جامعة قاصدي مرباح ورقلة

كلية الحقوق و العلوم سياسية

قسم العلوم سياسية

مذكرة تخرج لاستكمال متطلبات نيل شهادة الماستر في ميدان الحقوق و العلوم السياسية

شعبة : العلوم السياسية

تخصص : دراسات أمنية و استراتيجيه

بعنوان :

إستراتيجية تطوير الأمن السبيراني في الجزائر على ضوء تقارير الإتحاد الدولي للاتصالات السلكية واللاسلكية

من إعداد الطالب :

عمار بداي

الأستاذة المشرفة :

د. فريدة طاجين

أعضاء لجنة المناقشة

إسم ولقب الأستاذ	الصفة
د باسماعيل عبد الكريم	رئيسا
د/ طاج ن فريدة	مشرفا
د خميس محمد	مناقشا

السنة الجامعية 2020/ 2021

جامعة قاصدي مرباح ورقلة

كلية الحقوق و العلوم سياسية

قسم العلوم سياسية

مذكرة تخرج لاستكمال متطلبات نيل شهادة الماستر في ميدان الحقوق و العلوم السياسية

شعبة : العلوم السياسية

تخصص : دراسات أمنية و استراتيجيه

إستراتيجية تطوير الأمن السبيبراني في الجزائر على ضوء تقارير الإتحاد الدولي للاتصالات السلكية واللاسلكية

من إعداد الطالب :

عمار بداي

الأستاذة المشرفة :

د. فريدة طاجين

أعضاء لجنة المناقشة

إسم ولقب الأستاذ	الص فة
د باسماعيل عبد الكريم	رئيسا
د/ طاجين فريدة	مشرفا
د/ خميس محمد	مناقشا

السنة الجامعية 2020/ 2021

الشكر والتقدير

الحمد لله رب العالمين، و الصلاة و السلام على اشرف المرسلين سيدنا محمد و على آله و صحبه أجمعين

أما بعد .....

الشكر لله أولا، بتوفيقي في إنجاز هذا العمل، و لا يسعني في هذا المقام إلا أن أتقدم بجزيل الشكر و التقدير إلى الدكتورة المشرفة فريدة طاجين التي تكرمت بإشرافها علي و توجيهي في إثراء معارفي، و ما قدمته لي من نصائح و توجيهات لاستكمال هذه المذكرة.

كما أتقدم بالشكر و التقدير لكل أساتذة قسم العلوم السياسية بجامعة قاصدي مرباح ورقلة، و إلى كل عمال و عاملات الكلية، و كل زملائي و زميلاتي في الدفعة، و كل من ساعدني في الحصول على المعلومات، من قريب أو من بعيد بالقليل أو بالكثير.

و الله ولي التوفيق

عمار

الإهداء

أهدي هذا العمل إلى :

من كان سببا في وجودي في هذه الحياة الوالدين الكريمين

إلى الزوجة الكريمة و ابني الغالي و كذا كل أفراد عائلتي

إلى كل من ساعدني من قريب أو بعيد لإتمام هذا العمل

إلى كل هؤلاء أهدي هذا العمل و أرجو من الله العلي القدير أن يوفقنا لما فيه خير لنا و صلاح أمرنا و استقامة نهجنا إنه قريب مجيب الدعاء

عمار

ملخص الدراسة :

إن الهدف المرجو من الدراسة التي بين أيدينا هو توضيح أه ية وجود إستراتيجية وطنية للدول في مجال الأمن السبيراني، و الذي هو جزء لا يتجزأ من أمنها القومي، و هو ما حاولت الدراسة إسقاطه على الجزائر و إبراز مدى نجاعة الإستراتيجية معتمدة من طرف صانعي القرار لهذا الشأن و لقد اعتمدت الدراسة على مجموعة من المقاربات و النظريات الأمنية و التي عالجت موضوع الأم ، خاص ة في ظل التحولات التي عرفها المص طلح في هذا الشأن في العقود الأخير .

و من بين الأهداف الرئيسية للدراسة هو أيضا محاولة م رفة مدى مواكبة كل خطوات التي اتخذتها الجزائر في هذا الخصوص للتطورات الحاصلة في مجال ت نولوجيا ا علام و الاتصال عموما، و مجال التهديدات السبيرانية على وجه الخصوص و التي تهدد الأمن القومي الجزائري في كل مرة، و بالتالي فمن المهم هنا معرفة المكانة و المرتبة التي تح ها من بين باقي الدول خاصة و إن لدراسة ا تمدت على ؤشرات تقارير الاتحاد دولي للإ صلات السلكية و السلكية باعتباره هيئة دولية تابعة لمنظمة الأمم المتحدة.

الكلمات المفتاحية : الأمن القومي، الأمن السبيراني، التهديدات السبيرانية، الأمن القومي الجزائري، الإستراتيجية الجزائرية، الاتحاد الدولي للاتصالات السلكية و اللاسلكي ، سياسات ا تحاد الدول للإتصالات السلكية واللاسلكية .

Abstract:

The desired goal of the study before us is to clarify the importance of having a national strategy for countries in the field of cyber security, which is an integral part of their national security, and this is what the study tried to drop on Algeria and to highlight the extent of the effectiveness of the strategy adopted by decision makers in this regard The study relied on a set of approaches and security theories that dealt with the issue of security, especially in light of the transformations that the term has known in this regard in recent decades.

Among the main objectives of the study is also an attempt to know the extent to which all the steps taken by Algeria in this regard keep pace with the developments in the field of information and communication technology in general, and the field of cyber threats in particular, which threaten the Algerian national security every time, and therefore it is The important thing here is to know the position and rank it occupies among the rest of the countries, especially since the study relied on the indicators of the reports of the International Telecommunication Union as an international body affiliated with the United Nations.

Keywords : National Security; Security of Spain; Threats of Algeria; National Security of Algeria; Algerian Strategy; International Telecommunication Union; Policies of the International Telecommunication Union.

Résumé de l'étude :

Le but de l'étude qui est devant nous est de clarifier l'importance de l'existence d'une stratégie nationale pour les États dans le domaine de la sécurité, qui fait partie intégrante de leur sécurité nationale. C'est ce que l'étude a tenté de dire à propos de l'Algérie.

L'un des principaux objectifs de l'étude est également d'essayer de déterminer dans quelle mesure les mesures prises par l'Algérie à cet égard sont conformes à l'évolution dans le domaine des technologies de l'information et de la communication en général et en particulier dans le domaine des La sécurité nationale algérienne à chaque fois. Il est donc important de connaître le statut et le statut des autres États, d'autant plus que l'étude était basée sur les indicateurs des rapports de l'Union internationale des opérateurs de fil et de fil en tant qu'organisme international des États-Unis.

Mots clés : Sécurité nationale; Sécurité de l'Espagne; Menaces de l'Algérie; Sécurité nationale de l'Algérie; Stratégie algérienne; Union internationale des télécommunications; Politiques de l'Union internationale des télécommunications.

مقدمة

يشكل موضوع الأمن السبيراني واحدا من أكثر المواضيع التي تلقى رواجا في وقتنا الحالي وليس ضمن دراسات الباحثين والدارسين فقط، بل وكذا كثير من المهتمين الذين يحاولون التغلغل أكثر فأكثر في صلب هذا الموضوع الذي أضحى يؤثر على الحياة العامة للبشرية جمعا ، إذ أن هؤلاء يسعون دائما سواء كانوا دولا أو هيئات أو كيانات أخرى من أفراد وجماعات للعيش في كنف الأمن والسلم بعيدا عن التوترات والأزمات التي تهدد وجودهم وحياتهم على وجه المعمورة، وبالتالي تجلت مسألة التهديدات السبيرانية المتتالية و المتسارعة في العقود الأخيرة كخطر يتربص بكل البشرية ولا يمكن لأي دولة أن تعيش في منء عن هذا الخطر، وكنوع مستحدث من الأخطار التي تهدد وجود مصطلح الأمن الذي كنا نعرفه سابقا.

ولذا فإن الهدف من الاهتمام ومعالجة موضوع الأمن السبيراني خاصة فيما يخص حالة الجزائر هو معرفة مدى ا هتمام والأهمية التي يوليها صانع القرار لهذا الشأن، وهل هنالك سياسات أو استراتيجيات معتمدة ومدى نجاعتها وتجاوبها إن وجدت مع التقارير والمؤشرات التي يضعها الإتحاد الدولي للاتصالات السلكية واللاسلكية باعتباره هيئة دولية تابعة للأمم المتحدة مختصة في معالجة ه ا الموضوع بصفة خاصة ومواضيع تكنولوجيا الاتصالات بصفة عامة.

ومن هنا وبناء على ما تقدم يمكننا طرح السؤال الرئيسي التالي:

إلى أي مدى تمكنت الجزائر من بناء إستراتيجية الأمن السبيراني وفقا لمؤشرات تقارير الإتحاد الدولي للاتصالات السلكية واللاسلكية؟

الأسئلة الف عية:

– كيف تؤثر التهديدات السبيرانية على الأمن القومي للدول؟

– ما هي الإستراتيجية المعتمدة من طرف الجزائر في مجال مكافحة التهديدات السبيرانية؟

الفرضيات البحثية:

– كلما أعتمد صانع القرار الإستراتيجي في الجزائر على أساليب فعالة في الوقاية من التهديدات السبير انية، كلما جنب ذلك البلاد اختراقات في أمنها القومي.

– كلما اهتمت الجزائر بالمؤشرات التقنية والتنظيمية وكذا بناء القدرات، كلما قلل ذلك من التهديدات السبيرانية.

أهمية الدراسة ومبررات اختيارها:

تكمن أهمية الدراسة في كون هذا الموضوع يسلط الضوء على ظاهرة من أهم الظواهر حساسية بالنسبة للأمن القومي للدول واستقرارها، وطبعا ذلك راجع إلى كيفية تعامل كل منها معه ألا وهو الأمن السبيراني،فكل دول العالم أصبحت اليوم معرضة للتهديدات السبيرانية، وهو ما يحتم وضع آليات أو سياسات أو حتى إستراتيجيات فعالة من أجل حماية حـ ودها ليس من عدو قد يخترق مجالها من الجو أو البحر أو البر، بل عن طريق المجال التكنولوجي الذي جعل العالم اليوم بمثابة قرية واحدة مكشوفة وتلاشت من خلال ذلك الحدود الطبيعية للدولة القومية.

أدبيات الدراسة:

حاول الباحث من خلال إعداد هذه الدراسة الاعتماد على عديد الدراسات العلمية السابقة سواء من خلال المقالات الموجودة في المجلات أو المداخلات العلمية التي تم تقديمها في بعض الملتقيات التي نظمت في مختلف الجامعات والمؤسسات، وخاصة التي اهتمت بدراسة موضوع الأمن السبيراني في الجزائر وسلطت عليه الضوء كظاهرة يجب أن ؛ قى مزيدا من الاهتمام انطلاقا من الواقع الراهن، على أمل تقديم دراسات علمية شاملة تعد أرضية ينطلق من خلالها صانع القرار أو المهتم بالشأن الجزائري نحو إحداث ثورة أو خلق نقلة نوعية في مجال أو موضوع الأمن السبيراني بما أنه شأن يهم كافة أطياف المجتمع الجزائري ؛ لعلنا نذكر من هذه الدراسات:

– رغدة البهي، الردع السبيراني: المفهوم والإشكاليات والمتطلبات، حيث عالجت الكاتبة في هذه الدراسة مدى قدرة نظرية الردع التلاؤم في مواجهة الهجمات السبيرانية من خلال تحديد مفهوم الردع السبيراني، و ثانيا تحديد أنواع الهجمات السبيرا ة، و كذلك إعطاء أمثلة واقعية لهذه الهجمات وقعت في دول معينة، و أخيرا وضع جملة من المتطلبات التي يمكن استعمالها لمواجهة هذه الهجمات.

– يوسف بوغرارة، الإستراتيجية الجزائرية للأمن والدفاع في الفضاء السبيراني، و التي عالجت دراسته إطارا مفهوماتي حول الأمن السبـ راني و الفواعل المرتبطة به و في الشق

الثاني عالجت الدراسة كل من الآليات القانونية و المؤسساتية التي وضعت في الجزائر من أجل مواجهة الجرائم السبيرانية .

