PSYCHOLOGY AND EDUCATION (2024) 61(3): 140-165
ISSN:1553-6939

CYBERSECURITY CHALLENGES OF ALGERIAN NATIONAL SECURITY AND THE ROLE OF THE LEGALSYSTEM IN CONFRONTING THEM

Dr.BENAGOUNE Aissa

University of Algiers 3 (Algeria), E-mail: aissabenagoune@gmail.com

Received: 03/2024, Published: 04/2024

Abstract:

The rapid and extensive technological development in the world of computing and the internet, unprecedented in previous decades, has led to the accumulation of vast amounts of information, files, and various topics converging through digital media and communication networks, now known as cyberspace or the informational world. This reservoir of information and secrets is stored in information storage stations, in addition to the availability of stations and centers to ensure the flow of internet service. This abundance of information has led to the exploitation of this information by what is known as information pirates (criminals) or cybercriminals, which often negatively affects the national security of countries, especially weak and developing nations.

In this regard, the article is divided into three sections, with an introduction preceding these sections and a conclusion that summarizes the presented ideas and discussions within this scientific article. This summary will also touch upon some assumptions and problematic issues that should accompany this scientific summary.

The first section is titled: "Traditional National Security and the Emergence of New Concepts," relating to the most important developments in the field of international relations and the renewal of concepts of national security according to the requirements of the modern era, up to digital security or cyber national security for each country separately.

As for the second section, it falls under the title "Cybersecurity - Information as a New Form of National Security Concept." In this section, the focus will be on defining and explaining the concept of cybersecurity or informational security as one concept. The most important definitions of this new concept will be explored, as well as the main areas targeted positively or negatively. Furthermore, the discussion will cover the main areas in which cyber breaches have increased in the current era against many national interests, providing examples of that.

The third section, titled "The Role of National Legal System in Confronting Cyber Challenges to National (Domestic) Security," will focus on the most important texts and legal regulations issued by the authorities authorized to do so to set limits or at least work on preventing cyber attacks and assaults carried out by cyber pirates, whether individuals or groups. These pirates may work independently or on behalf of official entities such as giant companies or for the benefit of great powers. Initiatives and programs to address the phenomenon of cybercrimes adopted by some countries will also be addressed, along with the most important international laws and legal regulations in the field of combating digital or cyber crimes. It should be noted that Algeria has

joined many international, regional, and local agreements in the field of combating and addressing dangers.

Keywords: Traditional national security, Cyber security, The legal system to prevent cybercrimes.

التحديات الأمنية السيبرانية على الامن القومي الجزائري
ودور المنظومة القانونية الوطنية في التصدي لهذه التحديات

د.بن عقون عيسى

جامعة الجزائر 3-(الجزائر)، الايميل: aissabenagoune@gmail.com

ملخص:

إن التطور التكنولوجي الهائل والكثيف وغير المتنظر في عالم الرقمانيات وعالم الانترنيت والذي لم يسبقه مثيل في العقود الزمنية الفارطة، أدى إلى تجميع ما لا حدود له من المعلومات والملفات والمواضيع المختلفة والتي كانت تتقاذف عبر الوسائط الإعلامية والاتصالية الرقميةوهي التي تعرف الان بعالم السيبرانية أو المعلوماتية. هذا المخزون من المعلومات والاسرار يتم تخزينه في محطات لتخزين المعلومات بالإضافة لتوفر محطات ومراكز من أجل ضمان تدفق خدمة الانترنيت. وتوفر هذا الكم من المعلومات أدى إلى ظهور إستغلال هذه المعلومات من قبل ما يعرف بالقراصنة (المجرمين) المعلوماتيين أو السيبرانيين، الأمر الذي كثيرا ما يؤثر سلبا على الامن القومي للدول، خصوصا الدول الضعيفة والسائرة في طريق النمو. وفي هذا المجال سنقسم محاور المقالة إلى ثلاثة محاور بالإضافة إلى مقدمة تسبق هذه المحاور الثلاث وخاتمة تكون عصارة لما سوف يتم إستنتاجه من عرض ما يحب عرضه والتطرق إليه ضمن أفكار هذه المقالة العلمية والتي لن تخلو من الإشارة إلى بعض الفرضيات والإشكالية الواجب مرافقتها لهذا الملخص العلمي.وأول هذه المحاور تحت عنوان: الأمن القومي التقليدي وظهور مفاهيم جديدة، تتعلق بأهم التطورات الحاصلة في ميدان العلاقات الدولية وتجديد مفاهيم الامن القومي حسب متطلبات العصر الحديث إلى غاية الأمن الرقمي أو الامن القومي السيبراني لكل دولة على حدي. أما المحور الثاني: فجاء تحت عنوان: الأمن السيبراني – المعلوماتي كصورة جديدة لمفهوم الأمن القومي. وفي هذا المحور سيتم البحث في تحديد وتعريف مفهوم الامن السيبراني أو المعلوماتي على حد سواء باعتبارهما مفهوما واحدا،وأين سيتم التطرف إلى أهم التعاريف لهذا المفهوم الجديد وكذا أهم المجالات التي يستهدفها إيجابا أو سلبا،وكذا الحديث عن أهم المجالات التي كثر فيها في العصر الحالي إحداث اختراقات سيبرانية ضد الكثير من مصالح الدول وإعطاء أمثلة على ذلك.كما سيتم التطرق في المحور الثالث المعنون ب: دور المنظومة القانونية الوطنية في التصدي للتحديات السيبرانية على الامن القومي (الوطني)،وفيه سيتم التركيز على أهم النصوص والتشريعات القانونية الصادرة عن السلطات المخولة لذلك من أجل وضع حد أو على الأقل العمل على الوقاية من الهجمات والاعتداءات السيبرانية التي ينفذها القراصنة السيبرانيين سواء كانوا أفرادا أو جماعات، قراصنة يعملون لحسابهم الخاص أم لحساب جهات رسمية كالشركات العملاقة أو لصالح القوي العظمى. كما سوف يتم التطرق إلى بعض المبادرات وبرامج التصدي لظاهرة الجرائم السيبرانية المتخذة من قبل بعض الدول كما سيتم التطرق إلى أهم القوانين والتشريعات القانونية الدولية في مجال مكافحة الجرائم الرقمية أو السيبرانية كما

ذكرنا أنفا. كما أننا لن ننس التذكير بانضمام الجزائر إلى العديد من الاتفاقيات الدولية والاقليمية والجهوية في مجال المحاربة والتصدي للأخطار والهجمات والجرائم المعلوماتية – السيبرانية – الرقمية.

الكلمات المفتاحية: الامن القومي التقليدي، الأمن السيبراني، المنظومة القانونية وقاية الجرائم السيبرانية.

مقدمة:

لقد عرفت البشرية منذ وطئت أقدامها هذا الكون التواصل بين أفرادها و عبر مراحل مختلفة بطرق شتى , فأول ما كان بينها من طرق التواصل هو ما نزل به سيدنا أدم و حواء من علم بالأشياء من السماء إلى الأرض التي منها إنتشر ذريتهما . و مع مرور القرون و السنون لإثبات الخلافة في الأرض و هجرة البشر من مكان و من بلد إلى أخر ظهرت اللغات و الالسن المختلفة , و ظهرت الانانية و حب الذات في البشر , و هو ما أدى إلى الكثير من النزاعات و الصراعات و الحروب بين بني البشر , و ظهرت المصلحة و تجسدت في تشبث الانسان بالحيز المكاني و الزماني الذي وجد فيه . ومن بعض الأبناء لسيدنا ادم على تكوين مجموعات بشرية إلى تكوين وإنشاء قرى ومدن للإستقرارمن أجل العيش ومن أجل تحمل الصعاب والظروف المحيطة بالكائن البشري إلى تكوين ممالك ودول وإمبراطوريات حضارات عظيمة عرفها التاريخ وشهدت عليها الاثار المتبقية شاهدة على قوة وبطش هذه الامبراطوريات، و التي تجسدت في حضارات كبيرة و غنية بما تركته من شواهد و أثار مثل الحضارة البابلية والاشورية والكلدانية والفرعونية واليونانية والرومانية والفارسية والنوميدية (الشرقية و الغربية) العاترية و حضارة الانكا في أمريكا اللاتينية و الحضارات الشرقية في أسيا كالحضارة الصينية و الكورية و غيرها .هذه الحضارات لم تبنى على فراغ بل كانت قائمة على مناهج و قوانين و أنظمة سياسية و عسكرية و إقتصادية و دينية و إجتماعية و ثقافية .... . وللحفاظ على إستمرارها وتوهج شعلتها كانت تحافظ بكل الوسائل على أمنها من خلال مفهوم الامن التقليدي حينها وهو الحصول على جيش قوي له كل الإمكانيات والوسائل التي من خلالها يضمن الدفاع عن كيان تلك الممالك أو الدول أو الامبراطوريات التي أشرنا إليها فيما سبق من كلمات .و قد سارت الأمور على هذا المنوال لقرون عديدة , إلى غاية القرون الثلاث الماضية: الثامن عشر و التاسع عشر و القرن العشرين أين بدأ عصر الدول الوطنية و المناداة بإحترام الحدود , و ظهر مفهوم العلاقات الدولية و بداية تشكل نوع من الهيئات الدولية التي تحظى بنوع من القيادة الجماعية الدولية . والاتصال كله يتم بين الأطراف الدولية على الشاكلة الديبلوماسية والاتصال المباشر. هذا مع التذكير بالأنانية وحب التوسع على حساب الاخرين والذي كان نتيجته حروب مدمرة كثيرة أبرزها حربين عالميتين (1914–1919 و 1939–1945). هذا وكان الهدف الأساسي من هذه الحروب هو المحافظة على تقوية الجيوش الوطنية ودعم هذه الجيوش بوسائل الحرب التي بدأت في التطور، وإنتقلت من السيوف والخيول والبارود التقليدي إلى البنادق والرشاشات وعلى الطائرات والمقنبلات والسفن الحربية، وكل ذلك بدعم معلوماتي استخباراتي ولو تقليدي، الذي كثيرا ما كان يأتي بنتائج وتحقيق إنتصارات جمة. لكن مع إنتهاء أخر حرب عالمية والتي هي الثانية لم تتوقف القوى الكبرى خصوصا الولايات المتحدة الامريكية والاتحاد السوفياتي من إنتاج أسلحة دمار فتاكة ومدمرة للبشرية ألا وهي أسلحة الدمار الشامل المتمثلة فبي الأسلحة النووية. لكن هذه المنظومات المتطورة من الأسلحة واكبها أيضا تطورا كبيرا في الجانب التكنولوجي و الذي كان في الأساس الأول هذ خدمة الترسانة العسكرية الرهيبة , لكن تفطن المؤسسات و المركبات العسكرية الكبرى في صناعة الأسلحة و نظرت بعين إقتصادية و عين الربح المالي و تكوين ثروات مالية رهيب و خصوصا مركبات السلاح الامريكية و الغربية بإعتبارها

مجمعات و مركبات رأسمالية و إتجهت صوب القطاعات و المجالات المدنية و هنا حدثت الطفرة التكنولوجية و العلمية الرهيبة و ظهر ما يسمى الان بعالم الرقمانيات و العالم الافتراضي و السيبراني التي طفحت فيه المعلومات و البرامج الرقمية الالكترونية , غير أن هذا التطور الكبير لم يكن ليحدث لولا التطور العظيم في إنتاج الوسائل المادية المتمثلة في الحواسيب و الحواسيب الكبيرة القادرة على تخزين كم هائل لا حصر له من المعلومات . وحتى التطور في هذا الجانب لم يكن ذا معنى لو لم يتم غزو الفضاء وبناء محطات الأقمار الصناعية ومحطات بث الانترنيت عبر هذه المحطات والأقمار. إذا فلولا هذا التزاوج بين الوسائل المادية (الحواسيب والوسائل التقنية مع غزارة الانترنيت) لما حدث هذا الانفجار العظيم في مجال الاتصال السيبراني – الفضائي –. هذا المجال ومع إيجابيات الكثيرة للبشرية إلى إنه يحمل أيضا في طياته الكثير من السلبيات للمؤسسات والأشخاص وذلك بعد ما ظهر هنالك مجرمين سيبرانيين – معلوماتيين على شاكلة المجرمين في عالم الاعمال والمال والقانون العام، وذلك باعتبار ما يتم جنيه من فوائد مالية ومصالح معلوماتية لصالح هؤلاء المجرمين السيبرانيين والذين يعمل بعضهم لأطراف خاصة وأخرين يعملون لحساب مؤسسات عالمية ودول كبرى. وهو الامر الذي تفطنت له معظم الدول في العالم وقامت بسن قوانين تجرم الجريمة المعلوماتية وتعاقب هؤلاء المجرمين السيبرانيين الرقميين وتشدد في عقوبتهم ومن ضمن هذه الدول نجد الجزائر التي واكبت التطور في الميدان الرقمي وسنت قوانين صارمة من اجل مجابهة ومكافحة التعرض للمصالح الحيوية العمومية الوطنية والخاصة على السواء.

وإذا كان موضع مقالتنا العلمية هذا افردنا له ثلاثة محاور، فقد خصصنا المحور الأول للحديث عن الامن القومي التقليدي وظهور مفاهيم أمنية جديدة. أما المحور الثاني فكان بحثنا قد تركز على الامن السيبراني – المعلوماتي – كصورة جديدة لمفهوم الامن القومي. أما المحور الثالث فقد تناولنا فيه: دور المنظومة القانونية الوطنية في التصدي للتحديات السيبرانية على الامن القومي (الوطني). وهذا ما يجرنا إلى تحديد سؤال إشكالية مقالتنا والتي سوف على النحو الاتي:إلى أي مدى يمكن للتحديات السيبرانية أن تمس بالأمن القومي الجزائري، وما مدى نجاعة المنظومة القانونية الوطنية في التصدي لهذا التحديات؟.

