأدوات، النصوص، المفاهيم وميكانيزمات الأمن وطرق تسيير الأخطار والممارسات التكنولوجية المتعلقة بتكنولوجيا المعلومات والاتصالات المستخدمة لحماية الدول والمنظمات والأشخاص، كما يعرف على انه الحالة المرغوب فيها لعمل أنظمة

المعلومات والاتصالات والتي تمنحها القدرة على المقاومة والتصدي لكل ما ينجم عن الفضاء السيبراني، والذي من شأنه أن يعرض المعلومات المخزنة أو المعالجة أو المنقولة للتلف أو التغيير أو التجسس.

وقدمت وزارة الدفاع الأمريكية "البنتاغون" تعريفاً دقيقاً لمصطلح (الأمن السيبراني)، إذ اعتبرت انه: "جميع الإجراءات التنظيمية اللازمة لضمان حماية المعلومات بجميع أشكالها الالكترونية والمادية من مختلف الجرائم، والهجمات، والتخريب، والتجسس، والحوادث"[33].

وبحسب التعريف المعطى له في التقرير الصادر عن "الاتحاد الدولي للاتصالات"حول" اتجاهات الإصلاح في الاتصالات للعام 2011/2010 " يعرف الأمن السيبراني على أنه : "عبارة عن مجموعة الوسائل التقنية والتنظيمية والإدارية التي يتم استخدامها لمنع الاستخدام غير المصرح به، وسوء الاستغلال، واستعادة المعلومات الإلكترونية، ونظم الاتصالات والمعلومات التي تحتويها، وذلك بهدف ضمان توافر واستمرارية عمل نظم المعلومات، وتعزيز حماية وسرية وخصوصية البيانات الشخصية، واتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين من المخاطر في الفضاء السيبراني "[34].

ويمكن تعريف الأمن السيبراني، بأنه أمن الشبكات، والأنظمة المعلوماتية، والبيانات، والمعلومات، والأجهزة المتصلة بالانترنت. وعليه فهو المجال الذي يتعلق بإجراءات، ومقاييس، ومعايير الحماية، المفروض اتخاذها،أو الالتزام بها، لمواجهة التهديدات، ومنع التعديات،أو للحد من آثارها في أقسى وأسوأ أ الأحوال، ويرتبط هذا الأمن، ارتباطا وثيقا، بأمن المعلومات. فالاعتماد على المعلومة، حقيقة لا لبس فيها، تفرض اعتمادا أكثر، على الأنظمة الالكترونية التي تعالجها [35].

ثانيا:عناصر الأمن السيبرانى.

لتحقيق الأمن السيبراني تحتاج الدولة إلى تنسيق جهودها في جميع أنحاء نظام المعلومات الخاص بها. وتشمل هذه الجهود عناصر الأمن السيبراني ما يلي:

- **أمن الشبكة:** وهي إجراءات تستخدمها الشركات والأفراد لحماية شبكة المؤسسات من الاختراق.
- **أمن التطبيقات:** وهي وضع تدابير لحماية البرامج من الفيروسات الضارة وعدم سرقة المعلومات السرية.
- **امن المعلومات:** عبارة عن الضوابط التي تضمن خصوصية المعلومات وحمايتها والوصول بسهولة لها عند الحاجة سواء نقلها أو تخزينها.
- **الأمن التشغيلي:** هي عمليات لحماية المعلومات ومعالجتها وتخزين البيانات.
- **التعافي من الكوارث:** مجموعة خطوات تستخدمها الشركات للحد من التهديدات أو فقدان المعلومات.
- **استمرارية العمل:** خطة تتبعها الشركات لمواصلة العمل أثناء خرق المعلومات رغم الموارد المتأثرة [36].

إن التحدي الأكثر صعوبة في الأمن السيبراني التطور المستمر لمخاطر الأمن نفسها باستمرار. التهديدات تتقدم وتتغير بسرعة أكبر مما تستطيع المنظمات مواجهته. لذلك ، يجب إتباع نهج أكثر إستباقية في مجال الأمن السيبراني، من خلال دراسة المخاطر المحتملة و اتخاذ إجراءات وقائية لتجنب حدوثها ، و وضع خطة للتعافي من الكوارث في حال وقوعها لتقليل الخسائر و التعافي بسرعة.