– سمير بارة، الأمن السبيراني في الجزائر السياسات و الدفاع ، و هي دراسة نشرت للباحث في المجلة الجزائرية للأمن الإنساني سنة 2017، حيث عالجت جملة من المفاهيم خاصة بالأمن السبيراني و أبعاده، و كذلك عرجت للتهديدات السبيرانية و أنماطها من جهة، والمؤسسات الوطنية الرائدة في هذا الشلن بالجزائر وأهم القوانين والتشريعات المهيكلة لها من جهة ثانية و اختتمت هذه الدراسة بجملة من التوصيات في هذا الشأن.

– جمال بوازدية، الإستراتيجية الجزائرية في مواجهة الجرائم السبيرانية، التحديات والآفاق المستقبلية، حيث عالج الكاتب في دراسته هذه و بعد الإطار المفاهيمي لإستراتيجية الجزائرية في مجال الأمن السبيراني من خلال التطرق لها من الجـ نبين الداخلي و الذي عرج عليه الكاتب من زاوية جملة القوانين و التشريعات المخصصة لهذا الشق، و كذا الهيئات الوطنية التي تم وضعها لكي يكون لها دور الريادة في مواجهة أخطار الهجمات السبيرانية، و أما على المستوى الدولي من خلال آليات التعاون التي يمكن لصانع القرار الجزائري الاعتماد عليها مع دول و مختلف الهيئات و المنظمات سواء إقليمية أو دولية.

– منى جبور الاشقر، الأمن السبيراني : التحديات و مستلزمات المواجهة، و هي دراسة قدمت في اللقاء السنوي للمختصين في أمن وسلامة الفضاء السبيراني سنة 2012 بلبنان أين قدمت الباحثة ، فهوما للأمن السبيراني و تأثيره على الأمن القومي للدول و أخطاره و كذلك تعرضت على الأبعاد المختلفة لهذا المفهوم، و في الأخير قدمت الباحثة جملة من الآليات و الضوابط التي يجب إتباعها من أجل مواجهة التهديدات السبيرانية المختلفة.

و فيما يخص الدراسة المقدمة في هذا الخصوص فهي عبارة عن دراسة للسياسات و الاستراتيجيات الجزائرية في مجال الأمن السبيراني و آليات تطويرها بناء على مؤشرات تقارير الاتحاد الدولي للاتصالات للفترة الممتدة من 2015 إلى 2018، و في الأخير محاولة الخروج بجملة من التوصيات التي يمكن لصانع القرار الجزائري الاعتماد عليها مستقبلا.

مبررات اختيار الدراسة:

أ) الأسباب الذاتية: هذا راجع إلى الاهتمام الشخصي في دراسة موضوع الأمن السبيراني وما يشكله من قيمة ثابتة تفرضها إملاءات الواقع الحالي لواقع التكنولوجيا من جانب وتسليط الضوء على أساليب وطرق معالجة الموضوع من قبل صانع القرار في الجزائر من جانب أخر.

ب) الأسباب الموضوعية: يشكل هذا الموضوع أحد أهم المواضيع التي تهم الشأن العام لكافة الشعوب، وليس فقط لدارسي علم السياسة أو المهتمين بالشأن الأمني وحتى المولعين بالمجل التكنولوجي، بل هو يمس كافة أطياف المجتمع.

المناهج والأدوات البحثية المعتمدة ومبررات اختيارها:

- **المنهج الوصفي:** وهو عبارة عن طريقة من طرق التحليل التي يتم الاعتماد عليها في الشأن، وهو أيضا وسيلة يتم من خلالها أيضا وصف الظاهرة محل الدراسة، وهنا سنعتمد على المنهج من خلال وصف وتحليل واقع الأ ن السبيراني في الجزائر اعتمادا على التقارير والمؤشرات التي وضعها الإتحاد الدولي للاتصالات السلكية واللاسلكية.

حدود الدراسة:

تتمحور حدود الدراسة في نمطين هما حدود مكانية وزمانية، فبالنسبة للأولى فهي ترتكز أساسا حول دراسة واقع موضوع الأمن السبيراني في الجزائر وما يعرفه من تفاعلات بدءا من صانع القرار إلى الباحثين والدارسين وكذا المهتمين، ويضاف إلى ذلك حدود البيئة الخارجية ومالها من تأثير سواء كان إيجابي أو سلبي على الواقع الجزائري.

وأما فيما يخص الحدود الزمنية لدراسة الموضوع فهي تحدد أساسا في الفترة الم تدة من سنة 2015 إلى غاية يومنا هذا، انطلاقا من بداية الاهتمام المتزايد لدى الباحثين والدارسين الجزائريين والذي تزامن مع صدور مؤشرات تقارير الإتحاد الدولي للاتصالات السلكية واللاسلكية والذي ظهرت على إثره تصنيفات الدول والتي كانت الجزائر من ضمنها.

الفصل الأول

مدخل مفاهيمي

الأمن السيبراني

و الاتحاد الدولي

للاتصالات السلكية و اللاسلكية

في ظل التزايد المذهل للتهديدات السبيرانية التي تتعرض لها جل دول العالم و بصفة دائمة و متكررة، و كعنصر تهديد ليس لمنظومتها المعلوماتية فحسب، بل لأمنها القومي ككل أضحى لزاما على كل دولة أن تتخذ أو تتجند بكل مقوماتها من أجل اتخاذ جملة من التدابير الوقائية في مجال أمنها السبيراني.

ففي المبحث الأول من هذا الفصل سيتم التطرق لماهية الأمن الس يراني من خلال عرض مجموعة من ا ر ا ات المختلفة ل جموعة الكتاب و الباحثين في هذا الشأن وتوضيح أهم نقاط الاتفاق و الاختلاف في هذا المجال.

أما المبحث الثاني و بعد التعر ف على الأمن السبيراني فإننا سنحاول معرفة مدى حجم و كذا الانعكاسات التي تخلقها التهديدات السبيرانية على الأمن القومي للدول في ظل التطورات الحاصلة في هذا الشأن و تعدد أشكال العناصر المهددة لأمن و استقرار الدول.

و في المبحث الثالث فسيتم التحدث عن جهود ا تحاد الدولي للاتصالات السلكي و اللاسلكية في مجال معالجة موضوع الأمن السبيراني على اعتباره هيئة دولية تابعة للأمم المتحدة.

وختام هذا الفصل سيكون من خلال التعرض للمبحث الرابع الذي سيكون عبارة على معالجة تقارير الاتحاد الدولي للاتصالات السلكية و لاسلكية من خلال عرض المؤثرات الخمسة التي وضعها في هذا الشأن

المبحث الأول : تعريف الأمن السبيراني و أبعاده

يعطي الأمن تعريفات عديدة تنطلق من الإمكانيات العسكرية، مرورا بالحفاظ على استقرار النظام، وصولا إلى حماية القيم الجوهرية لمجتمع ما. لكن و بغض النظر عن تقارب أو اختلاف النظرات الفلسفية و السياسية إلى الموضوع، فإن الراسخ هو الخشية التي تبديها معظم الدول حاليا من تعرض أمنها القومي نتيجة الاعتداءات السبيرانية لا سيما و أن تقنيات المعلومات و الاتصالات قد رفعت منسوب الخطأ عبر إتاحتها مصادر جديدة متشبعة و ، تعددة و إمكانيات هائلة لتحقيق هذا الخطأ مقابل انخفاض نسبة المخاطر و إمكانات الانكشاف في جانب الجهة المعتدية و الدليل على ذلك هو التنسيق المتزايد بين

إدارات الأمن و الاقتصاد، إضافة إلى الترابط الذي يراه قادة العالم بين أمن الفضاء السيبري و الاقتصاد و الأمن القومي .

و تبرز لنا هنا عدة تـ ر ات في هذا الشأن و سنحاول التعرض إلى أهمها :

عرفته وزارة الدفاع الأمريكية على أنه جميع الإجراءات التنظيمية اللازمة لضـــمان حماية المعلومات بجميـــع أشـــكالها (الالكتر ونيـــة و الماديـــة مـــن مختلـــف الجـــرائم الهجماتالتخريب ، و التجسس و الحوادث.[2]

واعتبره الإعلان الأوروبي بأنه يعني " قدرة النظام المعلوماتي على مقاومة محاولات الاختراق أو الحوادث غير المتوقعة التي تستهدف البيانات.[3]

كذلك يعرفه أستاذ الاتصالات في جامعة كاليفورنيا " ريتشارد كمرر" على أن الأمن السيبراني هو مجموعة وسائل دفاعية من شأنها كشف و إحباط المحاولات التي يقوم بها القراصنة، و قد أيده في هذا الطرح الأستاذ " إدوارد أموروزو" الذي عرفه بأنه تلك الوسائل التي من شأنها الحد من خطر الهجوم على البرمجيات أو أجهزة الحاسوب أو الشبكات و تشمل تلك الوسائل الأد ات المستخدمة في مواجهة القرصنة و كشف الفيروسات ووقفها و توفير الاتصالات المشفرة.[4]

و هناك من عرفه على أنه وانطلاقا من أهدافه بأنه النشاط الذي يؤمن حماية الموارد البشرية و المالية المرتبطة بتقنيات الاتصالات و المعلومات و يضمن إمكانات الخد من الخس ر و الأضرار التي تترتب في حال تحقيق المخاطر و التهديدات، كما يتيح إعادة الوضع إلى ما كان عليه بأسرع وقت ممكن، بحيث لا تتوقف عجلة الإنتاج و بحيث لا تتحول الأضرار إلى خسائر دائمة.[5]

- قوي بوحنية، الامن السيبراني و الصيانة في المنظمات و الحكومات دراسة في المؤشرات و التطبيقات ، **مجلة مصداقية** ، المدرسة العليا العسكرية للإعلام والإتصال،المجلد 01 ، العد 01 ، ديسمبر 019 ، ص ص 49،50 .

- عنترة بن مرزوق و محي الدين حرشاوي، **الأمن السبراني كبعد الجديد للسياسة الدفاعية الجزائري** ، الملتقى الدولي حول سياسات لدفاع الوطني، يومي 30 31 جانفي 017! ، جامعة قاصدي مرباح ورقلة، ص 06 .

- نفس المرجع، ص 06 .

- جمال بوازدية، ا ستراتيجية الجزائرية في مواجهة الجرائم السبرانية التحديات والأفاق المستقبلية **مجلة العلوم القانونية والسياسية**، المجلد رق 0 ، العدد رقم 01 ، الجزائر، أفريل 019 ، ص 266 .

- سمير بارة، الأمن السيبراني في الجزائر: السياسات والمؤسسات > ، **المجلة الجزائرية للأمن الإ سان** ، العدد 04 ، الجزائر، جويلية 017 ، ص 257 .

كما عرفه الاتحاد الدولي للاتصالات السلكية و اللاسلكية في تقريره الصادر حول اتجاهات الإصلاح في الاتصالات لعام 2010 ـــ 2011 بأنه مجموعة من المهمات مثل تجميع وسائل و سياسات و إجراءات أمنية و مبادئ وجيهية و مقاربات لإدارة المخاطر و تدريبات وممارسات فضلى و تقنيات يمكن استخدامها لحماية البيئة السيبرانية و موجودات المؤسسات و المستخدمين .[6]

و يعرفه البعض أيضا على أنه " المجال الجديد الخامس للحروب الحديثة بعد البر و البحر و الجو و الفضاء الحقيقي، وهو يمثل جميع شبكات الألياف البصرية و الشبكات اللاسلكية، والفضاء السيبراني ليس للانترنت فقط و إنما شبكات أخرى كثيرة متصلة.[7]

تجدر الإ ارة إلى أن لفظة سيبار" يونانية الأصل" أعيد استخدامها في منتصف القرن العشرين مع مصطلح السيبرنيتيقية الذي يعني دراسة سيرورة مراقبة الاتصال عند الكائن الحي أو الآلة وظهر مصطلح سيبار أو الفضاء الالكتروني وفي كثير من المراجع " الفضاء السيبراني" مع ظهور الانتر ت وتعميم استخدام الرقمنة موازاة مع كم هائل من المصطلحات مثل "الفضاء الرقمي" "الدفاع الالكتروني" و "الهجوم الالكتروني" " الجريمة الالكترونية" و غيرها. في حين أن مصطلح الأمن السيبراني أو الالكتروني ظهر حديثا وهو يعني مجمل القوانين السياسية، النصوص، المفاهيم، و ميكانيزمات الأمن وطرق تسيير الأخطار و الممارسات التكنولوجية المتعلقة بتكنولوجيا المعلومات و الاتصالات المستخدمة لحماية الدول و المنظمات و الأشخاص. كما يعرف على أنه الحالة المرغوب فيها لعمل أنظمة المعلومات و الاتصالات و التي تمنحها القدرة على المقاومة و التصدي لكل ما ينجم على الفضاء السيبراني و الذي من شـــأنه أن يعرض المعلومات المخزنة أو المعالجة أو المنقولة للتلف أو التغيير أو التجسس.[8]

- منى الأشقر جبور، الأمن السيبراني: التحديات ومستلزمات المواجه ، اللقاء السنوي الأول للمختصين في أمن و سلامة الفضاء السيبراني ، المركز العربي للبحوث القانونية والقضائية، بيروت 7! 8 أوت 012 ، ص ؛ .