المحور الأول: الامن القومي التقليدي وظهور مفاهيم أمنية جديدة:

– لقد واكب التطور الهائل في ميدان التكنولوجيا والمعلوماتية، تطورا كبيرا واتساعا خطيرا في مجال الجريمة المعلوماتية، وهو الأمر الذي أدى الى تكاثف الجهود الدولية والوطنية لإيجاد وسن قوانين وتشريعات قانونية تقف في وجه الجريمة المعلوماتية الأخذة في الاتساع مع مراعاة عملية الجهود المبذولة بالتوازي مع الحفاظ على حرية الإنسان وحقوقه الأساسية التي ينص عليها الإعلان العالمي لحقوق الإنسان وكذا الدساتير الوطنية الضامنة لتلك الحقوق. غير أن هذه الحقوق يمكن للقراصنة والمجرمين المعلومتين التعرض لها، وفي شتى المجالات سواء المالية أو المهنية أو العائلية أو الشخصية، بحيث تكون هذه المعلومات مخزنة في بنوك المعلومات، التي يمكن للمجرمين المعلوماتيين الوصول إليها من خلال حذفها أو تغيرها، أو تعديلها أو تخريبها وقد يكون المساس بالأنظمة المعلوماتية أو الأجهزة (الحواسيب), وذلك من أجل ارتكاب جرائم " خطيرة أو التخطيط لها مثل النصب والاحتيال وانتحال الصفة والتجسس وغسيل الأموال وتزوير بطاقات الائتمان وتسويق المواقع الإباحية والدعارة والقذف والتشهير ." (زيبحة زيدان 2011)

إن الأمن بمفهومه العام، متشعب ومتعدد وشامل المفاهيم. ويكاد يكون مفهوما مطاطيا وغير محصور في زاوية من الزوايا، منذ أن عرفت البشرية شكل التجمعات الإنسانية والبشرية، وقيام المدن والدول والممالك والإمبراطوريات، وقيام معنى ومفهوم المصلحة الخاصة لكل شعب من الشعوب والوحدات السياسية المختلفة باختلاف الأزمنة والمناطق الجغرافية، حيث كان دائما لمفهوم الأمن تعريفات بعضها محدد وبعضها يتعلق بزاوية من الزوايا فقط فالمفهوم التقليدي، كان يشير في الغالب إلى مسالة البقاء والحفاظ على النسل البشري، ومن ذلك العيش في آمان واستقرار، و ضمان الانتقاء الذاتي من القوت والغذاء، وهو ما يتوافق والآيتين الكريمتين من سورة قريش : " وَإِذْ قَالَ إِبْرَاهِيمُ رَبِّ اجْعَلْ هَذَا بَلَدًا آمِنًا وَارْزُقْ أَهْلَهُ مِنَ الثَّمَرَاتِ مَنْ آمَنَ مِنْهُمْ بِاللَّهِ وَالْيَوْمِ الآخِرِ قَالَ وَمَنْ كَفَرَ فَأُمَتِّعُهُ قَلِيلاً ثُمَّ أَضْطَرُّهُ إِلَى عَذَابِ النَّارِ وَبِئْسَ الْمَصِيرِ"، سورة البقرة , الاية:126.

ومعنى ذلك ضمان " الشعور بالطمأنينة والاستقرار والقدرة على تأمين وإشباع الحاجات الأساسية والدوافع العضوية والنفسية". (أحريق عبد الله 2022)

أما ما يتعلق بمعنى الأمن لغة، ضمن ما يمكن الاشارة إليه خلال الألفاظ في الانجليزية Security أو الفرنسية Sécurité ضمن اللغتين هو ضمان الأمن والأساس بالطمأنينة وعدم الإحساس بالخوف والاضطراب والهوس الدائم أو المؤقت من إمكانية حدوث شيء معين يمكن أن يعكر صنوف السلم, والسلام والهناء والطمأنينة في أية لحظة من اللحظات، ويمكن إضافة بعض التعريفات التي تبرز المفهوم التقليدي للأمن ومنها:تعريف روبارتماكنمارا(Robert Mc Namara) وزير الدفاع الأمريكي السابق الذي يقول: " إن الأمن يعني التطور والتنمية، سواء منها التنمية الاقتصادية أم الاجتماعية، ثم السياسية في ظل حماية مضمونة" (عبد الوهاب جعيجع 2017)

وأما لورنس كروز وجوزيف ناي(Lawrence kranse و Nye). فيؤكدان أن " الأمن هو غياب التهديد بالحرمان الشديد من الرفاهية". (عبد الوهاب جعيجع 2017)

ومدلول مصطلح القومية: في اللغة فإنه يمكن إيضاح ذلك من خلال التمعن في كلمة قومية والتي تعني قوم من الناس أو البشر أو الأفراد، فالمقصود بالقوم: فهي الكلمة المشكلة من ثلاث حروف (ق. و. م) والفعل الحاضر قام، يقوم ومعناها أخذ حيز من المكان الذي يقف أو يجلس أو يسامر أو يتفرج فيه أو منه مجموعة من الناس على شيء أو يستمعون إلى شيء سواء كلام أو توجيه او توبيخ أو إعلام، وما إلى ذلك.

ويمكن الايضاح أكثر معنى "القومي" اصطلاحا بكونه " 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 بان لها هوية خاصة تميزها عن " أقوام" أخرى مختلفة عنها في كل –أو بعض – هذه السمات. (مسيكة محمد 2022)

كما يمكن الإشارة أيضا من حيث الاصطلاح ان معني الامن القومي هو مصطلح يجمع بين الرجال والنساء (الذكور والإناث) مثل قوله تعالى " ويا قومي ما لي أدعوكم إلى النجاة وتدعونني إلى النار" سورة غافر الآية: 41 وهنا إشارة إلى مجموعة من الناس وإلى معشر من الحضور.

أما من حيث الاصطلاح العام، فمفهوم الأمن،هو ما يقصد به، السلام والطمأنينة وديمومة مظاهر الحياة واستمرار مقوماتها وشروطها، بعيدا عن عوامل التهديد ومصادر الخطر وأما المستخلص من ذلك، فهو أن تضمن الدولة بمفهومها الحديث استقرار وسلامة أرضيها، وكذلك سلامة أنظمتها السياسية والاقتصادية، والاجتماعية، والثقافية.

وفي هذا الإطار يمكن إفراد بعض التعريفات الخاصة بمفهوم الأمن العام، ومنها على سبيل المثال:

أن " الأمن هو قدرة المجتمع على مواجهة الأحداث والوقائع الفردية للعنف، وجميع المظاهر المتعلقة بالطبيعة الحركية للعنف". (عبد الوهاب جعيجع 2017)

ومفهوم الأمن ليس وليد العصر والحديث وإنما هو مفهوم تطور البشرية والرغبة فيالبقاء، ولقد عرف المفهوم التقليدي للأمن بضرورة توفير شروط القوة والبأس لضمان استمرار وجود الأمم و الدول والإمبراطوريات وإلا كان مصير ها الفناء والاضمحلال والسقوط، وهو شأن كل الأمم السابقة , مثل قصة ذو القرنين مع يأجوج ومأجوج، و قصة النبي داوود مع بني إسرائيل، وصراع داوود مع جالوت، وقول بني إسرائيل لسيدنا موسى عليه السلام اذهب أنت وربك فقاتلا إنا هاهنا قاعدون"الآية . " فهزموهم بإذن الله، وقتل داوود جالوت وأتاه الله الحكمةوعلمه مما شاء ولولا دفع الله الناس بعضهم ببعض لفسدت الأرض ولكن الله ذو فضل على العالمين". سورة البقرة، الآية 251.وفي سورةالمائدة،الآية: 24 " قالوا يا موسى، إنا لن ندخلها أبدا ما داموا فيها، فاذهب أنت وربك فقاتلا، إنا هاهنا قاعدون".

كماأن مفهوم إكتساب القوة ووسائل الردع في العصور الحديثة يمكن أن يتضح من أفكار"مكيافيلي" القائلة:" على الحاكم أن يتبع كل السبل، ويستخدم كل الوسائل لضمان أمن نظامه ودولته، كما أسس أيضا: توماس هوبز" Thomas Hobbs " فكره على: فرضية أن الإنسان شرير بطبيعته، ولابد من وجود سلطة تضبط طبيعته وتتحكم فيها." (عامر مصباح2011)

أما أهم التطورات الحاصلة على المفهوم التقليدي للأمن: فللأمن التقليدي مفهوما يمكن الإشارة إليه أو التركيز عليه من خلال الجوانب العسكرية ,غير أن توسع البشرية وحاجياتها لبعضها البعض والتداخلات التي حصلت بين الشعوب، من حيث العلاقات التي تنشب أيام السلم كالتجارة البينية عن طريق قوافل التجار أو البعثات العلمية والودية، وكذا تعيين السفراء لدى بلدان الممالك والإمبراطوريات فيما بينها، أو تلك العلاقات التي تنشب إثر حدوث حروب بين هذه الوحدات السياسية التي أشرنا إليها سابقا، (المدن، الممالك، الإمبراطوريات). من خلال الحروب أو الغزو، والتوسع على حساب بعضها البعض، أفرز واقعا ووقائع عديدة، تمثلت في انتقال مفهوم الأمن التقليدي إلى مفاهيم وأبعاد جديدة، فمنها الجديد، ومنها الأبعاد التقليدية والمتجددة في نفس الوقت ومن ذلكالمفهوم (البعد) العسكري والسياسي. ورغم أن هذين البعدين قديمين من حيث الوجود، غير أنهما طرأت عليهما تصورات جديدة من حيث المفهوم أو الحيز، وخصوصا لما عرفا هذين المجالين طفرة كبيرة في جانب التكنولوجيا والعلم المحيط بهما.

أما باقي الأبعاد أو المفاهيم الجديدة للأمن فيمكن الإشارة لها دون إمكانية تحديدها، ومنها:البعد الاقتصادي، البعد التكنولوجي، البعد البيئي والمناخ، بعد التدخل الأمني الإنساني لإنقاذ الأقليات البشرية، البعدالطاقوي، البعد الثقافي والأيديولوجي، البعد المدني والإثني والمجتمعي .

وضمن هذه المفاهيم وتحديدها. يمكن الإشارة إلى التفسير الذي أعطته"مدرسة كوبنهاغن"لمفهوم الأمن الجديد، وعلى رأسها المفكر والمنظر باري بوزان Barry Buzan، أين تتحدث عن توسيع مفهوم الأمن الذي أصبح يتضمن قطاعات خارج القطاع العسكري، وتعديد مستويات التحليل فيه، من حيث ربط الحديث عن الأمن بالحديث عن كل القطاعات وعلى كل المستويات المرتبطة بوجود تهديد ما بها (احريق عبد الله 2022).

وهي نفس الفكرة التي يؤيدها بالكامل تقريبا. ولتر لبيان (Waltarlippmann) من خلال القول: " تكون الدولة آمنة إلى الدرجة التي لا تكون فيها معرضة لخطر التضحية بالقيم الأساسية إذا كانت ترغب في تجنب الحرب، وهي قادرة، إذا واجهت التحدي، على المحافظة عليها بالانتصار في هذه الحرب." (جعيجع 2017)

ويمكن ربط حزمة من المفاهيم او الأبعاد الامنية التقليدية بالجديدة، مع مستويات الأمن الحديثة والتي قامالمنظرون والمفكرون في حقل العلاقات الدولية بالإشارة إليها، والتي تتمثل في المستوى الفردي والذي يشمل كل متطلبات الفرد من أمن وغذاء ورفاهية وضمان مستقبله وعائلته الصغيرة المتعلقة بالمسكن والعمل والعيش الكريم. أما المستوى الثاني، فهو مستوى الدولة، والذي يتمثل في ضمان استقرار أمن الدولة، من حيث الحفاظ على حدودها وعلى سيادتها وعلى أمن وسلامة مواطنيها دون تعرض هذه الشروط إلى أي تهديدات من قبل الفواعل الخارجية أو حتى الداخلية لممارسة الدولة لسيادتها على كل أراضيها وما شملت أما المستوى الرابع، فهو المتمثل في المستوى الإقليمي والجهوي والخاص بمحيط الدولة وما يترتب على ذلك من علاقات دولية جوارية، أين تسهر الدولة على الحفاظ على تلك العلاقات المختلفة الجوانب سياسيا، اقتصاديا، تجاريا و الحفاظ على سلامة رعايا الدول المتجاورة ليسلك جيرانها نفس المعاملات الايجابية مع جاليتها ومواطنيها المتواجدين على أراضي تلك الدول وقد تلجأ الدول في الغالب إلى عقد اتفاقيات وتحالفات مع محيطها وفي شتى المجالات، راغبة في ذلك تقوية نفسها بالانضمام إلى الجماعة الإقليمية وزيادة قوتها لمجابهة القوى الخارجية والأجنبية عن تلك التحالفات العسكرية. والسياسة وكذا الاتفاقيات الاقتصادية والثقافية والتجارية، لزيادة حجم التبادلات البينية بين الأعضاء المؤسسين والمنظمين والشركاء في مثل ما أشرنا إليه من التحالفات والاتفاقيات الإقليمية والجهوية أما المستوى الرابع، فهو المتمثل، في المستوى الدولي للأمن، وهو المتمثل في ذلك الفضاء الأوسع والاشمل، والذي يتعلق بتلك المؤسسات والمنظمات الدولية التابعة للأمم المتحدة أو المنظمات غير الحكومية وكذا الشركات العابرة للقارات، أو ما يطلق عليها بالشركات والمؤسسات فوق الوطنية" supranationales ", وهو مفهوم أو واقع ملازم للطالب بالعولمة التي نعيش مظاهرها وإفرازاتها في الوقت الحالي. و"لتحقيق الأمن على هذا المستوى يجب انتهاج آليات عمل جماعية ومنهاّ : نظام توازن القوى ونظام الأمن الجماعي (عبد الوهاب جعيجع 2017).