ثالثا: الأمن السيبراني و أجندات الأمن القومي غير التقليدي للدول:

و ذلك من خلال تحديث الجيوش و تدشين وحدات متخصصة في الحروب السيبرانية، و إقامة هيئات وطنية للأمن و الدفاع الالكتروني و القيام بالتدريب، و إجراء المناورات لتعزيز الدفاعات السيبرانية، و العمل على تعزيز التعاون الدولي في مجالات تأمين الفضاء السيبراني.

لقد أصبح الدفاع السيبراني لا يقل أهمية عن الدفاع العسكري التقليدي خاصة إذا علمنا أن الحرب الالكترونية تترجم الصراعات الواقعية بين مختلف الفواعل الدولية، و عليه عكفت الدول على تطوير قدراتها الالكترونية من خلال صياغة استراتيجيات سيبرانية تترجم تصور الدول لمصالحها و توجهاتها في هذا الفضاء، حيث تعمل الجيوش السيبرانية على جعل هذه الاستراتيجيات قابلة للتحقيق على غرار روسيا، الصين و الولايات المتحدة الأمريكية[37].

خاتمة :

رغم الأثر الايجابي الذي غير بها الفضاء السيبراني والثورة التكنولوجية الهائلة معالم الحياة الاجتماعية والسياسية والثقافية... للمجتمعات والدول، وتزايد منافعهما وتسهيل سير العلاقات بين الأفراد والمؤسسات، وتوجيه الدول نحو اعتماد الذكاء الاصطناعي في إدارة مختلف متطلبات الحياة اليومية بنظم الكترونية، إلا أن ذلك لا يعفي تلك النظم والدول وحتى المعلومات وخصوصية الأفراد والمؤسسات من خطر التعرض للاختراق والوصول إلى قواعد البيانات والمعلومات السرية بشكل يصبح معها نشوب الحروب السيبرانية ومخاطر الإرهاب السيبراني بعواقبها الوخيمة والحرجة خطرا شديد الاحتمال.

ولا تطال تلك التهديدات أمن معلومات الأفراد والمؤسسات فحسب، بل تهدد أيضا الأمن القومي للدول، التي يتوجب عليها اتخاذ تدابير تعاونية أكثر فعالية إزاء التهديدات السيبرانية التي تتجاوز الحدود التقليدية للأمن القومي للدول.

فالثورة التقنية والتطور التكنولوجي المتسارع وثورة المعلومات (مجتمع ما بعد المعلومات) وتجليات الفضاء السيبراني يحتم على الدول إعادة صياغة الكثير من المفاهيم كالقوة، الحرب، الصراع، الردع، باتخاذ التدابير التي تسهم في الحد من مخاطر تهديدات الفضاء السيبراني على الأمن القومي العالمي.

الهوامش:

[1] علاء عبد الحفيظ، الأمن القومي المفهوم والأبعاد، دراسات سياسية، المعهد المصري للدراسات، اسطنبول، 2020، ص1

[2] عبد الرحمان أسامة، الأمن القومي، الموسوعة السياسية، على الرابط: https://political-encyclopedia.org/dictionary ، تاريخ الزيارة في: 2022/05/22.

[3] علي سيد إسماعيل، الأمن القومي العربي، واقعه وآفاقه في ظل التحولات الاقتصادية العالمية المعاصرة، دار التعليم الجامعي، مصر، 2019، ص25.

[4] سورة قريش، الآيتان 3-4.

[5] حسن السيد حامد خطاب، تحديات الأمن الفكري في ضوء المفاهيم الإسلامية، ضمن سلسلة من قضايا الفكر المعاصر، ب د ن، 2012، ص4.

[6] علي سيد إسماعيل، مرجع سابق، ص25

[7] علاء عبد الحفيظ، مرجع سابق ص4

[8] منى الأشقر جبور، السيبرانية هاجس العصر، المركز العربي للبحوث القانونية والقضائية، جامعة الدول العربية، القاهرة، 2016، ص25.

[9] عبد الرحمان أسامة،مرجع سابق

[10] علاء عبد الحفيظ،مرجع سابق ص4.