- ادريس عطية ، م انة الأمن السبراني في منظومة الأمن الوطني الجزائري ، **مجلة مصداقية** ، المدرسة العليا العسكرية للإعلام والإتصال المجلد الأول، العدد الأول، ديسمبر 019! ص ص 04 05 .

- رضوا - ج، الأمن السبراني أولوية استراتيجيات الدفاع **مجلة الجيش**،العدد 30، جانفي 016 ،ص 41

التعريف الإجرائي :

الأمن السيبراني هو عبارة عن مجموعة السياسات و الضوابط و الآليات التي تتخذها الهيئات المعنية سواء كانت دول أو حكومات أو منظمات أو مؤسسات في مجال حماية

مواردها البشرية كانت أو المادية من كافة أخطار التهديدات التي يمكن أن تمس شبكات الاتصال وأجهزة الحواسيب عبر أعمال القرصنة أو الاختراقات المتعددة للنظم التكنولوجية الحديثة، و التي يمكن أن تعرضها لا شويش أو اللف التام.

و من بين النظريات و المقاربات التي اهتمت بدراسة موضوع الأمن السيبراني فنجد نظرية الهاكطولوجيا وهي النظرية التي تدرس أي محاولة مقصودة ومتعمدة للحصول وجمع وبث معلومات غير متاحة ضمن الفضاء العام وسياقه دون الحصول على موافقة المصدر أي صاحب المعلومة ومن ثم نشرها من خلال وسائل الإعلا .[9] و أيضا نجد مفهوم الردع و الذي عرفه الجنرال أندريه بوفر" بأنه منع دولة معادية من اتخاذ قرار باستخدام أسلحتها أو بصورة عم منعها من العمل أو الرد إزاء موقف معين باتخاذ مجموعة من التدابير و الإجراءات التي تشكل تهديدا كافيا حيالها و النتيجة التي يراد الحصول عليها بواسطة التهديد هي نتيجة سيكولوجية .[10]

و قد اهتمت مدرسة كوبنهاغن مفهوم الأمننة و الذي يمثل إطارا يمكنه أن يكون مثمرا من خلال دعواته إلى تحديد آليات أساسية خلف إعلان الأمن في مجموعة متنوعة ن القطاعات، وتجدر الإشارة إلى انه حتى الآن لم يتم استغلال إمكانيات هذا المفهوم التحليلية بشكل مثل لاستكشاف الكيفية التي تتشكل من خلالها السياسات التي تحاول معالجة الظواهر الأمنية، فهذا المفهوم يصف عملية القيام بتحويل قضية معينة إلى نهاية أمنية تم تقديمها بلغة أمنية، وهذه العملية في حد ذاتها تستدعي عدد من المفاهيم الأخرى مثل الموضوع المرجعي ويعني الشيء الذي يتم تهديده والذي يحتاج إلى الحماية كالدولة والأمة وسيادتها والبيئة وغيرها، وحركة الأمننة والتي تعني عملية تقديم قصية معينة

– يون برخو **الهاكطولوجيا ودورها في تفسير الالكترونية وتأثيرها على الممارسة الهجمات الصحفي** 2(1 2017، ttps://studies.aljazeera.net/ar/mediastudies/2017/11/171102072845 895.html ، تم الاطلاع بتاريخ 2(5 2021.

[10] - رغدة البهي، الردع السيبراني : المفهوم و الإشكاليات و المتطلبات، **مجلة الدراسات الإعلامية** ، المركز الديمقراطي العربي، العدد الأول، يناير،2018

باعتبارها تهديدا وجوديا للموضوع المرجعي المحدد، وهذه الحركة تتم منن طرف الجهات الفاعلة في عملية الأمننة وتقدم إلى الجمهور .[11]

كما تضمنت الدراسات النقدية في تسعينيات القرن العشرين اتجاهين مركزيين هما مقاربة كل من كيث كروز و مايكل ويليامز، التي تنتقد الدراسات المتعلقة في اختزال الأمن في الجانب العسكري، و تقر بضرورة إقحام الفرد، الجماعة، الهوية و تشجيع الفكر التعددي و المقاربات المتنوعة، بالإضافة إلى مقاربة كين بوث" و ريتشارد واين جونز" التي تقوم على أعمال هابرماس" و آخرين و تركز على تحرير الإنسان و مفهوم الإنعتاق ، و حسب كروز" إن الدراسات النقدية الأمنية تشترك في ثلاثة نقاط هي : كيفية بناء التهديدات، بناء الوحدات المرجعية للأمن، و إمكانية تحول المعضلة الأمنية .[12]

كما أن للأمن السيبراني أبعاد و هي كما يلي :

. / **الأبعاد العسكرية** : تكمن الميزة النسبية للقوة السيبرانية في قدرتها على ربط الوحدات العسكرية ببعضها البعض عبر الشبكات العسكرية في الفضاء الالكتروني، لما يسمح بسهولة تبادل المعلومات و تدفقها و كذا السرعة و إعطاء الأوامر العسكرية و القدرة على إيصال الأهداف عن بعد و تدميرها، و قد تتحول هذه الميزة إلى نقطة ضعف إن لم تكن الش كة الالكترونية المستخدمة في ذلك مؤمنة جيدا من أي اختراق خارجي قد ينسب في سن هجمات الكترونية مضادة على شبكات القوات المسلحة و أجهزة الاستخبارات، و من ثم تجسس على الأمن العسكري للدول و تعطيل قدرة الدولة على النشر السريع لقواتها وقدراتها أو قطع أنظمة الاقتصاد فيما بين الوحدات العسكرية و تعطيل شبكات الكمبيوتر كما يمكن أن يتم شل و تعطيل عمل أنظمة الدفاع الجوي أو التوجيه الالكتروني فضلا عن إمكانية و فقدان السيطرة على وحدات القيادة.[13]

! / **الأبعاد السياسية** : تتمثل الأبعاد السياسية للأمن السيبراني بشكل أساسي، في حق الدولة في حماية نظامها السياسي و كيانها و مصالحها الاقتصادية التي تعني حقها وواجبها في السعي إلى تحقيق رفاه شعبها، في وقت تؤثر التقنيات في موازين القوى داخل المجتمع نفسه، حيث أصبح بإمكان المواطن أن يتحول إلى لاعب أساسي في اللعبة

- – فريدة طاجين ، سياسات الدفاع الماليزية في ظل التهديدات الأمنية لل يئة الرقمية: الواقع والتحديات، مداخلة قدمت بالملتقى الدولي الثاني حول سياسات الدفاع الوطني بين الالتزامات السيادية والتحديات الإقليمية، جامعة قاصدي مرباح ورقلة، 10 و 11 جانفي 017 ، ص 41 .

2. - جويدة حمزاوي ، من الأمن القومي إلى الأمن الإنساني ، **مجلة الدراسات ال ستراتيجية و العسكري** ، المركز الديمقراطي العربي برلين، المجلد 2(، العدد 6 ، مارس 020 ، ص 6 .

3. - إدريس عطية، **مرجع سبق ذكر** ، ص 05 .

السياسية. كما أصبح بإمكانه الاطلاع على خلفيات و مبررات القرارات السياسية التي تتخذها حكومتها عبر الكم الهائل من المعلومات التي يمكنها الوصول إليها، التي يمكن أن توزع و تنشر على الانترنت و بقية الأجهزة التي توصل بها، و بالمقابل لا يتوانى العاملين في الشأن السياسي عن الإفادة من ما تق مها هذه التقنيات للوصول إلى أك ر شريحة ممكنة من المواطنين , الترويج لسياساتهم في العالم، و غني عن البيان مدى التأثير الذي يتركه هذا الأمر بغض النظر عن صحة السياسات و المبادئ و المواقف التي يروض لها، فقد استخدم أوباما" مثلا الشبكات الاجتماعية بشكل كثيف خلال حملته الانتخابية كما تركت التسريبات لآلاف الوثائق الدبلوماسية السرية عبر الويكيليكس أثرا سلبيا على العلاقات بين الدول ومصداقيتها.[14]

ا / **الأبعاد الاجتماعية** : من الضروري تعميم المفهوم الصحيح و السليم للأمن إلى كل المشتركين للشبكة الدولية للمعلومات، إذ تعتبر ن الخطوات الأساسية التي تقوى مستوى الأمن إذا ما صيغت بطريقة واضحة و عرفت و نفذت بذكاء، و لذلك يعتبر أن تنظيم الحملات الإعلامية و التثقيف المدني لأجل مجتمع معلومات مسئول من الضروري بمكان، بحيث تغطي التحديات و المخاطر و تدابير الأمن و الوقائية و الرادعة لأ. ل تثقيف جميع الأفراد السيبرانيين للتعاطي مع عملية الأمن.[15]

و ينبغي التشديد على واجب الأمن و المسؤولية الفردية و التدابير الرادعة و كذلك التداعيات المحتملة في إطار القانون الجنائي التي تترتب على عدم احترام الالتزامات التي يوجبها الأمن، و بصورة أكثر عموم ة فغن من الضروري توفير التثقيف و التدريب على تكنولوجيات المعلومات و الاتصال و ليس فقط على الأمن و التدابير الرادعة، إذ يجب للثقافة الأمنية أن تغرس داخل ثقافة تكنولوجيا المعلومات .[16]

ا / **الأبعاد الاقتصادية** : يرتبط الأمن السيبراني ارتباطا وثيقا بالاقتصاد فالتا زم واضح بين اقتصاد المعرفة و توسيع استخدام تقنيات المعلومات و الاتصالات كما بالقيمة التي تمثلها البيانات و المعلومات المتداولة و المخزنة و المستخدمة على كل المستويات، كما تتيح تقنيات المعلومات و الاتصالات تعزيز التنمية الاقتصادية لدول كثير عبر إفادتها من فرص الاستخدام التي تقدمها الشركات الدولية و الشركات الكبرى التي تبحث إدارة كلفة إنتاجها بأفضل الشروط يضاف إلى ذلك دخول العالم عصر المال الالكتروني ضمن بيئة تقنية متحركة بعد

---

4 - قوي بوحنية: **مرجع سبق ذكر** ، ص 62 .

5 – سمير بارة: **مرجع سبق ذكر** ، ص 262

6 - نفس المرجع، ص 262 .