وللتأكيد على دور الفاعلين المعاصرين على شاكلة الفاعلين السيبرانيين – المعلوماتيين – والذين غيروا من المعادلات الكثيرة التي كانت تؤكد وتثبت مسؤولية الدول بشكل كبير في غدارة دواليب الحكم والتسيير في محيط سيادتها وذلك إلى غاية نهاية الحرب الباردة.وإذا كان سابقا إلى غاية تفكك الاتحاد السوفياتي،وظهور الولايات المتحدة الامريكية بمظهر الدركي الوحيد في العالم الذي يسيطر ويهيمن على كل النزاعات والقضايا الدولية في هذا الكون،وذلك من خلال قوة أمريكا العسكرية والسياسية والاقتصادية والعلمية والثقافية ...،وكذا من خلال شركاتها العابرة للقارات، هي ما كان يعطي تلك الصورة النمطية التقليدية لمفهوم الدولة وممارسة لوظائفها التقليدية، على النحو الذي صورها به "توماس هوبز " حين رأها "الليفياثان العظيم" الذي سينهي حالة حرب الكل ضد الكل.وكما لم تعد الدول كما تصورها كينيث والتز بالمحتكر الوحيد للقوة ".(إيمان رجب2013)

و إضافة لبعض الشروحات و التفسيرات و إيضاحات لمفهوم الامن السيبراني : فإنه يمكن التطرق لهذا المفهوم من خلال الاتي: أي أن مفهوم الفضاء السيبراني من حيث أن صوره وأنماطه تطورت بشكل كبير وأصبحت أوسع من ذلك المفهوم التقليدي للأمن والمتمثل في الهاجس الناتج عن الثورة المعلوماتية الكبيرة، من حيث أن الامن القومي (الوطني) لم يعد ذلك الأمن التقليدي بمفهومه الضيق الذي ينحصر في الجانب العسكري ومجال الدفاع الوطني، وأصبحنا أمام انتقال – كبير – ينسحب و ينطبق

على مجال التهديدات الأمنية التي إنتقلت هي الأخرى إلى تهديدات غير تقليدية نتيجة الاستخدامات المتنوعة للثورة التكنولوجية والاتصالات وهو ما أوضح وأكد بأن مفهوم الامن السيبراني هو أحد العناصر الضامنة للأمن القومي للدولة". (عبد الوهاب جعيجع 2017)

و مما يمكن الاستشهاد به في تقليص دور الدولة التقليدي , هو تطور الاعلام العابر للحدود و تأثيره على سلطة الدولة المركزية و و خصوصا لما أصبح هذا الاعلام يبث عبر وسيلتين كلتاهما مهمة و جديرة بالملاحظة و كلتاهما اصبحتا عابرة للحدود و خارج رقابة الدولة , وهي المتمثلة في : " تعاظم ظهور الفضائيات الإعلامية التي تتخطى حدود الدولة . وتمتد تأثيراتها إلى الداخل المحلي و تؤثر فيه دونما إمكانية الحد منه من طرف الدولة المستقبلة، بالإضافة إلى المساحة الكبيرة التي أصبح يمتلكها الفضاء الالكتروني، و قدرته على تشكيل شبكة من التحالفات في العالم الافتراضي عبر شبكات التواصل الاجتماعي , مثل الفيس بوك و تويتر , تكون لها إنعكاسات على أرض الواقع ". (محمد بسيوني عبد الحليم 2013)

ويعتبر عنصر الفضائيات الإعلامية و عالم الفضاء الالكتروني شيئان مكملان لبعضهما البعض من حيث إستخدام أحدهما للأخر' فالفضائيات تستخدم الفضاء لبث برامجها و محتوياتها , كما تستغل شبكات التواصل الاجتماعي –الافتراضي– و تنشأ به صفحات خاصة لها , تقوم من خلالها ببث محتوياتها و الاشهار لنفسها , كما يقوم عنصر الفضاء الالكتروني بالاستفادة مما تقدمه هذه الفضائيات الإعلامية من إشهار ة تأكيد الحاجة لهذا الفضاء الالكتروني وعدم إمكانية الاستغناء عنه .

غير أن الفضاء السيبراني أو الالكتروني، يمكن أن يؤدي إلى فوضى إفتراضية قد تسبب أثار سلبية ضد الدول غير المتحكمة وغير القادرة على مراقبة و توجيه و تسيير الفضاء السيبراني الموجه لشعبها و مواطنيها , و خصوصا إذا لم تستطع الدولة المركزية إنشاء ضوابط و حواجز سيبرانية و قانونية للتصدي لموجات البرامج و المحتويات التي تدخل حدود الدولة المعنية , و ذلك نظرا للأسباب الأتية : (محمد بسيوني عبد الحليم2013)

وذلك نظرا لعدم إكتساب القدرة على معرفة هويات الفاعلين الافتراضيين الذين يقومون بإنتاج محتويات سيبرانية ويقومون بتوجيهها إلى دولة أو مجتمع ما. 2–كذلك يمكن للكم الهائل و الكبير من المعلومات التي تسوق و توجه لمجتمع أو دولة ما , أن يكون في الأصل غير صحيح و من ذلك يصعب التحقق من صحته و مصداقيته.3– فتقاد سلطة اعلى تقوم بضبط و معاقبة الفاعلين المخالفين للنصوص و التشريعات القانونية المحلية إذا ما أخلوا بها , و حتى و إن كانت الكثير من الدول الأن قد أصدرت قوانين و نصوص تشريعية لتنظيم هذا الفضاء السيبراني إلا أنه في الكثير من الأحيان تعجز هذه الدول من إكتشاف الهويات الحقيقية للفاعلين الناشطين في هذا الفضاء الالكتروني – السيبراني – و من ذلك يتنصلون من مسؤولياتهم تجاه الخروقات التي يكونون قد إقترفوها في حق الدولة المعتدى عليها سيبرانيا .4– كذلك فإن غياب المساحات المحددة و المسموحة في مجتمع الإعلام المجتمعي و الإفتراضي , قد ينتج عنه تهديد ا كبيرا للأمن المجتمعي و الأمن القومي – الوطني – , و ذلك إذا ما حدث و إن تم تسريب معلومات في خانة السرية و الخطورة لدولة ما , و كان العائق في تتبع تلك المعلومات السرية هو عدم إمكانية التعرف على هوية الفاعلين و المسربين لتلك المعلومات .5–كذلك فإن مجالات أو نطاقات المحيط الإفتراضي و من خلال الحرية الكبيرة التي نتمتع بها , و غياب المراقبة و السلطة عليها في غالب الأحيان يجعل من كل مواطن سيد نطاقه و هو الصاحب و الفاعل الأصلي في منصبه , و هذا الأمر يقضي على فكرة المصداقية الإعلامية و كذا يضفي نوعا منالغموض على الهدف أو الرسالة الموجهة من خلال نصة إفتراضية معينة .6–أم العنصر السادس فيمكن الإشارة إليه من خلال تلك الترسانة من الأدوات و

الوسائل التي تستخدم في عالم الفضاء السيبراني و منه في عالم الإعلام و الاتصال , أين أصبح من الممكن جدا أن يقم شخص معين التأثر من خلال شبكة الفايس بوك او تويتر , او اليوتوب على شريحة عريضة من المواطنين و الجمهور , ويقوم بتوجيههم عنفيا و عدوانيا , ضد أنظمتهم السياسية , و هو ما يؤدي إلى خطر إنفجار دول و مجتمعات بكاملها , وهنا يكون الإعلام الإفتراضي قد أثر سلبا على مصداقية و ثقة الإعلام التقليدي الذي لديه ضوابط و له هوية , يمكن ملامستها و تقييمها سلبا أو إيجابا .و في نفس الاتجاه ينقل الكاتب الفرنس : إريك ميشلونEric Mechoulan عن الكاتب العربي وائل غنيم قوله بمناسبة الثورات العربية ؟؟؟ (الانتفاضات وفي بعض الأحيان الفوضى العربية في سنوات: 2011–2012): " إذا أردت أن تحرر مجتمعا فأمنحه الانترنيت" وهو الأمر نفسه الذي ذهب إليه مستشار كاتبة الدولة الامريكية السابقة للخارجية: هيلاري كلنتونللإبتكار, عندما صرح قائلا : أن الأنترنيت هو تشي غيفارا القرن الواحد و العشرون. (Eric Mechoulan)

وإذا ربطنا مفهوم الأمن السيبراني في حلقة متشابكة ومتضامنة مع مفهوم الامن القومي، فإن المفهومين يشكلان دعامة أساسية للاستقرار القومي والحفاظ على مقوماته وفي مجالاته المختلفة، وخصوصا إذ أتضح مفهوم الامن القومي باعتباره، المحدد الرئيسي لصلابة المجتمع والدولة والمجتمع على السواء، من حيث أن هذه المفاهيم المختلفة، تنصهر في مفهوم كبير وأوسع ألا وهو مفهوم الأمن القومي، والذي ظهر جليا بعد مؤتمر"وستفاليا 1648", الذي نظم شؤون الأمن والدول والعلاقات الدولية على السواء في أوروبا ثم خارج أوروبا، ضمن مستعمراتها السابقة والتي قسمتها أوروبا حسب نفوذها في مؤتمر برلين 1884. فهذه المؤتمرات التي عرفت حقبة مهمة من تاريخ العلاقات الدولية، والتي على إثرها رسمت حدود وخطوط التماس والمصلحة بين الدول الأوروبية الاستعمارية على الخصوص، والتي من خلالها ظهرت مفاهيم ومصطلحات سياسية أكثر دقة، خصوصا بعدما عرفت أوروبا تصادمات عسكرية قوية منها الحربين العالميتين الأولى والثانية. (1914 – 1919) و(1939 – 1945)، أين خرجت منها أوروبا خاصة ما كان يعرف سابقا بأوروبا الغربية منتصرة، رغم ما عرفته أوروباالعجوز من دمار وخراب في الحربين العالميتين المشار إليهما سابقا.

بالإضافة إلى ما أشير إليه من شرح وإعطاء تفسير لمفهوم الفضاء السيبراني ما عرف بالإشارة إلى أن أصل الكلمة هو اشتقاق للكلمة اليونانية القديمة (Kybernetes) والتي تعني " مساعد التوجيه" أو " الحاكم" أو " الرائد" أو " الدفة"، وكذا ما أشير إلى أن أول مستخدم للمصطلح الالكتروني نجده: " ويليام غيبسون(William Gibson ، مسيكة محمد 2022)

وهو المفهوم الذي يقوم بتوسيعه: " فريديريك مايور" من حيث أن الفضاء السيبراني هو ثورة حديثة في عالم المعلومات والشبكات والوسائل المادية المتمثلة في الحاسوب أو الحواسيب، وهو كل متواصل من المعلومات والتطبيقات والبرمجيات متصلة بالأنترنيت والكوابل (الألياف) الناقلة والمحولة لهذا الكم من العلم والثقافة والمخزون السري من الأسرار والقيم والهويات وغيرها و يمكن أن نستشف و نستنتج أصناف و أنواع من هذه الاعتداءات و الجرائم السيبرانية – المعلوماتية – يمكن الإشارة إلى بعضها مع أن أنواعها كثيرة و متطورة و متسارعة في الخطورة كتسارع التطور التكنولوجي الحديث و منها : واقع الجرائم السيبرانية – المعلومات – وصورها:Cyber Attacks, الهجمات السيبرانية – أو –الحروب السيبرانية Cyber Warfare,أنماط هذه الهجمات: (هجمات التصيد –Phishing، هجمات وقف الخدمة DDOS,و كذا الأبواب الخلفية: Backdoors. (مسيكة محمد 2022)

المحور الثاني: الامن السيبراني – المعلوماتي–كصورة جديدة لمفهوم الامن القومي:

لإعطاء تعريف دقيق و ملم للأمن السيبراني فإنه يجدر بنا القول بأنه ذلك العلم أو التخصص أو المجال الذي يبحث في كنه النظريات والاستراتيجيات والسياسات التي تعمل على توفير الأدوات اللازمة لحماية المعلومات المتدافعة في أجهزة الكمبيوتر عن طريق الانترنيت، والتي قد تتعرض، بل تتعرض دوما لمجموعة من الأخطار و التهديدات والتي يكون مصدرها الهاكرز – (المجرم المعلوماتي)– ومن ناحية أخرى يمكن تحديد كيفية حماية المعلومات المخزنة في الأجهزة المعلوماتية، إن على المستوى التكنولوجي أو عن طريق " مجموعة الوسائل والأدوات والإجراءات التقنية المطلوبة كحماية المعلومات وسلامتها، ومن الناحية القانونية، هي التدابير والإجراءات التي من شأنها حماية سرية وسلامة وخصوصيات المعلومات ومكافحة الجرائم المعلوماتية" (عبد الوهاب جعيجع 2017).