[11] تعريف ومعنى القومية، معجم المعاني، على الرابط: https://www.almaany.com/ar/dict/ar-ar، تاريخ الزيارة في: 2022/05/15

[12] علي سيد إسماعيل، مرجع سابق، ص29

[13] جاسم محمد، الأمن القومي في ظل العولمة وتغيير ألمفاهيم، أضواء للبحوث و الدراسات، افريل 2020، على الرابط: https://adhwaa.net تاريخ الزيارة في: 2022/05/15

[14] محمد جمال مظلوم، الأمن غير التقليدي، جامعة نايف العربية للعلوم الأمنية، الرياض، 2012، ص ص 78- 82.

[15] صلاح مهدي هادي الشمري، زيد محمد علي إسماعيل، الأمن السيبراني كمرتكز جديد في الإستراتيجية العراقية، مجلة قضايا سياسية، العراق، العدد: 62 السنة الثانية عشر، 2020، ص 285.

[16] منى شلبي، الأمن السيبراني دعامة من دعائم الأمن القومي، موقع إيلاف المغرب، 12جانفي 2019، على الرابط: https://elaphmorocco.com/Web/opinion/2019/01/33433.html، تاريخ الزيارة في : 2022/07/08.

[17] المرجع نفسه.

[18] عبد المعطي زكي، الأمن القومي قراءة في المفهوم والأبعاد، المعهد المصري للدراسات السياسية والإستراتيجية، تركيا، 2016، ص3.

[19] محمد عاطف إمام إبراهيم ، الفضاء الإلكتروني وأثره على الأمن القومي للدول: الحروب الإلكترونية نموذجاً، المركز الديمقراطي العربي، 23. أبريل 2022، https://democraticac.de/?p=81775#_ftnref6، تاريخ الزيارة في:2022/07/12.

20 صفية نزاري، الامن الثقافي لمنطقة المغرب العربي في ظل تنامي العولمة: دراسة مقارنة لحالات الجزائر- تونس- المغرب، مذكرة ماجستير في العلوم السياسية، جامعة محمد خيضر بسكرة، 2011، ص47.

[21] عبد المعطي زكي، مرجع سابق، ص5.

[22] شباح فتاح ، بوصوردي صليحة، الامن الثقافي ودوره في المحافظة على الهوية الوطنية، المجلة الجزائرية للامن والتنمية، الجزائر، المجلد 10، العدد 2 ص63.

[23] منى الأشقر جبور، مرجع سابق، ص26.

[24] انظر على الرابط: https://ar.wikipedia.org/wiki ، تاريخ الزيارة في : 2022/07/07.

[25] قاسيمي صافية، الفضاء السيبراني والأغوار الالكترونية : إشكالية خلق فضاء الكتروني افتراضي حسب المنظور الهابر ماسي، مجلة الحكمة للدراسات الفلسفية، الجزائر، العدد 7، 2016، ص67.

[26] إيهاب خليفة، مجتمع ما بعد المعلومات: تأثير الثورة الصناعية الرابعة على الأمن القومي، العربي للنشر والتوزيع، القاهرة، 2019، ص ص 104-106.

[27] صلاح مهدي هادي الشمري ، مرجع سابق، ص 281.

[28] إيهاب خليفة، مرجع سابق، ص124.

[29] صلاح مهدي هادي الشمري ، مرجع سابق، ص 281.

[30] حنان دريسي، الحروب السيبرانية : تحول في أساليب القتال وثبات في المبادئ و الأهداف، مجلة الفكر القانوني والسياسي، المجلد 06، العدد 1، ص916.

[31] محمد عاطف إمام إبراهيم، مرجع سابق.

[32] إيهاب خليفة، مرجع سابق، ص ص 113- 116.

[33] خالد ظاهر المطيري، دور التشريعات الجزائية في حماية الامن السيبراني بدول مجلس التعاون الخليجي، مجلة البحوث الفقهية والقانونية، العدد38، 2022، ص996

[34] تقرير صادر عن الاتحاد الدولي للاتصالات، تابع لهيئة الامم المتحدة، عام 2010.

[35] منى الأشقر جبور،مرجع سابق، ص 25.

[36] للإطلاع أكثر انظر على الرابط: https://5aznh.com/cyber-security

[37] حنان دريسي، مرجع سابق، ص 920.