إطلاق الخدمات الالكترونية، إذ تتز يد اســتثمارات المصــارف والمؤسســا المالية فــي مجال الـ ال الرقمي و تتنافس الشركات على إصــدار تطبيقــات تســمح بآليــات دفــع آمنة و قد وضعت بعض الــدول التشــريعات خاصــة لحمايــة أ والهــا و مــا يمكــن يثيره هذا الأمر من صعوبات و ما يتطلبه من تشــريعات للحــد مــن بعــض الجــرائم الاقتصادية والمالية والعــابرة للحــدود كتبيــيض الأمــوال والتهــرب مــن الضــريبة فــالأمن الســيبراني يضــمن تقــديم الخــدمات التــي تقــدم بوا ـــــ طة تقنيــات المعلومات والاتصالات، و ما يضــمن الإقبــال عليهــا ممــا يتــرجم عمليــا بتطــوير أسس اقتصاد سليم.[17]

ز / **الأبعاد القانونية** : تعد العلاقة بين القانون و التكنولوجيا علاقة تبادلية فالتطورات التكنولوجية لمختلفة تفرض مواكبة التشريعات القانونية لها، من خلال وضع قطر و تشريعات للأعمال القانونية و الغير القانونية منها و لكن بصورة عامة قد تفتقد الجريمة السبيرانية في الوقت الحالي للأطر القانونية الصارمة للتعامل معها، و لعل ذلك يعود لعوامل مثل طبيعة الجريمة الالكترونية في حد ذاتها و صعوبة تحديد هوية مرتكبي الجرائم و مرونة التعريفات المرتبطة بتكنولوجيا المعلومات، إلى جانب ذلك أن الجرائم السبيرانية غير مقيدة بحدود الدول الأمر الذي يقتضي تفعيل التعاون الدولي المشترك لمكافحتها.[18]

على مستوى آخر تفرض الأبعاد الخاصة بالأمن السبيراني إرساء قواعد الحماية على فهم و تصور واضحين و شاملين للمكونات التقنية و الموارد البشرية، بحيث لا تسقط المخاطر التي يتسبب بها التصرف البشري، سواء كانت مجرد أخطاء أو أعمالا إجرامية و قياسا على المبادئ الأساسية في بناء الأمن الكلاسيكي أي تحديد التهديدات و المخاطر رسم إستراتيجية الدفاع و بناء قدراته، إعداد خطط مواجهة و اتخاذ تدابير احترازيةاستنادا إلى ذلك يستلزم بناء الأمن السبيراني لما يستلزم : إقرار تدابير و إجراءات ردعية حقيقية تتمثل في إطار تشريعي و تنظيمي يواكبها، و هيكلية مناسبة، و بناء قدرات و آليات تحقيق و ملاحقة و محاكمة، ما يستدعي إدراج قواعد خاصة لمكافحة الجريمة السبيرانية و إعلان المسؤوليات المدنية و الجزائية و المهنية.[19]

---

7 - إدريس عطية: **مرجع سبق ذ ر** ، ص 05 .

8 - نفس المرجع، ص 06 .

9 - قوي بوحنية **مرجع سبق ذكر** ، ص 4i .

المبحث الثاني : انعكاسات التهديدات السبيرانية على الأمن القومي للدول

في غمرة التطور المتسابق الـ ي عرفه مصطلح الأمن سواء القومي أو الإقليمي أو حتى الدولي، و في ظل التفكك الحاصل له مع توالي التحديات و الأزمات وكذا المشاكل المتعاقبة مع مرور الوقت ووصولا نحو مصطلح الأمننة الذي يضم في طياته عدة مخرجات أفرزتها التهديدات المتسارعة و المتداخلة حتى أصبح الحـ ث عن الأمن بمفهومه التقليدي غير مجدي و فعال في كثير من الدراسات الحديثة خاصة في ظل التقدم التكنولوجي الهائل المعلومة تعد بمثابة القاطرة الأمامية أو البوصلة التي يعتمد عليها البشر في جل حياتهم.

انطلاقا مما سبق فإن سعي الدول إلى حيازة أسلحة الهجوم أو ردع النووي يصبح بلا معنى، إذ إن هذا التطور المثير سيفرض على الدول التحول باتجاه الاستثمار في صناعة المعلومات بكل تقنياتها فائقة الحداثة و التطور بدلا من أن تستثمر في برامج مكلفة للغاية لتطوير طاقتها النووية العسكرية من دون أن تتوافر فرصة حقيقية لاستخداماتـ ا بصورة فعلية.[20]

وفي خضم هذا التطور و التوجه الحتمي الذي يجب على الدول أن تلجه نحو عالم المعلوماتية و التكنولوجيات الحديثة برز تحدي خطير وهو كيفية التعامل أو الاستغلال الأمثل لهاته الأخيرة، بحيث تزامن التوسع و التراكم الهائل للمعلومات و تداخل شبكات الـ تصال فيما بينها، تزامن مع توالي التهديدات الالكترونية في المجال السبيراني و بالتالي أضحت مسألة الأمن القومي للدول تحت الاختبار الدائم و التحدي المحتوم الذي تفرضه معادلة ضرورة حماية الأمن القومي للدولة بالتزامن مع مواكبة الانفتاح و ركوب كافة سلالم التكنولوـ يا وتحولاتها و مواجهة كافة التهديدات التي يمكن أن تحملها.

و لكن قبل التعرض لشيء من التفصيل لهذه التهديدات و طبيعتها يجب معرفة أو التعرف على الهجمات السبيرانية، فهناك من يعرفها على أنها "فعل يفوض من قدرات وظائف شبكة الكمبيوتر لفرض قومي أو سياسي من خلال استغلال نقطة ضعف ما تمكن المهاجم من التلاعب بالنظام.[21]

---

[20] – إسماعيل صبري مقلد، ثورة المعلومات وحروب المستقبل المحتمل ، **مجلة آفاق المستقبل**، العدد 5 ، جويلية/أوت/سبتمبر 012 ،صر 43 .

[21] – رغدة البهي: **مرجع سبق ذكر** ، صر 09 .

و على ذلك فالإرهاب الالكتروني يعرض الدولة بأركانها و مؤسساتها الالكترونية الرقمية للخطر، لأن أفعاله ناجمة عن جرائمه تتجاوز نطاقها المحلي إلى الوطني بأسره بل إلى الدول الأخرى، أي أن نتاج جرمه لا يضل محصورا في نطاق ضيق بل ينتقل إلى حدود أبعد بكثير من النطاق الواقعي المحلي و الوطني، و يصل إلى النطاق الافتراضي عبر شبكاته على مستوى العالم.[22]

أدت ثورة المعلومات إلى ظهور أنماط جديدة من التحديات الأمنية، ولقد ظهرت تحديات جديدة للأمن بمفهومه التقليدي، هذه لتحديات تتعلق بالاستعدادات اللازمة للتعامل

مع المستجدات و المهددات الأمنية ففي السابق يمكن للدولة إغلاق حدودها و التشويش على جيرانها، وعدم استقبال بثهم التلفزيوني و مع الاتصالات معهم، و كانت غالبية المهددات الخارجية تأتي من الجيران لخلافات حدودية أو أطماع في المصادر الوطنية أو بسبب تحالفات عسكرية معينة، أما في المجتمع المعلوماتي فلم يعد بالضرورة أن تكون الدول متجاورة لكي تهدد بعضها أمنيا، فتطور نظم السلاح الذي مكنه من الوصول لمسافات بعيدة واستخدام تقنيات بسيطة لتدمير البناء المعلوماتي للدولة وتخريب نظمها لإدارية والعسكرية قد جعل حرب المعلومات حرب الجميع، و إن جيشها الجميع صغارا وكبارا هواة أو قراصنة و متلصصين أفرادا أو جماعات.[23]

ويمكن توزيع الأخطار الناجمة عن الفضاء السيبراني انطلاقا من أهدافها إلى ما يلي [24]:

- **أخطار تطال الدول** : وهو كل ما يعرض الأمن القومي و العسكري و الاقتصادي و الاجتماعي و يهدد البنية التحتية و الحرجة للدول، و أسواق المال و القطاعات المصرفية و السلم الدولي و المنشآت النووية و المؤسسات الصحية و قطاعات النقل بكل أنواعه البري، البحري، الجوي، و رفاه الشعوب.
- **أخطار تطال الأشخاص** : مثل سرقة المعلومات الشخصية و تسريبها و استخدامها دون إذن، ودون وجه حق، و صرف الأموال و اختراق أنظمة المعلومات و الاعتداء على الملكية الفردية و الصناعية و العلاقات التجارية، كما تشمل هذه الفئة أيضا الاحتيال و البريد غير المرغوب فيه، و الجرائم ضد الأطفال و المحتوى غير المشروع.

---

[2] - مصطفى محمد موسى، **الإرهاب الالكتروني دراسة قانونية، أمنية، نفسية، اجتماعية**، مصر: دار الكتب و الوثائق القومية المصرية، ط1، 2009، ص 203.

[3] - ذياب البداينة، **الأمن وحروب المعلومات**، الأردن: دار الشروق للنشر والتوزيع، 2002، ص 24.

[4] - منى الأشقر جبور، **مرجع سبق ذكره**، ص 04.

مع التلاشي التدريجي لحدود الدولة القومية بمفهومها التقليدي و التحول العميق لمصطلح الأمن و عدم انحصاره بسبب رئيسي ألا و هو انكشاف العالم على بعضه البعض إثر انفجار ثورة نظم المعلومات و غزارتها ما أدخل الدول و الحكومات مهما كانت مرتبة تقدمها في تسابق دائم نحو أهمية الحذر و الحيطة من أعداء سواء كانوا داخليين أو خارجيين، أهم ما يميز أسلوبهم هو العمل بالطرق التكنولوجية و غير منظمين ووهميين في كثير من الأحيان و أيضا غير خاضعين لا للقواعد و القوانين الدولية ولا المحلية و هو ما يشكل تحدي ا تعامل مثل هذه المشاكل الأمنية المهددة للأمن القومي للدول.

و جوهر المشكلة أن الجريمة عبر الشبكة لا تعرف الحدود الجغرافية، فالجاني قد يكون في دولة أوروبية و محل الجريمة في آسيا أو في دولة إفريقية، كما في حالة اختراق الشبكات بقصد التجسس المعلوماتي أو التجسس الذي يهدد الأمن القومي، أو سرقة النقود بطريق الانترنت.[25]

و لعل أخطر ما يميز هذه الحرب (الهجمات السيبرانية) هو صعوبة الردع، ففي الحروب التقليدية يعد الهجوم المضاد هو الرادع الحقيقي أمام التفكير في شن الحرب و هو الأمر الذي يصعب القيام به في حالة الحرب السيبرانية، و يرجع ذلك إلى عدة عوامل منها صعوبة اكتشاف الهجوم السيبراني في وقته الحقيقي، فضلا عن صعوبة تقييم الأضرار الناتجة عن شن هذه النوعية من الحروب، و صعوبة التحكم في مدى الهجوم السيبراني المضاد، و أخيرا صعوبة تحديد هوية الطرف القائم بالهجمات السيبرانية على وجه اليقين.[26]

و يختلف حجم الاختراق أو الضرر الذي يمكن أن تتعرض له أي دولة ما في العالم بسبب الهجمات السيبرانية، و ذلك فحسب قوتها و مدي تقدمها فإذا كانت المعطيات الحالية تشير إلى أن كل دول العالم أضحت معرضة للاختراق و للهجمات الالكترونية المتعددة، إلا أن الدول المتقدمة تعد الأقل عرضة وذلك بسبب النظم الحمائية المعتمدة في هذا الشأن و البنية التحتية للاتصالات التي تمتاز عن غيرها بالحس العالي و الوعي ا مجتمعي و بالتالي

---

[5] – حجازي عبد الفتاح بيومي ، **جرائم الكمبيوتر والانترنت و التشريعات العربية(دراسة مقارنة مع تطبيق على نظام مكافحة جرائم المعلوماتية في المملكة العربية السعودية** ، القاهر : دار النهضة العربية 009 ، ص 3(.

[6] – شادي عبد الوهاب منصور، **حروب الجيل الخامس أساليب التفجير من الداخل على الساحة الدولية**، القاهر : المستقبل للأبحاث و للدراسات المتقدمة/ العربي للنشر والتوزيع 019 ، ص ص 00 ، 01 .

فهي معرضة للهجمات الخارجية أكثر من الداخلية مثلما يحصل من حين لآخر في القضايا التي حدثت في الانتخابات الرئاسية الأمريكية سنة 2016، و التي اتهمت فيها دولة روسيا الاتحادية بالتدخل في الشأن الداخلي للولايات المتحدة الأمريكية و غير ذلك، و أما فيما يخص الدول المتخلفة فالأمر هنا يعد غاية في الصعوبة بسبب أن هذه الهجومات السيبرانية تتوالى و تتكرر دائما و بشكل متسارع سواء كان مصدرها داخلي أو خارجي، و ذلك بسبب هشاشة البنية التحتية و نظم الاتصالات الضعيفة و بالتالي تأخر رهيب في أنظمة الحماية و كذا التوترات الاجتماعية المتكررة و هو ما يفتح الباب أمام أطراف غير خاضعة للقوانين و بالتالي التلاعب و تهديد الدولة في عمقها الاستراتيجي ألا و هو أمنها القومي.