وإنه ومنذ عقود من الزمن ومواطني الدول المتقدمة يطالبون بإنشاء جماعة نفوذ ومصالح أو ما يعرف باللوبي الجماعي من أجل المطالبة بجعل العالم السيبراني والفضائي تحت سلطة المؤسسات والشركات الكبرى الخاصة، والتي من جهتها تستطيع هذه الأخيرة أن تضمن حرية إستعمال " عالم النات " وتعطيه حرية كبيرة في مجال الإبتكار والمشاركة والإيثار، ويصبح السوق هو المتحكم في تنظيم هذا العالم الإفتراضي،وهذا عكس الحكومات التي تمتاز بالبطء في موضوع الإجراءات البيروقراطية , و هو الأمر الذي يسمح ببروز حضارة الانترنيت العظيمة , التي تنفتح على الاقتصاديات الحرة التي تمنح الفرصة الكاملة للجميع ." (2020– 2021MechoulanEric)

ولتأكيد إمكانية لعب الفضاءات السيبرانية وشبكات التواصلالاجتماعية السيبرانية مثل ما يعرف ب: شبكة قوقل وفروعها: يوتوب، أبل، فايس بوك، مع فروعها: واتساب والانستغرام، الامازون وميكروسوفت. بالإضافة إلى الشركات الكبرى التي تهيكل القطاعات الصناعية تقريبا بنسبة شبه كلية مثل نتفليكس Netflix وإيبر Uber وأير ب ن ب Airbnb، وشبكات التواصل الاجتماعي وكذا "المراكز الكبرى للتكنولوجيا Big Tech " الرائدة في العولمة المالية والتجارية وكذا الثقافية، حسب الإلهام و الروح الامريكية، و هذا ما يؤكد ان هذه الشركات العملاقة تلعب دورا كبيرا في تقاسم السيطرة و النفوذ في عالم الأعمال مع القوى العظمى في العالم بشكل متساو." (2021–2020EricMechoulan)

ويمكن إضافة تعريف آخر حسب " الاتحاد الدولي للاتصالات و الوكالة الأممية المتخصصة في ميدان الاتصالات و الأمن السيبراني بأنه:" مجموعة الأدوات والسياسات ومفاهيم الأمن و تحفظات الأمن والمبادئ التوجيهية ونهج إدارة المخاطر والإجراءات والتدريب وأفضل الممارسات واليات الضمان والتكنولوجيات التي يمكن استخدامها في حماية البيئة السيبرانية، وأصول المؤسسات والمستعملين لأجهزة الحوسبة الموصولة بالشبكة والمستخدمين والبيئة التحتية والتطبيقات والخدمات وأنظمة الاتصالات ومجموعة المعلومات المنقولة او المحفوظة في البيئة السيبرانية" (عبد الوهاب جعيجع 2017)

ومن ذلك أن مخاطر هذا الفضاء السيبراني جلية، فبعد أن تعرضت الأنظمة المعلوماتية سواء المختصة بعالم الاقتصاد، أو السياسة أو الدفاع، أو الثقافة أو أصناف الاجتماعيات، وكل ذي مصلحة تتعلق بهوية المجتمع ومستقبله، إلى أن تعد هذا الإجرام الإرهاب الالكتروني أو الإرهاب السيبراني "cyber terrorism " وهو ما أدى إلى الإضرار بكيان الدول والمجتمعات والأمم، علاوة على الإضرار بالأفراد والجماعات المختلفة، بحيث أصبحت، " شبكات البنية التحية الحيوية التي تحتفظ بها الحكومات في جمع أنحاء العالم عرضة للهجمات الالكترونية الرئيسية في أي لحظة". (لامية طالة 2021)

وفي هذا الصدد يمكن الإشارة إلى تحول المعضلة السيبرانية إلى هاجس كبير بالنسبة للأمم والمجتمعات من اجل الحفاظ على مقوماتها،وهو ما حذا بوزير الدفاع الفرنسي السابق: جون إيف لودريو (JEAN YVES LE DRIAN) القول بأن المعركة الرقمية أصبحت في قلب كل المهام المتعلقة بالدفاع والأمن.

" (JEAN YVES LE DRIAN–2015)وهو يستذكر الاحداث والعمليات والانفجارات التي حدثت في جانفي 2015 بباريس والتي كانت الوسائل المستخدمة فيها معتمدة على الأدوات السيبرانية

وهو الامر الذي جعل الحكومة الفرنسية تأخذ بجدية التطورات والتعقيدات الكبيرة التي رافقت الفضاء والجريمة السيبرانية على السواء. وإذا كانت شبكة الانترنيت بكل تفرعاتها وأنماطها ثرية بما فيه الكفاية من التطوير والابتكار، أي في الوقت نفسه يمكن أن تكون هذه الشبكة في خدمة افراد أو دول غير واعية، ولا تقدر المسؤوليات والعواقب من حيث إستخدام هذه الشبكات للإضرار بمخزون هذه الشبكات، ولاستعمالها في مجالات إرهابية. وبالإضافة إلى جماعات الإرهاب السيبرانية، نجد المنظمات والعصابات والجماعات الاجرامية المنظمة أو ما يطلق عليها "بالمافيا ". بحيث نجد هذه الأخيرة تستعمل وتتخذ وسائل ذات مستوى عالي من التكنولوجيا الرقمية بالخصوص وأين تتفوق من حيث الاستعمال والامتلاك لهذه التكنولوجيا المتطورة جدا في الكثير من الأحيان على بعض الدول.فعصابات المافيا سواء كانت تستغل هذه المعلومات لنفسها أم كانت تقوم ببيعها وتوريدها لمن يدفع أكثر." (JEAN YVES LE DRIAN 2015)

ويمكن في ذات السياق والمتعلق بالاستعمال الإرهابي للفضاء السيبراني – المعلوماتي من طرف الإرهابيين مهما كانت مشاربهم العرقية والدينية، وبوصول الكثير من شبابهم المتعلم والدارس في المعاهد والكليات والجامعات والتحاقهم بعد ذلك بالجماعات الإرهابية والتي غالبا ما ألصق بهذه الجماعات صفة الإسلاميين، أين مكنهم تمكنهم من إستعمال التكنولوجيا الرقمية من التحكم في الكثير من المواقع الالكترونية وأصبحت هذه المواقع عبارة عن مكاتب متقدمة للإشهارو الترويج لأفكارهم.وهو ما جعل المحللين المختصين فيقضايا الإرهاب الرقمي، يعتبرون أن المعركة هي نفسها، أي أن لها نتائج وخيمة على الافراد والمؤسسات العامة. فهو إذا فضاء استراتيجي بكل معنى الكلمة. وهو الامر الذي جعل الكثير من الدول تأخذ مأخذ الجد، الإرهاب السيبراني لتحضير وإيجاد القدرات الهجومية اللازمة لهذا الفضاء السيبراني الواسع،ومن ضمن هذه الدول نجد على سبيل المثال وإن كانت في الحقيقة هي السباقة إلى إتخاذ الإجراءات الوقائية والدفاعية فيذلك،فنجد: "روسيا، الولايات المتحدة الامريكية،وإسرائيل." (JEAN YVES LE DRIAN 2015)

إن الحرج الذي يسببه عالم الانترنيت ومن خلاله كنهه العظيم العالم السيبراني فإن النزاعات حول المحتويات التي تبث في هذا الفضاء الفسيح ل يتسبب فيه فقط القراصنة السيبرانيين وإنما قد يتسبب فيه عمالقة الانترنيت أو ما يعرف بمالكي البيق داتا – Big Data – في الكثير من المرات أين يتصادمون مع دول مختلفة , و يتسببون في المساس بمسؤولياته و سيادتهم و صلاحياتهم من تنظيم المصالح الكبرى لدولهم , و للمثال على ذلك ما وقع خلاف عام 2006 بين دولة الهند و مصالح الخرائط لشركة قوقل إيرث للأنترنيت بأن إتهمت الهند هذه الأخيرة بأنها قامت بإنتهاك حق الدولة الهندية في حماية سيادتها الترابية , و ذلك من خلال نشر شركة قوقل لصور واضحة ودقيقة لمناطق تعتبرها الهند حساسة . وبعد مفاوضات بين الدولة الهندية وشركة قوقل إنتهى الطرفان إلى قبول شركة قوقل بإزالة بعض الصور. وهذه الواقعة تكررت عدة مرات عبر العالم. ولقوة هذه الشركات العملاقة ودورها

الحساس والمنوط بها في إمكانية الحفاظ على الكثير من المعلومات الاسرار، تعتبر الدولة الفرنسية أن شركة قوقل محاور حتمي وبدون منازع تجاه الكثير من الدول"(Eric Mechoulan 2020-2021)

و في المقابل أيضا نجد أن الكثير من المنصات و شبكات التواصل الاجتماعي مثل:يوتوب،فايس بوك و تويتر أصبحت عبارة عن وسائل الضغط و النفوذ , و أيضا للتدخل الدولي لأطراف دولية على حساب دول أخرى , وهو ما يمكن الإشارة إليه في واقعة الانتخابات الرئاسية الامريكية لعام 2016 , أين أبانت الواقعة على التدخل الروسي في ترجيح فوز المرشح الجمهوري " دونالد ترامت " بإنتخابات الرئاسة الامريكية على حساب المرشحة الديمقراطية "هيلاري كلينتون " و هي الواقعة التي سال حبر كثير من أجلها و دارت حولها و في محيطها الكثير من الحوارات و نشرت من أجلها الكثير من الوثائق . وهو الأمر الذي أبان عن تدخل روسي لصالح المرشح دونالد ترامب وذلك من خلال الرسائل النصية التي كانت توجه لشريحة ذوي البشرة السوداء والتي تدعوهم إلى الامتناع عن التصويت، وهذا التوجيه نحو الامتناع كان يخدم دونالد ترامب المؤيد من شرائح كبرى من المحافظين الأمريكيين , كما أبانت التوجيهات عن توجيه واضح و بارز للناخبين الأمريكيين ودعوتهم للاقتراع مرشح الجمهوريين دونالد ترامب , و الذي حقيقة فاز بإنتخابات الرئاسة الامريكية لعهدة ما بين نوفمبر 2016 إلى غاية نوفمبر 2020.

ومن ضمن أهم الأهداف المتوخاة من جانب السلطات القومية للدول والحكومات في ظل قيامها بالاحتياطات اللازمة لحماية فضائها السيبراني من الأخطار المحتملة من المجرمين الالكترونيين، أو ما يطلق عليهم بالها كرز هو: أن تصبح مؤسسات الدولة والمجتمع ككل، " في مأمن من خطر التعرض للهجوم، وإجراءات الحماية ضد تعرض المنشآت الحيوية للبنية التحتية للتهديد، من خلال الاستخدام السيئ لتكنولوجيا الاتصال والمعلومات . (لامية طالة 2021)

بحيث أن هناك تداخلا كبيرا في العصر الحديث والمعاصر من حيث العلاقة المتوازنة واللصيقة بين مفهوم الأمن القومي مع مفهوم الأمن السيبراني. وذلك كون أن الثورة الرقمية والتدفق الكبير والمرتفع للأنترنيت متلازمة مع الأمن القومي والأمن السيبراني و هاتين المتلازمتين، تستوجب الضرورة الربط بين بعضهما البعض، كون مجمل برمجيات ومعلومات ومنظومات الدول والحكومات في الوقت الحالي أصبحت عبارة عن أرقام وشفرات ناقلة للمعلومات ووثائق وملفات وبرامج مختلفة لمجالات مختلفة تخص واقع الدول والحكومات و أصبحت عبارة عن قيم معرفية الكترونية ورقميةتتقاذفها المنصات والتطبيقات الالكترونية الرقمية والتي هي عبارة عن مصاهرة بين الأجهزة مع عالم الانترنيت وأي استخدام خاطئ يكلف صاحب الرزم والملفات التقنية والمتناثرة في الفضاء الواسع للأنترنيت ويمكن أن يضر بمصلحة البلد مالك و صاحب هذه التدفقات الرقمية الكبيرة والضخمة.

كذلك فإن بروز متحكمون جدد في الأدوات والوسائل الرقمية المرتبطة بعالم الانترنيت والحاسوب من غير الفواعل الكلاسيكيين المتمثلين في الدول والمؤسسات الحكومية، فقد ظهرت مؤسسات وشركات خاصة متحكمة في التقنية المستعملة للأجهزة الالكترونية وعالم الرقمانيات، وهي شركات عابرة للحدود " cybranationales " وأصبحت إمكانياتها التقنية والمالية الاستثمارية أكبر من إمكانيات الدول والحكومات، وهو الأمر الذي فرض نوع من الانفلات بالنسبة للدول النامية والسائرة في طريق النمو، عكس الدول الكبرى العملاقة التي لديها من الإمكانيات التقنية والمالية ما يعطيها القدرة والحصانة لحماية مخزوناتها ومعطياتها الرقمية، ومع ذلك فقد تعرضت بعض منشئاتها وتطبيقاتها للاختراق والقرصنة من طرف قراصنة معلوماتيين وفي بعض المرات ظهر أن هؤلاء القراصنة (الهاكرز) كانوا عبارة عن هواة وليس محترفون بالمرة.

في ظل التحولات الكبرى التي حدثت في ميدان العلاقات الدولية والاتصالية حيث الفواعل المختلفة المكونة للنظام الدولي سواء الفواعل الأساسية المتمثلة في الوحدات السياسية (الدول) او الفواعل الثانوية , لكنها مؤثره في تفسير ادوات وحركية النظام الدولي الحالي والمتمثلة في الشركات عبر الوطنية أو المنظمات غير الحكومية وكذا المنظمات الدولية المتفرعة عن منظمة الامم المتحدة، فان الظهور بمظهر قوي وذا نفوذ في مسرح العلاقات الدولية فرض على هذه الفواعل المختلفة الحصول على اكبر قدر ممكن من النفوذ والسيطرة على عالم التكنولوجيا والعالم الافتراضي المتمثل في العالم السيبراني، واذا كانت هذه الطموحات طبيعية وجوهرية لصالح بعض الدول فإنها تعتبر تهديدات واخطار محدقة ضد الدول الاخرى السائرة في طريق النمو وغير القادرة على اكتساب هذه المعارف والتكنولوجية وكذا غير القادرة على اكتساب امنها السيبراني – المعلوماتي– ويمكن اجمال التهديدات السيبرانية المعاصرة على العناصر الاتية.

1–تهديدات السيبرانية المحدقة بالجانب العسكري.