المراجع:

الكتب:

1- إيهاب خليفة، مجتمع ما بعد المعلومات: تأثير الثورة الصناعية الرابعة على الأمن القومي، العربي للنشر والتوزيع، القاهرة، 2019.

2- علي حسن السيد حامد خطاب، تحديات الأمن الفكري في ضوء المفاهيم الإسلامية، ضمن سلسلة من قضايا الفكر المعاصر، ب د ن، 2012.

3- عبد المعطي زكي، الأمن القومي قراءة في المفهوم والأبعاد، المعهد المصري للدراسات السياسية والإستراتيجية، تركيا، 2016.

4- سيد إسماعيل، الأمن القومي العربي، واقعه وآفاقه في ظل التحولات الاقتصادية العالمية المعاصرة، دار التعليم الجامعي، مصر، 2019.

5- محمد جمال مظلوم، الأمن غير التقليدي، جامعة نايف العربية للعلوم الأمنية، الرياض، 2012.

المقالات:

- حنان دريسي، الحروب السيبرانية : تحول في أساليب القتال وثبات في المبادئ و الأهداف، مجلة الفكر القانوني والسياسي، المجلد 06، العدد 1.

- شباح فتاح ، بوصوردي صليحة، الامن الثقافي ودوره في المحافظة على الهوية الوطنية، المجلة الجزائرية للامن والتنمية، الجزائر، المجلد 10، العدد 2.

- علاء عبد الحفيظ، الأمن القومي المفهوم والأبعاد، دراسات سياسية، المعهد المصري للدراسات، اسطنبول، 2020.

- قاسيمي صافية، الفضاء السيبراني والأغوار الالكترونية : إشكالية خلق فضاء الكتروني افتراضي حسب المنظور الهابر ماسي، مجلة الحكمة للدراسات الفلسفية، الجزائر، العدد 7، 2016.

- صلاح مهدي هادي الشمري، زيد محمد علي إسماعيل، الأمن السيبراني كمرتكز جديد في الإستراتيجية العراقية، مجلة قضايا سياسية، العراق، العدد: 62 السنة الثانية عشر، 2020.
- منى الأشقر جبور، السيبرانية هاجس العصر، المركز العربي للبحوث القانونية والقضائية، جامعة الدول العربية، القاهرة، 2016.

الرسائل:

صفية نزاري، الامن الثقافي لمنطقة المغرب العربي في ظل تنامي العولمة: دراسة مقارنة لحالات الجزائر- تونس- المغرب، مذكرة ماجستير في العلوم السياسية، جامعة محمد خيضر بسكرة، 2011.

مواقع الانترنت:

- عبد الرحمان أسامة، الأمن القومي، الموسوعة السياسية، على الرابط: https://political-encyclopedia.org/dictionary، تاريخ الزيارة في: 2022/05/22 .
- تعريف ومعنى القومية، معجم المعاني، على الرابط: https://www.almaany.com/ar/dict/ar-ar
- جاسم محمد، الأمن القومي في ظل العولمة وتغيير ألمفاهيم، أضواء للبحوث و الدراسات، افريل 2020، على الرابط : https://adhwaa.net
- منى شلبي، الأمن السيبراني دعامة من دعائم الأمن القومي، موقع إيلاف المغرب، 12جانفي 2019، على الرابط : https://elaphmorocco.com/Web/opinion/2019/01/33433.html
- محمد عاطف إمام إبراهيم ، الفضاء الإلكتروني وأثره على الأمن القومي للدول: الحروب الإلكترونية نموذجاً، المركز الديمقراطي العربي، 23. أبريل 2022، https://democraticac.de/?p=81775#_ftnref6
- انظر على الرابط: https://ar.wikipedia.org/wiki
- خالد ظاهر المطيري، دور التشريعات الجزائية في حماية الامن السيبراني بدول مجلس التعاون الخليجي، مجلة البحوث الفقهية والقانونية، العدد38، 2022، ص996
- تقرير صادر عن الاتحاد الدولي للاتصالات، تابع لهيئة الامم المتحدة، عام 2010.
- للإطلاع أكثر انظر على الرابط: https://5aznh.com/cyber-security