بالرجوع قليلا إلى الوراء و إلى سنوات بداية الألفية الجديدة و مع التطور و الانتشار الرهيب للنظم التكنولوجية و شبكة الانترنت باتت مسألة الأمن بصفة عامة على المحك ليس فقط الأمن القومي للدول فحسب، بل مسألة الأمن الإقليمي و وصولا إلى الأمن الجماعي للبشرية و للمنظومة الدولية، فالهجمات السيبرانية أضحت مصدر قلق ليس فقط للوضع الداخلي للأنظمة الحاكمة فقط، و إنما قد تكون المسألة تمس الأمن الجماعي لتكتل أو هيئة قارية ككل كالاتحاد الأوروبي مثلا و الذي امتحن لأكثر من مرة في هذا الشأن، ووجهت أصابع الاتهام وقتها للولايات المتحدة الأمريكية بالتصنت على المكالمات لبعض قادة الاتحاد الأوروبي، و كذلك الشأن بالنسبة للاتحاد الإفريقي الذي وضع أمن القارة وشعوبها على المحك لأكثر من مناسبة، وبالتالي و من خلال هذين المثالين البسيطين يتجلى لنا خطورة التهديدات التي تعرضت لها المنظومة الدولية ككل سواء كان المتهمون دول او مؤسسات أو كيانات تابعة لدول ما و تحارب بالوكالة، أو أفرد هواة، و هو ما دفع بهذه الهيئات إلى التجند في شكل تحالفات أو تكتلات خاصة في مجال المواجهة.

تأخذ الأحلاف السيبرانية عدة أشكال منها، شكل الأحلاف التقليدية و كمثال على ذلك يعد تحالف الناتو السيبراني أحد أهم هذه الأمثلة و الذي يتجه نحو معالجة مجموعة واسعة من التهديدات على تعزيز السياسة السيبرانية التي جاءت بموجب اتفاق استونيا سنة 2007 ، و ركز الحلف بشكل أساسي على تنفيذ تدابير الحماية السلمية المطلوبة للجانب العسكري، حيث دفعت هجمات الفضاء الالكتروني التي وقعت في استونيا عام 2007 الحلف لإعادة التفكير في حاجته لسياسة دفاع إلكتروني، و من ثم وضع الحلف للمرة الأولى في تاريخه سياسة رسمية للدفاع

الالكتروني ثم ا تمادها في جانفي 008، ترتكز على ثلاث دعائم أساسية **أولها التضامن** : بمعنى تقديم المساعدة عند الطلب مع احترام مبدأ سيادة الدولة، و **ثانيها عدم التكرار** : بمعنى تفادي الازدواجية غير الضرورية في الهياكل و القدرات على المستوى الدولي و الإقليمي و الوطني، و **ثالثها لتأمين** : من خلال التعاون القائم على الثقة مع الأخذ في الاعتبار حساسية المعلومات ذات الصلة التي لا بد أن تكون متاحة، و أماكن الانكشاف الممكنة التي يمكن أن تعرض للاختلاف بصورة أسهل.[27]

من جهة أخرى و حسب آخر الإحصائيات التي تمس قارة إفريقيا فإن (% فقط لدول الإفريقية هي التي تمتلك اليوم إطارا قانونا يعاقب الأعمال المتعلقة بالجرائم السيبرانية، و أنه حتى إن وجدت هذه القوانين في بعض الدول الإفريقية الساعية لتطوير مجال الأمن السيبراني قاريا، إلا أنها لا تواكب الوتيرة المتسارعة للابتكارات المتجددة في مجال ا كنولوجيا الرقمية.[28]

ففي ظل هذا التطور الملحوظ يتجلى اليوم في إفريقيا التهديد السيبراني بشكل ملفت بحيث تؤكد إحدى التقارير الدولية الصادرة حول الأمن المعلوماتي في إفريقيا أن تكلفة الخسائر المالية التي تكبدتها الشركات الإفريقية في سنة 2017 جراء الهجمات ا لكترونية قاربت 3.5 مليار دولار أمريكي، و حسب التقرير ذاته تبقى المؤسسات البنكية و الخدمات المالية و المصالح الحكومية و الإدارة العمومية هي أكثر القطاعات تضررا من الهجمات السيبرانية، بالإضافة إلى تعطيل التجارة الالكترونية و المعاملات التي تتم باستخدام الهـ اتف النقالة و الاتصالات السلكية و اللاسلكية، و بشكل عام تم تصنيف قرابة 0 % من المؤسسات الإفريقية تحت عتبة فقر الأمن السيبراني.[29]

يجمع خبراء عصر المعلومات علـــى أن العقـــود القليلـــة القادمـــة قـــد تشـــهد تحولا مدهشا للعالم الذي سيتخذ شـــكل مدينـــة ذكيـــة صـــغير ة مرتبطـــة بالكامـــل بالأقمار الصناعية، و إذا كانت عجلـــة التقـــدم فـــي مجـــال التقنيـــة الرقميـــة قـــد تسارع إيقاعها باتجاهات و مجـــالات مختلفـــة فـــي عـــالم اليـــوم حتـــى صـــارت عنوانا للعصر ومفتاحا لتقدم الأمم، فإن مسيرة التقدم الرقمـــي فـــي طريـــق تعزيـــز قدرات الأمم على إدارة الحـــروب و تحقيـــق الســـيطرة و النصـــر، ســـيكون لهـــا

---

[7] – محمد بوكبشة، الأمن والدفاع السبراني أولوية قصوى، مجلة الجيش، العدد 51، أكتوبر 017، ص 34 .

[8] – إسماعيل جنادي، الأمن السبراني التحدي القادم للإتحاد ا فريقي، مجلة الجيش، العدد 63، أكتوبر 018، ص ص 43 44 .

[9] – نفس المرجع ص 43 .

تداعيات مستقبلية أكثر خطورة و تـأثيرا نتيجـة لمتغيـرات عـدة أهمهـا حجـم الدعم المادي الكبير الذي تخصصـه الـدول للاسـتثمار فـي هـذا القطـاع مـن جانب، و أهمية الأهداف الحيوية المـراد تحقيقهـا لاسـتخدام هـذه الوسـائل مـن جانب آخر.[30]

و في سياق متص ل رفع الخبير الاستراتيجي الأمريكي اللواء فلاديمير بيلوس" سقف القناعة بقوله " أن تبدأ المعركة في المستقبل بالتحول أكثر فأكثر باتجاه الفضاء الافتراضي مع تنامي قدرة الدول المهاجمة على تطوير و لإدارة سيناريو حرب المعلومات ضد دول أخرى في محاولة تدميرها من الا خل دون الحاجة لشأن حرب دامية أو مكلفة على المستوى الاستراتيجي أي سيضحى بالإمكان إجبار العدو على الاستسلام دون استخدام الأنواع التقليدية من الأسلحة.[31]

و من المتوقع مثلا نشوب حرب الكترونية بين الصين و الولايات المتحدة الأمريكية بعد تقرير (سي آي ايه) لأن لصين أصبح بمقدرتها تشويش الأنظم و الأجهزة وإلحاق الضرر بها و إدخال الفيروسات و البرامج الخبيثة بها، و حرب الفضاء الالكتروني لا توجد بها أي إراقة للدماء و لكنها أخطر من الحروب العسكرية لأنها تستطيع تدمير الأنظمة و الأجهزة مما يمنعها عن العمل بش كل تام و إتلافها.[32]

المبحث الثالث : جهود الاتحاد الدولي للاتصالات السلكية و اللاسلكية في مجال الأمن السيبراني

يعد الاتحاد الدولي للاتصالات السلكية و اللاسلكية أحد أهم الوكالات التابعة للأمم المتحدة و الرائدة في مجال تكنولوجيا الاتصالات محاولا بذلك مو كبة كل التطورات الحاصلة في هذا الشأن.

ف 17 ماي 865 م تشكل الاتحاد الـدولي للتلغـراف الـذي ورثـه الاتحـاد الدولي للاتصالات السلكية و اللاسلكية علـى أسـاس الاتفاقيـة الدوليـة للتلغـراف التـي وقعتهـا عشـرون 0!) دولـة أوروبيـة، وبـذلك يعـد الاتحـاد الـدولي

---

[30] – سامر مؤيد عبد اللطيف، الحرب في الفضاء الرقمي رؤية مستقبلية ، **مجلة رسالة الحقوق** ، السنة السابعة العدد 2(015 ، ص 2(.

[1] – نفس المرج ، ص 04 .

[2] – نسرين الصباحي ، الحروب السيبرا ية و تحديات الأمن العالمي ، **ملف نشر في المركز العربي للبحوث و الدراسات**، سبتمبر 017! ، على الرابط: http://www .acrseg.org40594 تاريخ الإطلاع 3(4(021! .

للاتصالات السلكة ة و اللاسلكية أقدم منظمة دولية مازالت قائمة حتى اليوم.[33]

يتوالى الأحداث العالمية البارزة خاصة مع مطلع و منتصف القرن العشرين 0!) من الحربين العالميتين الأولى و الثانية في النصف الأول منه و ما عرفته من ظهور جملة من الاختراعات و الاكتشافات التي أملتها صدامات الحروب و النزاعات الخاصة في مجال الاتصالات و في مجال سلاح الإشارة و الراديو و التلغراف.

ومع انعقاد مؤتمر مدينة أطلا نطا في عاء 1947 استوجبت التطورات التي حدثت في مجال الاتصالات مراجعة إجراءات تسجيل و تأمين الاعتراف الدولي باستخدام الطيف، و لذلك تم تبني خطط تفصيلية للخدمات في أقاليم ثلاثة جديدة ثم تقسيم العالم إليها، الإقليم الأول يضم أوروبا و إفريقيا، و الإقليم الثاني يضم الأمريكيتين و الإقليم الثالث يضم آسيا وجنوب المحيط الهادي.[34]

لقد كان للتطورات الجديدة في مجال الاتصال تأثير عميق على المنظو ات السياسية و الاقتصادية و الثقافية و الاجتماعية، فقد غيرت هذه التطورات و بشكل مثير الطريقة التي يعيش بها معظم الناس و الطريقة التي يتفاعلون بها مع بعضهم البعض و مع البيئة التي يعيشون فيها، و لذلك في العصر الحالي أصبح يعرف بعصر المعلومات و الواقع أن كل د ل المركز تمتلك أحدث تكنولوجيات الاتصالات بينما تمتلك دول الأطراف عددا قليلا من أجهزة الكمبيوتر و التلفونات المحمول و الخدمات الرقمية.[35]

فالانتشار الرهيب لكل ما يمت بصلة بالجانب التكنولوجي فرض على كل مكونات المجتمعات المختلفة من أفراد و جماعات، د ل أو حكومات أو أأشخاص عاديين أو مؤسسات، فرض عليهم الانخراط في هذه التحولات التكنولوجية الحاصلة في العالم، رغم الفوارق البارزة بين الدول في حد ذاتها و الشعوب، و بالتالي إما رفع التحدي و التماشي مع ما هو يتقدم و يتطور و الانخراط التام أو البقاء في موقف متراء ع و هو ما يعني قبول منطق الأقوياء على الضعفاء و هذه النقطة بالذات كثيرا ما أثيرت في مناقشات الهيئات الدولية المعنية و من بينها الاتحاد الدولي للاتصالات السلكية و اللاسلكية.

---

[3] - حسني محمد نصر و عبد الله الكندي، **الإعلام الدولي(النظريات،الاتجاهات،الملكية** ،، ! الإمارات العربية المتد د دار الكتاب الجامعي 011 ص 414 .

[4] - **نفس المرجع** ص 415 .

[5] - **نفس المرجع** ، ص 413 .