لقد أدى التطور الكبير في الميدان التكنولوجي الى تطوير المنظومات المعلوماتية للدول لتتأقلم مع الوضع، وتنتقل من العالم التقليدي للحرب واستعمال المواجهة المباشرة بين الجيوش المتخاصمة بما في ذلك الاليات المدرعة والأسلحة الأوتوماتيكية و الطائرات النفاثة وما الى ذلك غير ان ادخال الأنظمة المعلوماتية الحديثة والمتطورة جدا على منظومات الدفاع والهجوم على السواء اصبح لهذه الحروب السيبرانية دورا كبيرا في زيادة على الحرب المباشرة، فهي تقوم بجمع المعلومات الاستخباراتية، وتجنب العملاء وتخترق المجال الجوي بسهوله وتؤدي عمليات اختراق جوية بطائرات الدرونز (طائرات بدون طيار). كما تقوم الحروب السيبرانية بتخريب المنظومات المعلوماتية للدول المتصارعة معها من امثلة هذه العمليات نذكر بما حدث بين روسيا واستونيا عام 2007، وكذا بين روسيا وجورجيا عام 2008، واذا كانت هذه الحروب السيبرانية وكما يصفها البعض بانها حروب من دون نار ولا دخان، فهي لها عمل عنيف من حيث الاقتراحات والقرصنة ونشر الفيروسات وغيرها من الاساليب، وبالرغم من فداحة الخسائر فان الأسلحة بسيطة لا تتعدى في اغلب الاحوال الكيلومايتس من الفيروسات الإلكترونية تخترق شبكة الحاسوب الالي وتتميز هذه الحروب بالسرعة والدقة في تنفيذ العمليات العسكرية وتعتبر من ادوات الحروب الشاملة وهذه الحروب بعد ان كانت تستهدف اجهزة الانترنت والحواسيب الان تستهدف قطاعات وصناعات محددة" (زياد العلي 2019).وإذاأردنا الجمع بين حرب المعلومات والعمليات العسكرية فإننا نوردها فيما يأتي:

من الجانب الاول (حرب المعلومات) نجد: الحرب الالكترونية الكلاسيكية ومنها: القرصنة الالكترونية أو حرب المعلومات الاقتصادية.

أما من جانب الحرب العسكرية، فانه حري بنا ذكر ما يلي: جمع المعلومات الاستخبارية وعمليات تستهدف المعنويات النفسية لطواقم جيش معين، وتحليل العمليات الهجومية وكذلك تحليل كافي للعمليات الدفاعية.

2–التهديدات السيبرانية المحدقة بالجانب الاقتصادي:

وهي تلك الهجومات السيبرانية التي تمس مصالح الدولة والمؤسسات العمومية وكذا المؤسسات الخاصة، وكذا المساس بمصالح الاشخاص الاقتصادية، وهي هجومات عديدة يمكن الاشارة الى بعضها على سبيل المثال لا الحصر و منها : العبث بمخازن المعلومات وتعطيل برامج العمل في الوزارات والمؤسسات السياسية وكذا تعطيل الأنظمة المالية والبنكية واختراق المواقع الإلكترونية لكل المؤسسات العامة، الخاصة سرقة الهويات الشخصية للأفراد والرسميين ، وكذا الابتزاز والتهديد وعمليات الاحتيال الكثيرة والتي

تطال أيضا الأموال العامة والخاصة ويمكن تلخيص ما قيل في المعلومات الواردة من كتاب ايهاب حنيفة المشار اليه سابقا في الصفحة: 122 بان "معدل نسبة الجرائم الإلكترونية في العالم يصل الى 57.6% حيث يكلف الاقتصاد العالمي ما يقارب 12.950 مليار دولار سنويا، وبان معدل الهجمات الإلكترونية في السعودية وصل عام 2009، ما يقارب الى 45.8% وهو في تزايد كبير في السنوات الأخيرة. وكشفت السلطات الأمريكية عام 2009 ان عمليات قرصنة وسرقة طالت أكثر من 130 مليون بطاقة ائتمان وبطاقة سحب مصرفية(زياد العي 2019)

3–التهديدات السيبرانية المحدقة بالجانب السياسي:

لقد ادت التطورات الكبيرة التي عرفها عالم التكنولوجيا في فضاء عالم الاعلام والاتصال الى ظهور عناصر مؤثرة جدا غير تلك العناصر التقليدية المعروفة سابقا في ميدان السياسة سواء في العمليات الانتخابية او الولاءات او نفوذ على التفكير واللوبيات السياسية وتأثيرها وتوجيهها لنتائج الانتخابات. وأصبح السياسيون يطلون على المواطنين المنتخبين على السواء من خلال شبكات التواصل الاجتماعي دون اللجوء الى الوسائط الاعلامية التقليدية مثل التلفزيون والراديو الصحافة المكتوبة، وأصبحت اطلالاتهم عن طريق الفايسبوك والتويتر، واليوتيوب وغيرها كثيرا. ولنتذكر تأثير التغريدات التي كان يبثها وينشرها الرئيس الامريكي السابق دونالد تراب والتي كان لها تأثير كبير في اوساط المواطنين والمنتخبين الامريكيين، حتى انه اتخذ قرارات وأمضي مراسيم رئاسية ونشرها أول ما نشرها عبر شبكة تويتر والتي كان لها تأثير كبير، ومن تلك القرارات الهامة والمؤثرة، امضاءه لقرار انسحاب الولايات المتحدة من معاهدة المناخ، وكذلك انسحاب الولايات المتحدة من المعاهدة الدولية مع الاتحاد السوفياتي سابقا (روسيا حاليا) المتعلقة بأسلحة الدمار الشامل ستارت 1 وستارت 2. وكذلك الإشارة الى ما يسمى اتفاقيات السلام الإبراهيمية بين الدول العربية واسرائيل، وكذلك الاعتراف بمغربية الصحراء الغربية، وغيرها كثير. كما يمكن الإشارة الى التهديدات السيبرانية على نتائج الانتخابات الرئاسية الأوكرانية لسنه 2014 وكيف أطلق القراصنة الموالين لروسيا حملة سيبرانية هجومية من أجل التأثير على نتائج الانتخابات وكذا إثارة الشك والريبة في نتائجها.

ويمكن الإشارة أيضا الى الهجومات السيبرانية بمناسبة عملية الاستفتاء التي حدثت في بريطانيا بمناسبة الاستفتاء على مسار خروج بريطانيا من الاتحاد الاوروبي، أين إتهم رئيس وزراء بريطانيا السيد "ديفيد كامرون" روسيا بالوقوف وراء الحملة السيبرانية الداعمة والداعية لخروج بريطانيا من الاتحاد الاوروبي وكان ذلك عام 2016. وكانت النتائج كما هو معروف ايجابيا بالنسبة لدعاة خروج بريطانيا من الاتحاد الاوروبي.

وهو الامر الذي أشار الى دور الاستخبارات السيبرانية الروسية في هذا الفعل، كما كشف التقرير الذي أصدرته لجنة الإدارة العامة والشؤون الدستورية التابعة لمجلس العمومالبريطاني عام 2016 دور الاستخبارات الروسية في انشاء وتمويل حركه الدعائية الإلكترونية التي تحث الناخبين للتصويت بنعم للخروج من الاتحاد الأوروبي. (زياد العي 2019)

ويمكن الإشارة إلى أوجه الجرائم الواقعة على نظم المعلومات، أو ما يسمى بالهجمات السيبرانية وذلك من خلال شرح وتفصيل" ايهاب خلية" المشار إليه من طرف الباحث مسيكة محمد وذلك حسب الإضافات الآتية:[16] وذلك من خلال معايير تصنيف هذه الهجمات السيبرانية الخطيرة. فهو يقسمها على شكل أنماط وصور:

1–فالصورة الأولى من التوجهات، تتمثل في تلك الهجمات التي تمس الهندسة الاجتماعية (Engineering Social) وهي أخطر العمليات الاجرامية في عالم المعلومات، فهي تقوم بتصيد النخب الاجتماعية وتؤثر فيهم سلبا تجاه ثقافاتهم وهوياتهم.

2–جرائم معلوماتية سيبرانية تمس خدمة الانترنت والمعلوماتية DDOS وأهم طريقة لتنفيذ هذه السياسة العدائية تجاه الدولة الضعيفة خصوصا والسائرة في طريق النمو، أنها تقوم بإرسال كم هائل من الرسائل وبشكل يفوق المعقول، وهو الأمر الذي يؤدي إلى تعطيل خدمة الانترنيت أو تعطيل خدمة المنصة أو الموقع سواء كانت مواقع حكومية أو خاصة.

3 – بالإضافة لما يعرف بالأبواب الخلفية، أين يتم تركيب أجهزة لاصقة بأجهزة الكمبيوتر، وذلك بغية التجسس على الأفراد والجماعات دون مراعاة حرمة تلك المعلومات والأسرار على حياة الناس ومحيطهم.

ومن ضمن التهديدات الأمنية المعاصرة , نجد التهديد الأمني الإرهابي التقليدي و الإرهاب السيبراني الحديث والذي ظهر مع ظهور وتطور الوسائل التكنولوجية والتي أصبحت مؤثرة كثيرا وبتقنية عالية، وتجاوزت الحدود الجغرافية , و هو ما تتبعه الجماعات الإرهابية والتي تمددت بصورة كبيرة من الحدود المحلية والإقليمية إلى ما بعد الحدود الوطنية أو ما يعرف بالإرهاب عبر الوطنية " Supranationales"، ففي " ظل الثورة التكنولوجية التي يعرفها العالم أصبح الإرهاب السيبراني من أخطر الجرائم التي تهدد الأمن القومي الجزائري من خلال تنامي مظاهر الترويج لكل أشكال العنف والإرهاب والتطرف باستخدام أحدث التقنيات التكنولوجية" (ليندة معيزي – دهقاني أيوب2023)

ومن أمثلة هذه التهديدات الإرهابية وأنماطها نجد أن هذه الجماعات الإرهابية تقوم بإنشاء مواقع الكترونية كثيرة ومتنوعة، يتم فيها تبادل وتمرير المعلومات والاتصال والمخططات البينية بين الإرهابيين عبر مواقع إلكترونية ومنها على سبيل المثال:(موقع النداء وذروة السنام، وصوت الجهاد). (ليندة معيزي – دهقاني أيوب2023)

وهي كلها مواقع إشهارية عدوانية تخريبية للأوطان والمجتمعات. وفي ظل الأسباب السياسية والتأثير الذي يمكن أن تلعبه التطبيقات السيبرانية في عالم الانترنيت وكذا إمكانية أن تقم القوى العظمى بالتأثير على أفكار وقناعات شعوب ومواطني القوى والدول الأخرى قات أمريكا في عهد الرئيس السابق دونالد ترامب بعد ما أحست أمريكا بخطر عمالقة الانترنيت والمحولات والمخزنات الكبرى للمعلومات السيبرانية بإصدار أمر رئاسي يخص منع الأمريكيين من كل معاملة مع شركة بايت دانس Byte Dance وهي الشركة الام للتطبيقة السيبرانية – (تيك توك–(tiktok), و هي المنصة المتخصصة في حمل الصور و التي يستعملها أكثر من 160 مليون مواطن أمريكي , و هي المنصة التي يعتبرها الساسة الامريكيون بأنها تقوم بتحويل المعلومات و تخزينها لصالح الصين , و التي يمكن أن يستعملها الصينيون لصالحهم خارج الأطر القانونية . وأمام هذا الهاجس في إستعمال معلومات الأمريكيين من قبل الشركة الصينية إقترح الرئيس الأمريكي دونالد ترامب على الصينيين التنازل عن أسهم لشركتين أمريكيتين وهما: أوراكل Oracleووالمرتwalmart،وذلك بغية قيام هاتين الشركتين الامريكيتين بتخزين معلومات الأمريكيين في الحواسيب والخوادم الخاصة بها عوض إنتقاله لصينيين. (Eric Mechoulan2020–2021)

وفي ظل الصراع والتسابق نحو إمتلاك التكنولوجيات الفائقة والمتطورة للسيطرة على عالم الأنترنيت والفضاء السيبراني وفي سياق الحديث عن الحرب الرقمية المستقبلية، يمكن الإشارة إلى تأكيد السيد: تيري بورخاد (Thiery Burkhard) من خلال مجلة ملحق السياسة الدولية رقم 174 , الصادرة في شتاء 2021–2022 , أين تحدث عن مصطلح " الحرب قبل الحرب (guerre avant la guerre) , و الذي أعقبه بالحديث عن المصطلحات الثلاثية : التنافس و الرفض و المواجهة (– compétition

(contestation – affrontement) , و هو المصطلح الذي يجمع بين ثلاثية تفسيرية أخرى تتمثل في : السلم – الأزمة – و الحرب (paix – crise– guerre) (Thierry Burkhard 2021–2022) .

ويضاف إلى الأخطار التي تواجه الفضاء السيبراني من خلال إختراق القراصنة والمجرمين السيبرانيين، أين أضحى هذا العلم الرقمي يتعرض لنونع من الوباء الجديد المتمثل في الهجمات السيبرانية التي تصيب كل الأدوات والوسائل المستعملة في عالم المعلوماتية سواء الحواسيب وكذا الانترنيت وهو ما جعل مجلة: إكسبراس(Express) الفرنسية تطلق على الحرب المعلنة في الفضاء المعلوماتي الرقمي الخفي , بالوباء وهي بذلك تشبه هذه الصورة السلبية للعالم الرقمي الخفي بوباء كورونا الذي ضرب المعمورة بين عامي : 2020–2022 , و الذي قضي على الملايين من البشر دون سابق إنذار . ويضاف على هذا الموصوف بالوباء إستغلال وإستهداف المجرمين المعلوماتيين للضحايا الرقميين في إختراقات عديدة وكثيرة غالبا ما تنتهي بطلب فديات مالية كبيرة و في بعض الأحيان خيالية. وهو ما يجعل من جهة أخرى الدول العظمى، والتي ينتظر منها أن تعلب دورا على الساحة الدولية ان تحضر نفسها بكل جدية لخوض حرب رقمية – سيبرانية – في المستقبل.) (POUPARDGUILLAUME)

المحور الثالث: دور المنظومة القانونية الوطنية في التصدي للتحديات السيبرانية على الأمن القومي (الوطني):

وإذا كنا قد تعرفنا على مفهوم الامن العام ومفهوم الامن السيبراني في المحورين السابقين لهذه المقالة العلمية , فإنه يجدر بنا أن نبحث في علاقة هذين المفهومين بمفهوم الامن القومي– الوطني– السيبراني و هو الامر الذي يتضح جليا من خلال تعريف الأمن السيبراني الصادر عن " الاتحاد الدولي للاتصالات" في عام 2010/ 2011, والذي أعطى التعريف التالي "بكون الأمن المعلوماتي–السيبراني هو: "عبارة عن مجموعة الوسائل التقنية والتنظيمية والإدارية التي يتم استخدامها لمنع الاستخدام غير المصرح به، وسوء الاستغلال، واستعادة المعلومات الالكترونية، ونظم الاتصالات والمعلومات التي تحتويها، وذلك بهدف ضمان توافر واستمرارية عمل نظم المعلومات، وتعزيز حماية وسرية وخصوصية البيانات الشخصية، واتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين من المخاطر في الفضاء السيبراني". (محمد مسيكة 2022)

أهم الثغرات في الفضاء المعلوماتي، السيبراني التي يجب حمايتها:

–ضرورة حماية أمن المعلومات وهي عبارة عن تلك الخطوات والمبادرات من أجل حماية المعلومات في خصوصيتها، حتى يتم استغلالها بطريقة جيدة ويمكن الوصول إليها بسهولة التي فرضت الحاجة ذلك.