وقد تزايد دور الاتحاد الدولي للاتصالات السلكية و اللاسلكية بشكل كبير نتيجة الـ بتكرات التكنولوجية و تعدد المستثمرين في مجال الاتصالات من الحكومات إلى الإذاعيين و الشركات المصنعة لأجهزة الاتصال. و عن هذا أصبح الاتحاد منظمة كونية رئيسية تتعامل مع قطاع الاتصالات.[36]

وينفذ الاتحاد الدولي للاتصالات السلكية و اللاسلكية إستراتيجية على مـ حلتين للتصدي للتهديدات المحدقة بالأمن السيبراني، و يوفر البرنامج العالمي للأمن السيبراني (GCA) للإتحاد إطارا للتعاون في مجال الأمن السيبراني، بما في ذلك تحديد استراتيجيات رئيسية لتنسيق الاستجابة الدولية للتحديات المتزايدة و تعزيز الثقة و الأمن في مجتمع الـ علومات و يسهل عمل برنامج الأنشطة ذات الصلة لأعضاء الاتحاد والبلدان النامية على وجه الخصوص لتنفيذ هذه الاستراتيجيات الرئيسية على أساس متكامل و الموائمة بين المتطلبات والاحتياجات على الصعيد الوطني والإقليمي و الدولي. وقد ساعد هذا البرنامج البلدان على بناء الـ درات في المجالات التي تتصل بالأمن السيبراني و حماية البنى التحتية الحرجة للمعلومات، ومثال ذلك في جملة أمور وضع استراتيجيات وطنية، و تدابير قانونية تتعلق بالأمن السيبراني و إنقاذ القانون وهياكل تنظيمية مثل (المراقبة و الإنذار و الاستجابة للحوادث) و حماية الـ طفال على الخط، و ذلك من خلال تطوير و نشر مجموعة أدوات عبر الانترنت وغير ذلك من الموارد، و بتبادل المعلومات من خلال فعاليات الأمن السيبراني الإقليمية و تقديم المساعدة المباشرة إلى الأعضاء و التنسيق داخل الاتحاد الدولي للاتصالات وخارجه.[37]

و كذلك من الـ هود التي تحسب للاتحاد، فهو يعتبر الوكالة الرائدة لمنظومة الأمم المتحدة في قضايا تكنولوجيا المعلومات و الاتصالات، كما يعد مصدرا هاما للتدريب و التثقيف و المعلومات في هذا المجال، و تحمل هذه المكانة الرائدة الاتحاد مسؤولية أن يوفر التدريب و التثقيف و المعـ ومات بأعلى جودة في جميع أنحاء العالم و أن يمثل رأس الحربة في التكنولوجيات و التغيرات البازغة سريعا في هذا القطاع و للوفاء بذلك يجب أن تستفيد أنشطة التثقيف و التدريب من الطرائق و الوسائل

---

[6] – حسني محمد نصر و عبد الله الكندي ؛ **مرجع سبق ذكر** ص 420 .

[7] – الإتحاد الدولي للاتصالات السلكية واللاسلكية، الاجتماع الإقليمي التحضيري للمؤتمر العالمي لتنمية الـ صالات 2010 منطقة الدول العربية ، الجمهورية العربية السورية: قطاع تنمية الاتصالات، من 17 إلى 19 جانفي 010 ص 9ا . **على الرابط**: http// :www omferas.com

الأحدث لتوصيلها مع مراعاة أن النفاذ إلى المعدات و التكنولوجيا لازمة لهذه الأنشطة من بعض مناطق العالم قد يكون محدودا.[38]

قبل أن يكون سياسات و استراتيجيات الاتحاد الدولي للاتصالات السلكي و اللاسلكية حيز هام لموضوع الأمن السيبراني، فإنه و انطلاقا من كون هذا الأخير لا يمكن له أن ينفصل على الجانب التكنولوجي و التطورات و التغيرات الحاصلة في هذا الشأن خاصة في ظل الانتشار الواسع و الرهيب لشبكة الانترنت نجد أن الانخراط في هذا الخصوص ظهر منذ عقود طويلة، فكلما ظهر تقدم جديد في مجال الاكتشافات إلا و نجد له عناية كبيرة في دراسات و أبحاث الاتحاد خاصة في نهاية القرن العشرين و بداية القرن الحادي و العشرين و بالتالي تم عقد عدة اجتماعات و منتديات و مؤتمرات عالمية و إقليمية في مجال تكنولوجيا المعلومات و الاتصال . و الهدف من كل هذا هو مواكبة التطورات و التحولات الرهيبة التي يشهدها عالم التكنولوجيا و لعلنا نلخص أهم المؤتمرات و المنتديات فيما يلي :

. / **القمة العالمية لمجتمع المعلومات** : وهي قمة عقدت على مرحلتين من 10 إلى 12 ديسمبر 2003 في جنيف وفي تونس من 16 إلى 18 نوفمبر 005! ، و تعتبر هذه القمة من المعالم العامة للأمم المتحدة و الاتحاد الدولي للاتصالات السلكية و اللاسلكية الذي قام بالدور الإداري الرائد في القمة، و كذلك لجميع أصحاب المصلحة . فقدت كانت القمة العالمية لمجتمع المعلومات محاولة طموحة لمواجهة المسائل التي تثيرها تكنولوجيا المعلومات و الاتصالات من خلال اهم منظم و شامل.[39]

و من أهم معالم القمة أنها اتخذت نهجا يشترك فيه جميع أصحاب المصلحة و هو النهج الذي يتبع الآن في مرحلة التنفيذ بمشاركة مباشرة من جانب المجتمع المدني و القطاع الخاص إلى جانب الحكومات و المنظمات الدولية. و تقدم مبادرة ربط العالم التي يقودها الاتحاد الدولي للاتصالات السلكية و اللاسلكية مثلا ملموسا لدور الشراكات بين أصحاب المصلحة المتعددين في بناء الجسور لسد الفجوة الرقمية.[40]

---

[38] – الإتحاد الدولي للاتصالات السلكية واللاسلكية، **مرجع سبق ذكر** ، ص 8 .

[39] – الإتحاد الدولي للإتصالات السلكية واللاسلكية ، وثيقة صادرة عن القمة العالمية لمجتمع المعلومات، جنيف 2003 وتونس ديسمبر 005 ص . https ://www.itu.int .

[40] – **نفس المرجع** ، ص .

ا / **المؤتمر العالمي لتنمية الاتصالات لعام 2006 بالدوحة (قطر)** : وهو المؤتمر الرابع الذي ينعقد منذ إنشاء قطاع التنمية في الاتحاد الدولي للاتصالات السلكية و الا سلكية عام 989 ، و كان ما سبق من مؤتمرات عالمية لتنمية الاتصالات انعقد في بوينس أيريس عام 994 ، وفي فاليتا عام 998 ، و في اسطنبول عام 992 و يتولى مكتب تنمية الاتصالات القيام بأنشطة أمانة قطاع تنمية الاتصالات في الاتحاد طبقا لما رسم له في المؤتمر الـ عالمي لتنمية الاتصالات عام 2006 .[41]

اعتمدت خطة عمل الدوحة التي حددت اختصاصات أنشطة قطاع تنمية الاتصالات خلال فترة 2007 ـــــ 2010 و بصفة عامة تدعم أنشطة قطاع تنمية الاتصالات و تشجع توافر و استعمال تكنولوجيا المعلومات و الاتصالات على نطاق واسع كأدوات لتحق ق الأهداف الإنمائية للألفية كما وضعتها الأمم المتحدة، و كذلك مساعدة البلدان على تلبية نتائج و أهداف القمة العالمية لمجتمع المعلومات.[42]

ا / **المنتديات الإنمائية الإقليمية الخمسة لسنة 2009** : و ارتكزت سياسة الاتحاد الدولي للاتصالات على ستة 6) مجالات وهي[43] :

. تعز يز الاستراتيجيات الوطنية لتكنولوجيا المعلومات و الاتصالات.

ب . المواءمة بين سياسات تكنولوجيا المعلومات و الاتصالات في مختلف المناطق.

ت . إيجاد مبادرات إقليمية و مبادرات وطنية واسعة النطاق.

ث . إطلاق مبادرات عالمية تتناول مواضيع محددة متعلقة بالهياكل الأساسية لتكنولوج ا المعلومات و الاتصالات.

ج . إنشاء منصة للتمويل الافتراضي.

ح . استحداث أداة إلكترونية لتقييم مدى تطور تكنولوجيا المعلومات و الاتصالات.

نظم الاتحاد الدولي لـ اتصالات السلكية و اللاسلكية خمسة منتديات إنمائية عبر الأق يم في سنة 2009 واحد لكل منطقة ، أعد موارد دريبية بالتعاون الوثيق مع شركاء آخرين لسد فجوة التوحيد القياسي ، تعزيز تنفيذ شبكات الجيل التالي ، الشبكات العريضة النطاق في البلدان النامية.[44]

---

1 – الإتحاد الدولي للاتصالات السلكية واللاسلكية، **مرجع سبق ذكر** ص . .

2 – **نفس المرجع** ص . .

3 – تقرير الأمين العام للأمم المتحدة حول : **متابعة نـ ائج مؤتمر القمة العالمي لمجتمع المعلومات على الصعيدين الإقليمي والدوا** ،ص 2 .

4 – تقر ر الأمين العام للأمم المتحدة ، **مرجع سبق ذكر** ص 2 .

ا / **المؤشرات الأساسية لتكنولوجيا المعلومات و الاتصالات :** و هي تعتمد على 6( ) مؤشرات عالمية في مجال تكنولوجيا المعلومات و الاتصالات و هي كما يلي[45] :

- مؤشرات البنية الأساسية لتكنولوجيا المعلومات والاتصالات و النفاذ.
- مؤشرات النفاذ إلى تكنولوجيا المعلومات و الاتصالات و استخدامها من قبل الأسر
- مؤشر ت استخدام تكنولوجيا المعلومات و الاتصالات من قبل مؤسسات الأعمال.
- مؤشرات قطاع تكنولوجيا المعلومات و الاتصالات الإنتاجي.
- مؤشرات التجارة الدولية بسلع تكنولوجيا المعلومات و الاتصالات.
- مؤشرات تكنولوجيا المعلومات و الاتصالات في التعليم.

و كل مؤشر من بين هذه المؤشرات يضم مؤشرات أساسية و معايير و منهجيات إحصائية.

المبحث الرابع: قياس الأمن السيبراني وفق مؤشرات تقارير الاتحاد الدولي للاتصالات السلكية واللاسلكية

شكل موضوع الأمن السيبراني أحد أهم أولويات الإستراتيجية المعتمدة من طرف الاتحاد الدولي لاتصالات السلكية و اللاسلكية في مجال تكنولوجيا الاتصالات و المعلومات، خاصة في التطور الرهيب و السريع للتكنولوجيا و الأدوات المعتمدة عليها من جهة، ولظهور أشكال متعددة للتهديدات المصاحبة لهذه التكنولوجيا من جهة ثانية و هي أمور جعلت العالم بأكمله تحت التأهب و الاستعداد أحيانا لمواجهة و مجابهة أي تهديد أو خطر قادم أو حتى متوقع، أو البحث عن الآليات التي يمكن من خلالها التعامل مع هذه الأخطار على صعيد آخر.

و لتشجيع و تحفيز الدول على مضاعفة جهودها في مجال الأمن السيبراني طور الاتحاد الدولي للاتصالات السلكية و اللاسلكية " مؤشر الأمن السيبراني العالمي GLOBAL CYBER SECURITY INDEX GCI) يقيس مستوى التزام الدول في خمسة مجالات هي : التدابير القانونية و التدابير التقنية و التدابير التنظيمية و بناء القدرات و التعاون الدولي) و هي المعايير التي سبق أن حددتها الأجندة عالمية للأمن

[45] – الإتحاد الدولي للاتصالات السلكية و اللاسلكية، المؤشرات الأساسية لتكنولوجيا المعلومات والاتصالات 010. ، جنيف مكتب تنم ة الاتصالات 010 ص ص 5 إلى 3 .

السيبراني GLOBAL CYBER SECURITY AGENDA GCA) التي أطلقها الاتحاد الدولي للاتصالات عام 2007 و نستطيع من خلال هذا المؤشر قياس التأهب و العمل على ضمان الأمن السيبراني و النهوض به في مختلف الدول[6] .

و اعتمادا على مؤشرات قياس مستوى التأهب التي ضعها الاتحاد أضحى هذا الأخير يقوم بنشر تقارير دولية في هذا الشأن تحدد الترتيب العالمي لمدى التزام الدول فيما يخص مجال الأمن السيبراني لكافة دول العالم المنخرطة في عضويته.

و المشروع نتاج أبحاث أولية و ثانوية مكثفة من جانب كلا من الاتحاد الدولي للاتصالات السلكية و اللاسلكية و مؤسسة ABI للبحوث، فقد أرسلت استقصاءات قطرية إلى الدول الأعضاء كافة في الاتحاد، ثم استكمالها بأبحاث كمية متعمقة، جمعت المعلومات عن القوانين و اللوائح وفرق الاستجابة لحالات الطوارئ الحاسوبية وفرق الاستجابة للحوادث الحاسوبية و السياسات العامة و الاستراتيجيات الوطنية و المعايير و طرق منع الشهادات و التدريب المهني و زيادة الوعي و الشراكات التعاونية [7] .

و الهدف من الرقم القياسي GCI توفير لمحة بشأن إلى أي مدى وصلت البلدان في تناولها الأمن السيبراني على الصعيد الوطني، و تتمثل الرؤية بـ نسبة لكل من مؤسسة ABI و الاتحاد في النهوض بالوعي بالأمن السيبراني و الدور الهام للحكومات في دمج الآليات المناسبة من أجل دعم هذا النظام الحرج و النهوض به، و يجب أن تتضمن حماية سلامة الفضاء السيبراني تطوير الأمن السيبراني[8] .

و يوضح الجدول التالي الترتيب العالمي في مجال المن السيبراني للخمسة 5( ) دول الأولى للتقارير الصادرة لسنوات 2015 - 2017 - 2018) و التي يتغير ترتيبها من تقرير لآخر و هو كما يلي :

---

[5] رضوان - ج، **الأمن السيبراني أولوية في استراتيجيات الدفاع**، **مجلة الجيش**، العدد 630 ، جانفي 2016 ، ص 41 .

[47]- الاتحاد الدولي للاتصالات السلكية و اللاسلكية ، الرقم القياسي العالمي للأمن السيبراني و سمات السلامة السيبرانية لسنة 2015 ، جنيف : مكتب تنمية الاتصالات 2015 ص . .

[48] الاتحاد الدولي للاتصالات السلكية و اللاسلكية، **مرجع سبق ذكره** ، ص . .

جدول : ترتيب البلدان حسب الرقم القياسي العالمي للأمن السيبراني و سمات السلامة السيبرانية

سنة التقرير	دول الخمسة الأول عالميا	التنقيط	الترتيب العالمي
الرقم القياسي العالمي للأمن السيبراني و سمات السلامة السيبرانية لسنة 2015	الولايات المتحدة الأمريكية	0.824	01
	كندا	0.794	02
	استراليا	0.765	03
	ماليزيا	0.765	03
	عمان	0.765	03
	نيوزيلندا	0.735	04
	ا رويج	0.735	04
	البرازيل	0.706	05
	استونيا	0.706	05
	ألمانيا	0.706	05
	الهند	0.706	05
	اليابان	0.706	05
	كوريا الجنوبية	0.706	05
	المملكة المتحدة	0.706	05
الرقم القياسي العالمي للأمن السيبراني و سمات السلامة السيبرانية لسنة 2017	سنغافورة	0.925	01
	الولايات المتحدة الأمريكية	0.919	02
	ماليزيا	0.893	03
	عمان	0.871	04
	استونيا	0.846	05
الرقم القياسي العالمي للأمن السيبراني و سمات السلامة السيبرانية لسنة 2018	المملكة المتحدة	0.931	01
	الولايات المتحدة الأمريكية	0.926	02
	فرنسا	0.918	03
	ليتوانيا	0.908	04
	استونيا	0.905	05

المصدر: تقارير الإتحاد الدولي للإتصالات السلكية واللاسلكية حول الأمن السيبراني لسنوات 015 - 017 - 2018.

الفصل الثاني:
الإستراتيجية الجزائرية
في مجال الأمن السيبراني
وآليات تطويرها
اعتمادا على مؤشرات
تقارير الإتحاد الدولي
للاتصالات السلكية واللاسلكية

بعدما تم التطرق لجملة من النقاط المفاهيمية في موضوع الأمن السبيراني في الفصل الأول من الدراسة وكذا ـ دد من النقاط ذات الصلة به، وأيضا التحدث عن إحدى أهم الهيئات والمؤسسات الدولية التابعة للأمم المتحدة، والتي تهتم بمجال تكنولوجيا المعلومات والتطورات الحاصلة في هذا الشأن عموما، والأمن السبيراني وكل ما يحيط به على وجه الخصوص.

سيتم التحدث في البداية عن ا ستراتيجية الجزائرية في مجال الأمن السبيراني ومعرفة مدى إمكانية وصف الجهود المبذولة في هذا الشأن من طرف صانع القرار الجزائري بأنه فعلا قام بوضع إستراتيجية حقيقية أم أنها مجرد سياسات لحد الآن لم ترقى إلى مستوى الإستراتيجية.

وكمبحث ثاني في هذا الفصل كان زاما هنا وضع جملة من الآليات والضوابط التي يمكن عبرها تطوير الإستراتيجية الجزائرية في مجال الأمن السبيراني، وكنوع من الاجتهادات التي يحاول الباحث القيام بها و الخروج في الختام بعدد من النقاط التي لم تكن موجودة في السابق ضمن خطط برنامج صانع القرار الجزائري.

أما فيما يخص المبحث الثالث فسيكون عبارة عن تقييم نقدي للإستراتيجية الجزائرية في هذا الخصوص من خلال عرض جملة من النقاط الايجابية وكذا النقاط السلبية من جهة ثانية.

وفي ختام هذا الفصل سيتم طرح عدد من النقاط التي هي عبارة عن توصيات تم استنتاجها في هذا لشأن، والتي يمكن لصانع القرار الجزائري الرجوع والاعتماد عليها كنوع من الاجتهادات الخاصة بالباحث.

المبحث الأول: الإستراتيجية الجزائرية في مجال الأمن السبيراني.

مع مطلع الألفية وموازاة مع التطور الهائل لتكنولوجيا المعلومات، كان من الضروري أن تتحرك الدول ، ن اجل مكافحة التهديدات السبيرانية وتبني نظاما دفاعيا سبيرانيا يمكنها من تحسين أداء مؤسساتها من جهة، وجعل سياستها أكثر فعالية وتكاملية من جهة أخرى

هذه الحاجات خلقت برامج متعددة وهياكل متخصصة مهامها الدفاع والأمن السيبراني تتماشى مع التطور التكنولوجي للأجهزة الرقمية الحديثة.[49]

إن قدرة الدولة مهما كان مستوى تطوره المعلوماتي على مواجهة المخاطر التي تسببها الحروب المعلوماتية تخرج عن حدود الواقع الممكن، و يترتب على ذلك أن أقصى ما يمكن للدولة أن تفعله هو أن يزيد بدرجة ما من قدرتها على الدفاع و الردع للحد من ا هديد المعلوماتي الذي يشمل مداه العديد من المحاور لكي تبقي هذا التهديد ضمن حدود يمكن تحملها، و ربما يزيد من صعوبة تلك المهمة أن الهجوم على نظم المعلومات و قواعدها في الدولة الخصم قد يصل في شموله إلى مستوى التهديد الاستراتيجي و هو الأشد فتكـ[0] .

لعل من ابرز تداعيات التطور التكنولوجي بروز المشكلات التي تهدد الأمن القومي الجزائري و على رأسها الجرائم المعلوماتية. و تعد الجرائم المعلوماتية و الالكترونية صنفا جديدا من الجرائم و تتخذ أشكال متعددة لعل من أبرزها جرائم الاختراقات، بغرض الاستيلاء على اشتراكات لآخرين و أرقامهم السرية و إرسال الفيروسات، و هناك كذلك الجرائم المتعلقة بالمواقع المعادية سيما المواقع السياسية و التي و إن كانت من جهة تعبر عن تنامي القيم الحضارية الديمقراطية، لكنها كثيرا ما تكون مصدرا للأخبار الفاسدة التي تخلق شرخا بين النظام السياسي و مواطنيه، إضافة إلى كل ذلك هنالك جرائم القرصنة و النسخ غير المشروط أين تعد الجزائر من البلدان التي أنهكتها هذه المعضلة، و يمكن أن نذكر كذلك بجرائم التجسس الالكتروني بفعل وجود تقنيات عالية التقدم بالتجسس على الدولة، بالإضافة إلى الإرهاب الالكتروني و الذي يتم من خلاله الاستيلاء على المعلومات و القيام بتدميرها و تعطيلها في عصر الازدهار الالكتروني.[51]

ومن هذا المنطلق و الأساس كانت السياسات والخطط المسطرة لدى صانع القرار في الجزائر معنية بمواكبة كل تلك التحولات والتطورات التي يعرفها العالم، خاصة إذا رجعنا قليلا إلى الوراء نجد البلاد عاشت ما يعادل العشر سنوات الأخيرة من القرن العشرين

---

9 – إلهام غازي، الدفاع السيبراني ، **مجلة الجيش**، العدد 63، أكتوبر 2018، ص 46 .

10 – إسماعيل صبري مقلد: **مرجع سبق ذكر** ، ص 43 .

11 - سارة بودح، الإستراتيجية الجزائرية في ا نفاق على التسلح في ظل التهديدات الأمنية الجديدة 2010 – 2014، مذكرة لنيل شهادة الماستر أكاديمي في تخصص العلوم السياسية و العلاقات الدولية، جامعة قاصدي مرباح ورقلة، السنة الجامعية 2014/ 015 ، ص 4 .

تحت ضغط التوترات الأمنية التي خلفت الدمار والخسائر الفادحة في الأرواح والعتاد والممتلكات، والتي مثلت ظاهرة الإرهاب إبانها أهم صورة مهددة لكيان الدولة الجزائرية وأمنها القومي، فهي لم تقتصر على نمط وسلوك معين اتجاه فئة أو مؤسسة معينة بل تعدت لكل ما هو خاضع لسلطة الدولة الجزائرية.

ومن أهم التحديات التي أفرزتها بداية القرن الحادي والعشرين هي التطورات و التحولات الهائلة التي شهدها الكون في مجال التكنولوجيا والرقمنة عبر كافة المـ لات وهو أمر كان لزاما على صانع القرار الجزائري الوقوف عنده، فهو تحول في غاية الصعوبة وغير آمن على الدول التي ليست لديها رؤية وتبصر من ناحية ايجابيات وسلبيات الموضوع.

وإدراكا للطبيعة الحاسمة والفعالة للدفاع السبيراني عملت الجزائر ومنذ سنوات على تبني هذا المفهوم ووضعه في قلب السياسات والآليات لاسيما في الخطط العسكرية، فقد أضحى النظام المعلوماتي والرقمي أمرا لا يمكن تخطيه داخل المؤسسات والقطاعات المختلفة.

ويمتد إطار الدفاع السبيراني إلى أبعد من مجرد العمل على سلامة وأمن الحواسيب ليصل إلى الحد الذي يكون ه تأثير مباشر على الأمن القومي، وبالتالي العمل على الدفاع على مختلف النظم الإلكترونية الخاصة بالدولة وما توجهه من حرب إلكترونية، كما يسمح الدفاع السبيراني بالتصدي للتهديدات المحدقة بالشبكات والأجهزة الرقمية الحساسة للمؤسسات الكبرى. [2] وهو يقودنا للتطرق للإس راتيجية الجزائرية في هذا الشأن والتعرف على أهم الآليات المعتمدة من طرف صانع القرار هنا، وبالتالي الحصول على أهم النتائج في هذا الأمر خاصة إذا رجعنا إلى المقومات والإمكانيات والمكانة التي تحتلها الجزائر كدولة محورية في قارة إفريقيا وكذا العالمين العربي و ا سلامي.

إستراتيجية الجزائر في مجال مكافحة التهديدات السبيرانية

أدرجت الجزائر الأمن السبيراني كإحدى الأولويات في برنامج المواجهة ضد الجريمة الإلكترونية، بل أصبح يشكل جزأ لا يتجزأ من استراتيجيات الدفاع، لأن الدروس المستخلصة من الدول التي لها تجربة في هذا المجال، أثبتت أن النجاعة في التطبيق

[2] – الهام غازي؛ **مرجع سبق ذكر** ، ص 17 .

وفعالية المعايير والوسائل المستعملة لا يمكن لها أن تتجسد ما لم يكن هناك تخطيط محكم وتنسيق بين الفاعلين في الميدان، وعليه توجهت الجزائر إلى رسم استراتيجياتها مركزة على النقاط التالية [3] :

- تحديد المخاطر.
- اتخاذ التدابير اللازمة.
- تحديد الهيئات المكلفة بإدارة الأمن.
- تحديد الهيئات المكلفة بالتنسيق.
- تحديد الهيئة المكلفة بالجانب التقني للبحث عن الثغرات وتوجيه التحقيق.