–ضرورة حماية أمن التطبيقات المعلوماتية، وهو ما يتعلق بوضع ضوابط لحماية هذه التطبيقات من الفيروسات الموجهة من قبل القراصنة المعلوماتيين لها من أجل تخريبها والمساس بها.

–ضرورة حماية أمن الشبكات والتي تتعلق بحماية أعمال ومهام الأفراد والمؤسسات التي تنجز من قبل هؤلاء بطريقة الشبكات المعلوماتية.

–ضرورة حماية وتوظيف المعلومات السيبرانية ومعالجتها وتخزينها بطريقة آمنة.

–ضرورة ضمان حماية ويقظة لمجمل أعمال الشركات بطريقة وبوسيلة المعلوماتية كفاية، ووضع خطط احتياطية بديلة مستعدة لمقاومة أي طارئ يمس ويخترق أمن المعلومات لهذه الشركات وكذا الأفراد.

ومن ذلك ضمان صيرورة واستمرارية عمل هذه الأخيرة، رغم تعرضها لأي اختراق خارجي.

–وهذا ما يجرنا إلى الحديث عن الأمن السيبراني وضمان الأمن القومي في المستقبل، وقد يثبت ذلك ويصبح حقيقة من خلال تحديث الجيوش وتدشين وحدات متخصصة في الحروب السيبرانية، وإقامة هيئات وطنية للأمن والدفاع الالكتروني والقيام بالتدريب، وإجراء المناورات لتعزيز الدفاعات السيبرانية، والعمل على تعزيز التعاون الدولي في مجالات تأمين الفضاء السيبراني. (محمد مسيكة 2022)

إن استخدامات الشبكات الاجتماعية عبر الانترنت جعل الجزائر في المرتبة الرابعة عربيا من حيث مستخدمي الفاسبوك بحيث وصل عدد الجزائريين وخصوصا الشباب المستخدمين لشبكة الفاسبوك أكثر من 15 مليون شخص (دهقاني أيوب ومعيزي ليندة).

وهذا العدد الهائل والضخم والذي تزايد من سنه 2016، تاريخ صدور التقرير العالمي الذي اشار الى هذه الاحصائيات يكون الان وفي الفترة الحالية لدخول الجزائر في عام 2024 العدد قد تجاوز حدودا كبيرة ولا حصر لها. وهو الامر نفسه في العالم أين تشير التقارير الى أن مستخدمي شبكات التواصل من العالم قد وصل تعداده، إلى ما يزيد عن 05 مليار شخص أي بنسبة تزيد عن 60% من سكان العالم.

وهو الامر الذي ينبئ بظاهرة مزدوجة، من جهة إحداث قفزة نوعية في إستخدام شبكات التواصل الاجتماعي ومن جهة اخرى سلبية, أين يمكن أن يكون هذا الاستخدام خطر على المجتمع الجزائري من حيث بلوغ العام الماضي 2023 عدد مستخدمي الانترنيت بكل شبكاته 32،09 مليون شخص مقابل 28،27 مليون خلال عام 2022، وترجع هذه النسب المرتفعة من استعمال هذه الشبكات الى ذلك الارتفاع المحسوس في نسبة الاشتراك في فضاء الانترنيت في جانفي بحيث بلغت نسبة هذا الانتساب إلى عالم الانترنيت في جانفي 2023 الى 70.9% من نسبة السكان في الجزائر والبالغ عددهم ما يقارب 47 مليون نسمة , وذلك بارتفاع نسبة تدفق الانترنيت في الجزائر سنة 2023 الى 11.01 ميغابايت في الثانية في جانفي 2023 مقارنة بنسبة 2022 أين كانت نسبة تدفق الانترنيت 9.78 ميغابايت في الثانية ويرجع ذلك الى مجهودات السلطات العمومية في تحسين خدمة الانترنيت لصالح الطبقات الواسعة من السكان وفي كل مناطق الوطن (وكالة الانباء الجزائرية :21 فيفري 2024)

وفي هذا المجال لا يمكن بحال من الأحوال مقاومة الاختراقات الرقمية لأنظمة المعلومات عن طريق التقويمات والتصويبات الرقمية فقط، وإنما يستوجب الأمر إعداد منظومة قانونية كاملة لمجابهة هذه الخروقات على أنظمة الحواسيب، والمساس بأمن المعلومات المخزنة في الحواسيب سواء كانت مملوكة لأشخاص فرادي أم لمؤسسات وشركات سواء كانت عمومية أو خاصة، ولقد عرفت المنظومة القانونية لمجابهة الأخطار والتهديدات الواقعة على أنظمة الكمبيوتر، تطورا كبيرا سواء من حيث المنظومة القانونية الدولية، أو المنظومة القانونية الإقليمية والمحلية لكل دولة على حدى.

فلقد تزايدت الجريمة المعلوماتية كما تصنف قانونيا، تزايدا كبيرا، خصوصا بعد ما اعتمدت الحكومات في تسيير دواليبها، على الأنظمة الرقمية سواء من حيث التحويلات المالية والخدمات المصرفية وكذا التسوق عبر الفضاء الأزرق الأوسع منه من طرف منظمات الجريمة المعلومات عبر العالم سنويا.(GUILLAUME POUPARD2021)

بحيث جلب تطور عالم الأعمال والمال والجوانب التكنولوجية المرتبطة به تطور الجرائم السيبرانية والمرتبط بالعوائد المالية أو ما يعرف بطلب الفدية عن طريق الواب (web) بداية من سنة 2017،وهو ما أصبح يطلق عليها (جرائمالفدية) ببرامج الفدية (rancongiciels) (HIVER–2021–2022GUILLAUME PITRON–)

وقد تعممت بعد ذلك هذه الظاهرة بداية في فرنسا ومن بعد ذلك على مستوى العديد من الدول.

وإذا أردنا أن نشير إلى الدول الأولى التي بادرت لمجابهة الجريمة المعلوماتية فإننا نجد دولة السويد أين كان لها السبقومجابهة الجريمة السيبرانية سنة 1973 من خلال قانون تجريبي يسمى بقانون البيانات ثم تبعتها أوروبابعد ذلك في سنة 2001 من خلال إمضاء اتفاقية أوروبية في مجال مجابهة الجريمة المعلوماتية سنة 2001 في العاصمة المجرية بودابست، وهي الاتفاقية التي انضمت اليها الولايات المتحدة الأمريكية سنة 2006.

ويمكن القول بأن الجريمة المعلوماتية من حيث تعريفها الإجرائي والقانوني هي: " وقوع أي سلوك أو إجراء على أنظمة الحواسيب من خلال الاعتداء على البرامج والمعلومات أو البيانات المخزنة بأجهزتها، سواء بالإضافة أو التعديل أو المسح، أو النشر دون إذن صاحبها، أو التصرف فيها بأي وجه من الوجوه، أو بأية صفة من الصفات. ويمكن الإيضاح في هذا الموضوع أكثر من حيث القول، بوجود نوعين من الجريمة المعلوماتية، فالصنف الأول يتمثل في الجرائم التي تستهدف: " النظام المعلوماتي مثل التعدي على البيانات الخاصة كاستخدام البيانات المجمعة لشخص والتداول والتوظيف غير المرخص لها أو التشهير والإساءة إلى السمعة، والضغط والابتزاز ". أما الصنف الثاني فيتمثل في الإضرار بأنظمة المعلومات بحد ذاتها.

أما الأجهزة والحواسيب فهي الجانب المادي في عملية الجريمة المعلوماتية، والتي تضر بالنظام المعلوماتي بحد ذاته، وهي الجرائم التي تعني بالمساس بالبرامج والتطبيقات والبيانات التي تحوزها الحواسيب والشبكات.

إن تطور الجرائم الالكترونية (السيبرانية) حتم على المشرع الوطني أن يسن قوانين لمواجهة الأخطار والتحديات التي يفرزها هذا الفضاء السيبراني، وكون القاضي الجنائي مقيد بنصوص قانونية على رأسها" لا جريمة ولا عقوبة إلا بنص" وأمام القاضي الجنائي الاستفاقة سواء من خلال الاستعانة بقانون خاص محدد للجرائم المعلوماتية. أو حتى تلك النصوص الموجود في قانون العقوبات الجزائري الذي يعطي حماية للأموال، وضمن هذه الفكرة، صدر أول قانون جزائري ينظم المعلوماتية ويحميها من أي خطر من خلال القانون. (قانون العقوبات 2001).

وهو قانون العقوباترقم: 01-09-المؤرخ في 26 جوان 2001. وذلك في المادتين 144 مكرر و144 مكرر1، والذي سوف نتناوله بالتفصيل فيما يأتي من توضيحات في هذه المقالة لاحقا. بالضافة إلى قانون خاص بالجريمة المعلوماتية الذي صدر بتاريخ : 05 غشت (اوت) 2009 و الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال وقد أصبح الاهتمام بسن قوانين ونصوص قانونية لمقاومة ومكافحة الجرائم المعلوماتية نظرا لتفاقم خطورة الاستعمال السلبي للفضاء السيبراني ومنه الاستعمال الخاطئ لروح هذا القضاء المتمثل في الانترنت، اين ظهر ونتج عن الكم الهائل من الفضاءات والشبكات والتطبيقات، ظهور مجموعات وجماعات خطيرة تمارس الجريمة المعلوماتية و صعدت و تفاقمت جرائمها من حيثإرتكاب مخالفات وجنح وجرائم وجنايات في حق الاشخاص والجماعات وكونت لنفسها عالما سمي فيما بعد بالجريمة المنظمة، وحتى وان كان هذا المصطلح ظهر للوجود بداية من 1919 في الولايات المتحدة الأمريكية وبالتحديد في ولاية شيكاغو. (إسراء أحمد إسماعيل 2011)

ومن حيث أن شبكات الجريمة المنظمة هدفها هو الربح وتحقيق المنفعة، وهو الهدف الذي ينهجه القرصان المعلوماتي و المجرم المعلوماتي، وفي نظرنا أنه في الأصل يلتقي المجرم التقليدي مع المجرم المعاصر الالكتروني أو مجرم الانترنيت أو القرصان السيبراني والمعلوماتي في مصير واحد، بحيث أن الصيرورة هي نفسها, فالمجرم التقليدي الذي كون لنفسه عالما إجراميا وأحترف الجريمة المنظمة في شكل جماعة، تطور مع الزمن والوقت وصادف التطور التكنولوجي الهائل في حين ان الاستخدامات الكثيرة

لوسائل متطورة وأجهزة عالية الدقة منصهرة مع عالم الانترنيت وهو ما أنتج ما يعرف الأن بالجريمة المعلوماتية أو السيبرانية وما إلى ذلك من مصطلحات خارقة ومنفتحة على تطور أكبر, وتتعدد مجالات الخروقات عبر شبكات الانترنيت وكذا الفضاء السيبراني وذلك باختلاف نوع الجرائم، سواء كانت: جرائم الاتجار في المخدرات، وغسل الأموال وتزويرها وصك العملات والإتجار بالبشر وسرقة الاعمال الثقافية والفنية وتهريبها، وجرائم المعلومات (الجرائم الإلكترونية) والإتجار غير المشروع في المواد البيولوجية والنووية، بالإضافة الى الأسلحة النارية، وانشطة الارهاب. (إسراء أحمد إسماعيل 2011)

وإذا أقمنا مقارنة في ميزان الاستعمال التكنولوجي لتكنولوجيات الاعلام والاتصال (الانترنيت والشبكات والتطبيقات المتفرعة المستخدمة للأنترنيت وجهاز الحاسوب) فان الفرق يكون كبيرا بين مجرمي عالم الجنوب الضعيف ومجرمي عالم الشمال ومنطقة أسيا، الذين يبرزون في التفوق الكبير في ميدان إستعمالالتكنولوجيا الإعلامية والاتصالية، والانترنيت , فمثلا فيما يخص الأجهزة و الوسائل المحيطة بعالم الانترنيت نجد أن أروبا تمتلك ما عدده : 450 من الكابلات العابرة للقارات عبر مياه المحيطات و 3 ملايين محطة لتخزين المعلومات بالإضافة لمحطات و مراكز إحتياطية قائمة دائما من أجل ضمان تدفق خدمة الانترنيت , و كذلك طرق سيارة رقمية للإتصالات التي تغطي سطح المعمورة , و كذلك تثبيت محاور المحيط الأطلسي و الهادي . (GUILLAUME PITRON–hiver 2021–2022)

وهو ما يعطي إنطباعا بأن نوعية الجرائم المنظمة في الوطن العربي، جرائم ليست بحاجه لقدرات علمية كبيرة مثل عمليات التهريب وجرائم المخدرات (إيهاب خليفة 2021) . وكذا انخفاض جرائم الفضاء السيبراني في العالم الاسلامي والعربي والافريقي، واصبحت النتيجة بحد ذاتها تحمل نتيجتين وطموحين متناقضين فأحد أوجه العملة ايجابي بانخفاض الجريمة المنظمة والمعلوماتية في عالم الجنوب السائر في طريق النمو، والثاني وجه سلبي ينبئ بتخلف عالم الجنوب النامي، وعدم امكانيته اللحاق بركب الحضارية المادية والتقنية التي عرفتها الحضارة الغربية، (اوروبا وامريكا الشمالية، واسيا : الصين واليابان، كوريا الجنوبية، سنغافورة، وماليزيا، وعموما الدول المنظوية في منظمة الأسيان (دول جنوب شرق اسيا) بالإضافة الى روسيا، تركيا، وايران.

ويضاف الى محور الامن القومي والمنظومة القانونية والسياسية التي تعدادها الدول الموقوف امام خطورة الجرائم المعلوماتية – السيبرانية، وهو الامر الذي لا يمكن ان يتحقق في ضل عدم تمكن الدول القومية (الوطنية) من امتلاك العناصر القوى اللازمة لتحقيق الانتصار في حالة الحرب، وذلك يهدف الحفاظ على بقائها ولتحقيق اهدافها وبسط نفوذها وردع اعدائها[1]. ومن اجل السيطرة وتحقيق سواء في الحروب او في الحفاظ على سيادة الدولة على اراضيها، واذا كانت مجلات التكنولوجية قد تطورت كثيرا والى درجة التعقيد في بعض المجالات، فان السيطرة التكنولوجية الحديثة والمعاصرة اصبح ظاهرها بل مجالاتها اغلبها السيبراني – غير تقليدي – تلعب اوراقه في فضاءات ومعارك سيبرانية فضائية، أدواتها الانترنيت وأجهزة الحواسيب، وتحولت وتغيرت الوسائل والاسلحة المستعملة في الحروب من السيوف والبنادق سابقا تباعا، الى المواجهة المباشرة بين جنود الاطراف المتخاصمة والمتحاربة الى القتال عن بعد عبر الدرونز– الطائرات بدون طيار. والروبوتات . (إيهاب خليفة 2021)

وهي نفس التكنولوجيا التي احدثت فوارق كبيرة بين الاسلحة التقليدية والمعاصرة والحديثة، وان كانت من نفس النوعية والاستخدامات، فأصبحت تلك المدافع والطائرات والغواصات والفرقاطات والدبابات والمدرعات التي يتم تحديثها وادخال برمجيات الكترونية حديثة، اكثر فكتا وتطورا وفعالية بالمقارنة مع نفس الوسائل والاليات التقليدية في سابق عهدها، فتوجه الدول لبناء المدن

الذكية والاعتماد على التقنيات الرقمية في ادارة كافة شؤون الحياة اليومية سواء الاقتصادية او السياسية او الاجتماعية او الإعلامية او الصحية فان معدلات بناء القوة وتحقيق النفوذ تتغير فلم تعد مساحة الدولة بعد سكانها عنصر للقوة كما كانت على مر التاريخ، حيث يمكن لدولة صغيرة الحجم قليلة السكان، بالعلم والابتكار، ان توقع خسائر فادحة بدولة كبيرة الحجم كثيفة السكان. (إيهاب خليفة 2021)

مجالات استعمال القوة والنفوذ السيبرانيين:

ويتضح ذلك من خلال تفحص افكار المفكر الأمريكي "جوزيف ناي"من خلال القول بان "الفضاء السيبراني لن يزيل وجود الدولة أو يغير حدودها الجغرافية، أو يذهب ويقضي على السيادة الوطنية للدولة على مجالها الحيوي تماما، وإنما سوف يؤثر سلبا على نفوذ هذه الدولة ويغير مفهومها ورؤيتها للأمن القومي ومصلحتها الوطنية، وذلك من خلال:

1-قدرة الدولة للحفاظ على سيطرتها على مجالها الحيوي، وذلك من خلال التأثير على سلوكيات الاطراف الخصوم أو المنافسة، وإمكانية قياس درجة منافستهم لهذه الدولة، كما يستوجب على الدولة المعنية بالمحافظة على سيادتها إستشعار خطر الجماعات الإرهابية المستعملة للفضاء السيبراني الواسع. فعلى سبيل المثال تعرضت استونيا سنة 2007 إلى هجمات سيبرانية إستهدفت بنيتها المعلوماتية، كما تم إستخدام القوة االسيبرانية من أجل التعرض وإستهداف القوة الصلبة لدول اخرى، من خلال نشر فيروسات تدمر أجهزة الدولة الخصم أو العدو،أو تستهدف نظم الكمبيوتر الخاصة بالخدمات الحكومية (إيهاب خليفة 2021)

1- قدرة الدول صاحبه النفوذ الدولي، على التأثير والتحكم في سلوكات الدول الاخرى سبرانيا.

قدرة الدول من حيث ترتيب أولويات الأطراف الدولية الأخرى ومن أمثلة ذلك في باب ممارسة القوة الصلبة: قيام بعض الدول، مثل الصين والسعودية بحجب بعض المواقع ونزع شرعياتها لدى المواطنين، وترك مواقع أخرى وقيام الولايات المتحدة باتخاذ عدة إجراءات ضد شركات بطاقات الائتمان لمنع ممارسة القمار عبر الانترنيت ومنأمثلة القوى الناعمة العمل على نشر أو تقييد قيم وثقافات عبر الانترنت مثل تطوير قيم رافضة لنشر الإباحة عبر الانترنيت . (إيهاب خليفة 2021)

2-إن تطور الجرائم الالكترونية (السيبرانية) حتم على المشرع الوطني أن يسن قوانين لمواجهة الأخطار والتحديات التي يفرزها هذا الفضاء السيبراني، وكون القاضي الجنائي مقيد بنصوص قانونية على رأسها" لا جريمة ولا عقوبة إلا بنص" وأمام القاضي الجنائي الاستفاقة سواء من خلال الاستعانة بقانون خاص محدد للجرائم المعلوماتية. أو حتى تلك النصوص الموجود في قانون العقوبات الجزائري الذي يعطي حماية للأموال، وضمن هذه الفكرة، صدر أول قانون جزائري ينظم المعلوماتية ويحميها من أي خطر.

وأول ما أصدره المشرع الجزائري في هذا المجال هو القانون رقم:01-09-المؤرخ في 26 جوان 2001. (عبد الكريم نعمان 2016-2017).

وذلك في المادتين 144 مكرر و144 مكرر1،وقد جاء هذا القانون ثمرة الاتفاقيات الدولية والمعاهدات وكذلك النصوص التشريعية الدولية الإقليمية المحلية السابقة، التي كانت كلها تسعى لحماية المجال (المعلوماتي) أو كل ما له صلة بعالم الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وأهم المعاهدات والاتفاقيات التي أبرمتها الجزائر وما تمخض عنها من نصوص وتشريعات: (عبد الكريم نعمان 2016-2017).

أما بالنسبة للاتفاقيات والمعاهدات الدولية التي انضمت إليها الجزائر وصادقت عليها نجد: (عبد الكريم نعمان 2016-2017)

– اتفاقية باريس لحماية الملكية الصناعية والاتفاقية الدولية حول حقوق المؤلف لسنة 1952 والتي تمت مراجعتها في باريس في 24 جويلية 1971 والتي جاءت بعد ذلك تحت رقم: 73–26 بتاريخ 5 جويلية 1973. وكذلك اتفاقية إنشاء المنظمة العالمية للملكية الفكرية التي تم انعقادها وإمضاؤها في ستوكهولم بتاريخ: 14 جويلية 1967 واتفاقية برن لحماية المصنفات الفكرية والأدبية وقد تم ذلك بمرسوم رئاسي تحت رقم: 97–341 المؤرخ في 13 سبتمبر 1997. وتمكن الإشارة إلى أن الجزائر لم تنضم لحد الآن إلى الاتفاقية الدولية المسماة:إتفاقية بودابست المنشأة بتاريخ: 23 نوفمبر 2001. والتي سميت بالاتفاقية الدولية لمكافحة الجريمة الالكترونية " convention on cyber crime " وهي بين الدول الأوروبية والأمريكية والأسيوية ويرجعسبب تأخر الجزائـر على التصديق على هذه الاتفاقية هو تحفظها على المواد المتعلقة – بدعارة الأطفال، والأخلاق، غير أنه من جانب أخر انضمت الجزائر إلى الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، ووقعت عليها بتاريخ: 21 ديسمبر 2010، وقد تم انعقاد أشغال هذه الاتفاقية بمقر الجامعة العربية – بالقاهرة. وضمت هذه الاتفاقية 22 دولة عربية وضمن الاتفاقية 43 مادة محررة باللغة العربية.

– كما صادقت الجزائر على اتفاقية مكافحة وتمويل الإرهاب، وكذا المصادقة على الاتفاقية العربية لمكافحة الفساد المحررة بالقاهرة، وكذلك الاتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود المنعقدة والممضاة في القاهرة وبنفس التاريخ.

وخلاصة لما جاء في سرد هذه النصوص التشريعية الدولية والمحلية (الوطنية)، نقولإن الجانب القانوني أو المنظومة القانونية لمقاومة ومكافحة أي ضرر يصدر من جانب الأخطار التي تصدر عن القضاء السيبراني الذي يمكن أن يمس بسلامة أمن الوطن من حيث عالم التكنولوجيا والحاسوب قد تمت عملية التصدي لهذه الأخطار من حيث التصدي لها من خلال المصادقة على الاتفاقيات والمعاهدات الدولية، أو من خلال سن القوانين والتشريعات الوطنية. فبالإضافة إلى القانون 15.04 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم لقانون العقوبات فلقد تضمن القانون 04.09 المؤرخ في: 05 أوت 2009 الخاص بمكافحة الجريمة الالكترونية. والذي تضمن القواعد الخاصة بتحديد الجرائم المتصلة بتكنولوجيات الاعلام والاتصال. وكيفية حماية المنظومة المعلوماتية الوطنية من القرصنة والتخريب.

حدود تدخل النصوص التشريعية لحماية الثوابت الوطنيةمن الأخطار المنجرة عبر الفضاء السيبراني.

إن تطور الوسائل الالكترونية، أنجر عنه ظهور الكثير من الأخطار والتحديات مست جوانب الثوابت الوطنية، وهو ما تصدت له التشريعات الوطنية من خلال القانون رقم 01–09. المؤرخ بتاريخ 26 جوان 2001 وذلك

المواد: 2001–09–المؤرخ في 26 جوان 2001 المذكور. والمحتوى الثاني " تطبق على الاهانة أو السبب أو القذف الموجه بواسطة الوسائل التي حددتها المادتان 144 مكرر و144 مكرر[1]. والمتعلقة بجريمة القذف والسب والاهانة إلى رئيس الجمهورية، وهذا بالتحديد ف ي النص التالي " كل من أساء إلى رئيس الجمهورية بعبارات تتضمن اهانة أو سب أو قذف، سواء كان ذلك عن طريق الكتابة أو الرسم أو التصريح أو بأية آلية لبث الصوت أو الصورة أو بأية وسيلة الكترونية أو معلوماتية أو إعلامية أخرى".

كما أشارت المادة 144 مكرر 2 الى تحريم كل من يقوم بـ " الإساءة إلى الرسول (ص) أو بقية الأنبياء أو استهزأ بالمعلوم من الدين بالضرورة أو بأية شعيرة من شعائر الإسلام سواء عن طريق الكتابة أو الرسم أو التصريح أو بأية وسيلة أخرى أو ضد الهيئات العمومية".

وأهم شيء ميز هاتين المادين بين قانون العقوبات الجزائري. هو نص المشرع الجزائري على: " أو بأية وسيلة إلكترونية أو معلوماتية أو إعلامية أخرى".

وتأكدت هذه التحديات في قانون العقوبات المعدل والمتمم رقم 04-15 المؤرخ في 10 نوفمبر 2014 والذي ركز على مصطلح: المساس بأنظمة المعالجة الآلية للمعطيات – وذلك من خلال المواد – 394 مكرر إلى 394 مكرر 7.

وقد واكب المشرع الجزائري أهم التطورات في عالم التكنولوجيا، بحيث قام بتعديل قانون العقوبات السالف الذكر، لسنة 2004، وبعده 2009 وبعد ذلك عدله في سنة 2016، وذلك بمقتضى القانون رقم 2016 " المؤرخ في 19 جوان 2016، بحيث ركز على تعديل المواد 87 مكرر و11 و87 مكرر 12. والمادة 394 مكرر 8، وهو القانون الذي يشمل 19 مادة قانونية حول الموضوع موزعة على 6 فصول ويعتبر هذا القانون مواكبة للطفرة الالكترونية أو التكنولوجية الكبرى التي عرفها الفضاء السيبراني cyberespace. بحيث تتم فيه كل التبادلات للمعلومات الرقمية. ما يعتبر مسرحا للجريمة الالكترونية. فهذا المسرح تقوم فيه كل المعاملات والخدمات الالكترونية من حيث التجارة الالكترونية الافتراضية والتوقيع.

و من أجل التصدي للجريمة السيبرانية – المعلوماتية – و إلى جانب هذه الترسانة الكبيرة من القوانين و المراسيم قامت السلطات العمومية بوضع استراتيجية محكمة من خلال إنشاء فرق أمنية تقنية متخصصة في الجريمة الالكترونية والتي كانت مهمتها هي مراقبة الأعمال و" الأنشطة المشبوهة على مدار الساعة والتعامل بفاعلية مع البلاغات التي تصلها بشكل سمح بإفشال نشاط عشرات الخلايا الإرهابية في ظرف قياسي، إذ قررت القيادة العليا للأمن الوطني استحداث مخابر وخلايا مختصة في مكافحة الجريمة الالكترونية، فقد تدعمت المديرية العامة للأمن الوطني سنة 2010 بما يقارب 23 خلية لمكافحة الاجرام الالكتروني بكل أنواعه. (عتيقة كواشي 2023)

هذا من جانب الحماية والمخطط الوطني لمكافحة الجريمة المعلوماتية – السيبرانية – فإن السلطات العمومية، وفي إطار التعاون الدولي، قامت الدولة الجزائرية بالانضمام إلى الاتفاقية العربية لمكافحة جرائم تقنية المعلومات في ديسمبر 2010.

كما انضمت الجزائر إلى " اتفاقية بارن" الأوروبية لحماية المصنفات الأدبية والفنية والاتفاقية العالمية لحقوق المؤلف والمراجعة. (عتيقة كواشي 2023) ومثلما قامت الجزائر بإستحداث مصالح و خلاليا لمجابهة الجرائم السيبرانية يمكن الإشارة إلى بعض المبادرات و الإجراءات و كذا الاحتياطات التي قامت بإنجازها و تحضيرها بعض الدول، فيمكن الاستعانة و الإشارة إلى ما قامت به دولة فرنسا، أين اعتبرت من سنة 2013 و في زمن وزير الدفاع الفرنسي السابق : " جون غيف لو دريون " برسم الخطوط الكبرى من خلال" فصول الكتاب الأبيض للأمن", اين رتب موضوع الحمائية للفضاء السيبراني الفرنسي وجعل الامر في مقدمة الأولويات , وتم ترجمة هذا الاهتمام إلى تحديد 50 (خمسون) إجراء و الذي تجسد فيما بعد في "قانون البرنامج العسكري" الخماسي (2014-2019) و الذي رصد ما قيمته : 01 مليار أورو لمجابهة الاخطار السيبرانية و هو الامر الذي يسمح بتوظيف 1000 (ألف) عون موجهين كلهم للتصدي لظاهرة الجرائم السيبرانية , و خصوصا في ميادين قيادة الأركان و المديرية العامة للجيش و كذا التوظيف في مصالح الاستخبارات . 11-3--- جون ايف لودريون ص 07... نفس المرجع السابق. و هو نفس التصدي و العمل الذي سارت فيه الحكومة الفرنسية في عهد وزيرة الدفاع فلورنس بارلي (Florence Parly) في سبتمبر 2021 , و من أجل تدعيم وسائل التصدي و الوقاية من الجرائم السيبرانية بتوظيف 1000 (ألف) إطار إضافي مختص في مجال السيبرانية , كمقاومين سيبرانيين , و الذين سوف يتصدون للمجرمين السيبرانيين – المعلوماتيين – , و هو ما يجعل العدد المستغل في مكافحة الجرائم السيبرانية يرتفع إلى 5000 (خمسة ألاف) عون . وهو ما يوضح بأن العدد شبه مهول هول الجرائم،وهذه الحرب الباردة في عالم الفضاء السيبراني. زيادة على ذلك فإن إنشاء الوكالة الوطنية الفرنسية لأمن نظم المعلومات

(ANSSI) والتي قامت بأعمال جليلة في مجال مكافحة والوقاية من الجرائم السيبرانية ومن ذلك فإنه وبين سنة 2017 على غاية خريف 2021 تدخلت الوكالة في أكثر من 50 تدخل أمني سيبراني في 2019،وفي حدود 200 تدخل عام 2020،وأمام هذه الأرقام يستشف أن هناك زيادة في عدد الجرائم السيبرانية،ومنه زيادة عدد التدخلات الرقمية،والتي زادت تبعا للجرائم السيبرانية المرتكبة في سنة 2021 وإلى غايةيومناهذا. (PITRON POLITIQUE 2021)

خاتمة:

في خاتمة هذه المقالة العلمية لا يسعنا إلا نسجل أولا ملخصا وجيزا لما جاء من محاور وأفكار فيها، وبداية لقد تم عرض أفكار هذه الخلاصة من خلال ثلاث محاور أساسية أين تعرض المحور الأول إلى الامن التقليدي ' مفهوما وتعريفا وكذا شرحا شبه واف لمفهوم الامن عموما وكذا الإشارة والتعرض للمفاهيم الأمنية الجديدة والمستحدثة. كما تم من خلال المحور الثاني التعرض على أهم التطورات التي دخلت على مفهوم الامن وذلك من خلال التطور الكبير في ميدان التكنولوجيا وخصوصا في جانبها المتعلق بعالم الانترنيت وكذا العالم السيبراني أو الرقمي أين أثر هذا التطور وأثر تأثيرا كبيرا في ميدان الحصول وتخزين المعلومات ولكن ليس بالطريقة التقليدية وإنما عن طريق الوعاء الافتراضي , أين قامت الكثير من الدول و منها الجزائر و كذا فرنسا و بعض الدول الأوروبية و منها النمسا التي تم ذكرها في هذه المقالة على عجل بصرف ميزانيات معتبرة من أجل تكوين أعوان متخصصين في الميدان السيبراني من أجل مواكبة التطور الكبير الحاصل في المجال الرقمي و منه القيام ببناء منظومات أمنية رقمية لحماية المجال الأمني القومي لهذه الدول من الأخطار التي يتسبب فيها القراصنة الرقميين أو السيبرانيين و الذين يتسببون من حين لأخر في إحداث أعطاب و تخريبات معلوماتية – سيبرانية – ضد مصالح هذه الدول و كذا

المساس بمصالح الافراد والمؤسسات الخاصة والعامة على السواء. وإلى جانب التدابير الفنية والتقنية التي تقوم بها الدول من أجل حماية فضاءاتها الرقمية – السيبرانية – فإن أغلب الدول الان إنضوت ضمن إتفاقيات دولية لمكافحة والوقاية من الأخطار التي تمس بالجوانب المادية والتقنية والسيبرانية الافتراضية لعالم الحاسوب والانترنيت مجتمعين. وهذه الاتفاقيات غالبا ما تؤكد على ضرورة التصدي لكل أشكال المساس بأنظمة المعلومات سواء التقنية أو الفنية والمعنوية، وذلك من خلال سن نصوص وتشريعات قانونية رادعة لكل أشكال التعرض لهذه الأنظمة المعلوماتية تبقى عملية تحيين القوانين الرادعة لهذه الأخطار المحدقة، مرافقة لكل التطورات التكنولوجية المسجلة في عالمنا هذا الكثير التطور والمفاجأة العلمية الخارقة. وأمام هذه الطفرة الكبيرة في الجانب العلمي والتكنولوجي يبقى المستقبل كفيل بتقديم أهم الإجابات العلمية ومعها أهم التشريعات القانونية والتي تبقى مرافقة حتمية لكل خطوة علمية من أجل حماية الانسان من ذاته ومن خياله وطموحه الذي لا حدود له.

هوامش المقال:

1- زيدان زيبحة، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى عين مليلة،الجزائر، 2011.ص 14.
2- عبد الله أحريك، الإرهاب السيبراني، التهديد الجديد لأمن الدول، الطبعة 22 , دار أدليس بلزمة للنشر و التوزيع , باتنة , الجزائر . ص 20.
3- عبد الوهاب جعيجع، الأمن المعلوماتي والعلاقات الدولية، منشورات دار الخلدونية. 2017 . ص 62.

4- مسيكة محمد، الفضاء السيبراني وتحديات الامن القومي للدول مجلة العلوم القانونية و الاجتماعية ' جامعة زيان عاشور الجلفة , المجلد السابع , العدد الرابع , ديسمبر 2022. الجزائر، ص 451.

5- مصباح عامر، نظريات التحليل الاستراتيجي والأمني للعلاقات الدولية، دار الكتاب الحديث، الجزائر , 2011. ص 09.

6- أحريق عبد الله، مرجع سبق ذكره. ص 25.

7- عبد الوهاب جعيجع، ص 11.

8- عبد الوهاب جعيجع، مرجع سابق. ص 61.

9- عبد الوهاب جعيجع، مرجع سبق ذكره. ص 66.

10-تحليل الفاعلين العنيفين من غير الدول في المراحل الانتقالية (مجلة ملحق السياسة الدولية، عدد أفريل 2013 رقم 192) القاهرة، مصر، ص. 11.

11-عبدالوهاب جعيجع،مرجع سابق. ص 67.

12-محمد بسيوني عبد الحليم، ملحق السياسة الدولية، أدوار الإعلام العابرة للقومية في مجتمعات مابعد الثورات، العدد 192 أفريل 2013 ,المجلد 48 , القاهرة , مصر , ص. 33.

13-محمد بسيوني عبد الحليم ملحق السياسة الدولية، أدوار الإعلام العابرة للقومية في مجتمعات ما بعد الثورات، العدد 192 أفريل 2013، المجلد 48،القاهرة،مصر. ص34.

14-Eric Mechoulan,opcité, p .278

15 – مسيكة محمد، الفضاء السيبراني وتحديات الامن القومي للدول مرجع سابق، ص 451.

16-مسيكة محمد، نفس المرجع، ص. 454.

17-جعيجع عبد الوهاب، مرجع سابق. ص 66.

18- Eric Mechoulan ; politique internationale, n 170 ; 2020-2021 ; Paris ; France. P.277

19-Eric Mechoulan , politique internationale, n 170 ; 2020-2021, IBID

20-جعيجع عبد الوهاب، مرجع سابق، ص 67.

21-طالة لامية، الإرهاب السيبراني والامن القومي: قراءة في تحولات الاستراتيجية الدفاعية، حوليات جامعة الجزائر1، المجلد: 35 / العدد: 04 -2021، ص 353.

22 -JEAN YVES LE DRIAN، CYBER DEFENSE ETCYBERGUERRE, REVUE DEFENSE NATIONALE –NOVEMBRE 2015، P 05.PARIS,France.

23-JEAN YVES LE DRIAN، CYBER DEFENSE ETCYBERGUERRE، REVUE DEFENSE NATIONALE NOVEMBRE 2015, OPCITE, P.06

24- CHATTON NICOLAS MAZZUCHI, CYBER DEFENSE ET CYBERGUERRE, REVUE DEFENSE NATIONALE –NOVEMBRE 2015, P 32

25-Eric Mechoulan, LE JEU DANGEREUX DES GEANTS DU NET, politique internationale, n 170 ; 2020-2021, OPCITE,Paris ; France .p.280.

26-طالة لامية، حوليات جامعة الجزائر1، مرجع سابق، ص 354.

27–علي زياد العلي، الصراع والأمن الجيوسيبراني في السياسة الدولية " دراسة في استراتيجيات الاشتباك الرقمي "، دار أمجد للنشر والاشهار الأردن , 2019.ص 114

28 –علي زياد العلي، الصراع والامن الجيوسيبراني، مرجع سابق، ص 122.

29 –علي زياد العلي، الصراع والامن الجيوسيبراني، مرجع سابق، ص 125.

30–معيزي ليندة، دهقاني أيوب، تأثير الفضاء السيبراني على الامن المجتمعي–مواقع التواصل الاجتماعي نموذجا، المجلة الجزائرية للأمن والتنمية، المجلد 12/العدد 02 أفريل 2023. ص 162.

31–نفس المرجع والصفحة.

32-Eric Mechoulan,Politique internationale, n 170 ; 2020-2021 ; Paris –P 281

33-Thierry Burkhard , UN NOUVEAU CONCEPTE STRATEGIQUE POUR DE NOUVELLES MENACES, politique internationale, n 174 –hiver 2020-2021, Paris, France ,P 214.

34- POUPARD GUILLAUME, .GUERRE FROIDE DANS LE CYBERESPA, POLITIQUE INTERNATIONALE N .173. AUTOMNE 2021, PARIS, France. P 243

35–محمد مسيكة، الفضاء السيبراني وتحديات الامن القومي للدول، مجلة العلوم القانونية والاجتماعية، المجلد السابع، العدد الرابع، السنة ديسمبر 2022، جامعة زيان عاشور، الجلفة، الجزائر، ص 458.

36–نفس المرجع، ص 459.

37–معيزيليندة،دهقانيأيوب، تأثير الفضاء السيبراني على الامن المجتمعي–مرجع سابق. ص 162.

38–المصدر وكالة الأنباء الجزائرية، صفحة، علوم–التكنولوجيا، الدخول يوم الأربعاء، الساعة 16:49 من يوم 21فيفري 2024.

39-GUILLAUME PITRON , POLITIQUE INTERNATIONALE , N 174 ; P. 244 .PARIS , France

40–قانون العقوبات الصادر بموجب الامر رقم 66–156 مؤرخ في 8 يونيو 1966 (جريدة رسمية رقم 49 المؤرخة في 11–06–1966) معدل ومتمم –بالقانون رقم 16–02–المؤرخ في 19 يونيو سنة 2016 (ج ر 37 مؤرخة في 22 يونيو 2016) ومحين بالقانون رقم 21–14 الصادر بتاريخ 28 ديسمبر 2021(ج ر العدد 99 الصادرة بتاريخ 29 ديسمبر 2021).

41–إسراء أحمد إسماعيل، الجريمة المنظمة وتحديات الأمن الانساني في المنطقة العربية، مجلة ملحق السياسة الدولية، عدد أكتوبر 2011، رقم 186، القاهرة، مصر، ص 13.

42–نفس المرجع والصفحة.

43 - GUILLAUME PITRON ; POLITIQUE INTERNATIONALE ; N 174 ; P. 229. PARIS ; France.

44–مجلة ملحق السياسة الدولية، إسراء أحمد اسماعيل، مرجع سابق والصفحة.

45–إيهاب خليفة، الحرب السيبرانية والاستعداد لقيادة المعارك العسكرية في الميدان الخامس، العربي للنشر والتوزيع، 2021، ص61

46–إيهاب خليفة، مرجع سابق، نفس المرجع ونفس الصفحة.

47–إيهاب خليفة، مرجع سابق، ص69.

48–إيهاب خليفة، مرجع سابق، ص70.

49––عبد الكريم نعمان، الجرائم الالكترونية وموقف المشرع الجزائري منها، رسالة ماجستير، كلية الحقوق، بن عكنون، جامعة الجزائر 1 , 2016–2017. ص 170.

50–نفس المرجع الصفحة. 171.

51–نفس المرجع والصفحة

52–كواشي عتيقة، تداعيات الإرهاب السيبراني على الامن القومي الجزائري للأمن والتنمية ، المجلد 12/العدد 03/جويلية 2023/ ص: 211.

53–نفس المرجع، الصفحة 213.

54- GUILLAUME PITRON، POLITIQUE INTERNATIONALE، N 173، opcite.P.244