الآليات القانونية والمؤسساتية في مجال مكافحة الجرائم السيبرانية في الجزائر:

الآليات القانونية: وتمخض عن ذلك جملة من القوانين والتشريعات وهي:

- **قانون العقوبات:** والذي يندرج ضمنه كل القانون رقم رقم 04 05) المتضمن تعديل قانون العقوبات [4] وتعديل القانون رقم 2306 المؤرخ في 20 ديسمبر 2006 . وصدر القانون رقم 09 04) الصادر في عام 2009 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها. [55]
- **قانون الإجراءات الجزائية:** تتبع الجريمة الإلكترونية بنفس إجراءات تتبع الجريمة التقليدية (التفتيش – المعاينة – الاستجواب – الضبط – التسرب – الشهادة – الخبرة...) مع زيادة تمديد الاختصاص المحلي لوكيل الجمهورية في لجرائم لالكترونية في المادة 37 من قانون الإجراءات الجزائية [6] .

وتتمثل القوانين الخاصة التي أقرها المشرع الجزائري في مجال الجريمة الإلكترونية فيما يلي:

---

[3] – جمال بو زدية، **مرجع سبق ذكر** ، ص ص 277 278 .

[4] – سمير بارة، **مرجع سبق ذكر** ، ص 264 .

[5] - الجمهورية الجزائرية الديمقراطية الشعبية، القانون رقم 09 04) المعلق: القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها المؤرخ في 14 شعبان 1430 الموافق لـ 05 أوت 2009 ، **الجريدة الرسمية**، العدد 47 ص ص 05 .

[6] – يوسف بوغرارة، **مرجع سبق ذكر** ، ص 10 .

قانون البريد والاتصالات السلكية واللاسلكية: حيث نصت عدة مواد منه فيما يخص المجال السيبراني، المادة 87 والتي نصت على سهولة إجراء التحويلات المالية إلكترونيا، والمادة 84 02 على استعمال حوالات الدفع العادية والالكترونية كما نصت المادة 105 على احترام المراسلات، أما المادة 127 بجزاء كل من يفتح أو يخرب بريد.[57]

* **قانون التأمينات:** وقد نص هذا القانون على تنظيم الجريمة الالكترونية من خلال مؤسسات وهيئات الضمان الاجتماعي، وذلك في عدة نصوص تخص البطاقة الالكترونية.[58]

***القانون الخاص بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها:** حيث جاء هذا القانون منظما للجرائم المتصلة بتكنولوجيا الإعلام والاتصال وكل ما له علاقة بالمنظومة المعلوماتية.[59]

بالإضافة إلى ذلك تدعمت الإجراءات القانونية بآلية تقنية جديدة تتمثل في صدور القانون 03 16 المؤرخ في 19 جوان 2016 المتضمن البصمات الجنائية في الإجراءات الجزائية لتحديد هوية الأشخاص، كما تم تعزيز الجهات القضائية على المستوى الوطني بأربعة محاكم خاصة (الجزائر – قسنطينة – وهران – ورقلة) لتسهيل عمليات البحث والتحري لذوي الاختصاص من الأجهزة الأمنية والبت في القضايا المعروضة دون الرجوع إلى الوصاية، كما شمل التشريع في بعض المجالات التي يحتمل أن تشملها الجريمة والتي لها صلة بمجال الحريات الخاصة على غرار قانون الملكية الفكرية، الثقافية وحقوق المؤلف قانون 03 15) و 03 16) الصادرين بتاريخ 19 جويلية 2003. وقانون مكافحة تبييض الأموال 01 15) الصادر بتاريخ 05 فيفري 2005. وقانون الوقاية ومكافحة المخدرات 04 18) الصادر بتاريخ 25 ديسمبر 2004.[60]

– تنص المادة 39 الفقرة 1 من الدستور الجزائري لعام 2016 على أن خصوصية المواطنين و شرفهم مصونان بموجب القانون، فيما تسير الفقرة 2

---

[57] – يوسف بوغرارة، **مرجع سبق ذكر** ، ص 10.

[58] – نفس المرجع، ص 10.

[59] – نفس المرجع، ص 110.

[60] – جمال بوازدية، **مرجع سبق ذكر** ، ص 278.

في نفس الاتجاه و النص على أن سرية المراسلات و الاتصالات الخاصة بجميع أشكالها مضمونة.

- و بدءا من يناير/كانون الثاني 2018 تصبح العملة الافتراضية البيتكوين ممنوعة رسميا في الجزائر، حيث حملت المادة 113 من قانون الموازنة العامة الذي صادق عليه البرلمان في نوفمبر 2017 المنع الرسمي و جاء فيها " إن شراء أو بيع أو استعمال أو حيازة العملات الافتراضية ممنوع ".[61]
- وقد كرس الدستور الجزائري الجديد المعتمد في نوفمبر 2020 هاتان الفئتان الأساسيتان من الحقوق من خلال المادة 47 التي جاءت على النحو التالي :

/ لكل فرد الحق في حماية خصوصيته و شرفه.

/ لكل فرد الحق في سرية مراسلاته و اتصالاته الخاصة بجميع أشكالها.

أدرجت المادة 47 نفسها فقرتين جديدتين 3 4 تقتضيان بأن حماية الأفراد في معالجة البيانات الشخصية حق أساسي يعاقب القانون على أي انتهاك للحقوق المذكورة أعلاه.[62]

الملاحظ والمستخلص من كل هذه القوانين والنصوص أنه ولو أسقطناها على المؤشرات التي يضعها الإتحاد الدولي للاتصالات السلكية واللاسلكية في مجال قياس الالتزام في مجال الأمن السيبراني نجد أنها تمس المؤشر الأول وهو القانوني، كما أن هنالك بعض الاتفاقيات التي أبرمت الجزائر في هذا الخصوص على المستويين الإقليمي والدولي.

أولا: على المستوى العربي والإفريقي:

من خلال الدراسات الأكاديمية وتحليل المعطيات المستقاة من المؤسسات المتخصصة في الأمن السيبراني المتضمنة النقائص والثغرات في حماية الأنظمة المعلوماتية للدول العربية المعلن عنها خلال اللقاءات يتضح أن المقاومات البشرية والمادية المتوفرة والقادرة على تفادي المخاطر لم تجدي نفعا، والدليل أن السلبيات التي أصبحت تشكل نسبة كبيرة من المخاطر لا تزال تطرح نفسها بشدة.[63]

---

[61] - كمال كحال، لمخاطرها العالمية ... الجزائر تمنع تداول البيتكوين بنهاية 2017، **العربي الجديد**، http://alaraby.co.uk ، 18/ 11 /2017، تم الاطلاع عليها بتاريخ 2021/05/04.

[62] - عمار بلحيمر، وزير الاتصال الناطق الرسمي للحكومة في حوار مع جريدة الشروق اليومي، يوم 5 02 2021.

[63] - جمال بوازدية، **مرجع سبق ذكر** ، ص 284 .

ورغم تعدد اللقاءات والاجتماعات والندوات التي توالت في السنوات الأخيرة حول الجرائم الالكترونية ومختلف التهديدات التي تتربص بالأمن القومي العربي عموما، فإنه من غير المعقول أن تتصف كل تلك الأعمال والمناشات بالهامشية وعدم الجدية في التجاوب معها من طرف صانع القرار العربي، فكل أو جل الآليات المطبقة في الدول العربية ميدانيا غير فعالة مقارنة مع المعايير الدولية، وكذلك ضعف الأداء الداخلي للقوانين والتنظيمات والهيئات الموكلة إليها هذه المهام.

وفي نفس الإطار وبغية تحقيق التكامل بين المؤسسات الأمنية والقضائية العربية وسعت الدولة الجزائرية من دائرة التقارب لتشمل تبادل الزيارات الميدانية، الدورات التكوينية واللقاءات التشاورية في المجالات التي شملتها السياسة الجنائية لمكافحة الإجرام عامة والاستفادة من خبرات بعض الدول العربية والتعرف على البيئة التشريعية التي ينشطون فيها، وكذا الآليات المستعملة في مواجهة الفضاء السيبراني والقدرات البشرية المسخرة لهذه المهمة.[64]

وفيما يخص التعاون مع الدول الإفريقية وكذا الاتحاد الإفريقي في حد ذاته يمثل خطوات هامة بالنسبة للجزائر التي تحاول الدفع جاهدة في مجال الأمن السيبراني نحو الأمام على الرغم من التفاوت والاختلافات المسجلة في هذا الصدد من دولة لأخرى.

بتاريخ 27 جوان 2014 قطع الاتحاد الإفريقي شوطا مهما في طريقة لتجسيد مسار رقمنة إفريقيا، بحيث تبنى خلال قمته الـ 23 التي انعقدت بمالابو بجمهورية غينيا الاستوائية اتفاقية حول لأمر السيبراني وحماية البيانات الشخصية.[65] والتي كانت الجزائر إحدى أهم الدول الأعضاء المشاركين بفعالية في بلورة نتائج واقعية وملموسة على أرض الواقع.

تعكس معاهدة مالابو درجة وعي الدول الإفريقية بالخطر الذي يهددها بحيث يندرج تبنيها ضمن حرص دول الاتحاد الإفريقي على تحيين قوانينها وتشريعاتها الإقليمية في مجال الأمن السيبراني ومن أهمها : القرار بشأن تكنولوجيا الإعلام والاتصال في إفريقيا: التحديات والآفاق 2010) إعلان "أوليفر تامبو" بجوهانسبورغ بتاريخ 09 نوفمبر 2009

[4] – جمال بوازدية، **مرجع سبق ذكر** ، ص 285.

[5] – ، **مرجع سبق ذكر** ، ص 14.

، إعلان أبيدجان بتاريخ 22 فيفري 2012 وكذا إعلان أديس أبابا الصادر في 22 جوان 2012.[66]

اكتشف مهندسون جزائريون و أثيوبيون متخصصون بأنظمة المعلومات أجهزة تجسس مزروعة في كافة أرجاء مقر الاتحاد الأفريقي الذي بناه الصينيون عام 2012 في العاصمة الإثيوبية أديس أبابا، و قالت صحيفة " لوموند" الفرنسية انه وفقا مسئولي أنظمة المعلومات في المقر وضع الصينيون أجهزة تنصت في كل المصاعد و جذوع النخيل البلاستيكية بما في ذلك البرج الزجاجي الحديث الذي أنشأته الصين عام 2012 و الذي تعقد فيه القمة الإفريقية، ووفقا لعدة مصادر داخل مقر الاتحاد الإفريقي تجسست الصين على محتويات و معلومات حساسة و قامت بتسريبات مذهلة.[67]

ثانيا: على المستوى الأوروبي:

لتجسيد مبدأ الشراكة الأور ـ متوسطية الذي وقعت عليه الجزائر مع الدول الأعضاء في الوحدة الأوروبية بتاريخ 22 أفريل 2002 المتضمن التعاون في المجال الأمني والقضائي لمحاربة مختلف الجرائم، و ذا الاتفاق المبرم مع فرنسا بتاريخ 25 أكتوبر 2003 المتضمن التعاون في المجال الأمن ومكافحة الإجرام المنظم، وانطلقت الجزائر في خطوة بعنوان "التعاون لمواجهة الجرائم السيبرانية في الضفة الجنوبية" للاستفادة من التجربة الأوروبية، وعقدت في هذا الشأن عدة لقاءات في الجزائر جمعت فريق من الخبراء من مختلف المؤسسات الفاعلة في هذا المجال وخبراء أجانب.[68]

ثالثا: على المستوى الدولي:

تم مطابقة التشريع الداخلي مع ما جاء في التشريعات الدولية وخاصة الاتفاقية الدولية المبرمة في عاصمة المجر بودابست بتاريخ 23 نوفمبر 001 المتضمنة الجرائم السيبرانية وتعتبر هذه الاتفاقية بمثابة المرجعية القانونية لكل التشريعات الدولية الصادرة في هذا المجال.[69]

---

[66] - إسماعيل جنادي ، **مرجع سبق ذكر** ، ص 14 .

[67] _ موقع الجزيرة ، حسب " لوموند" الفرنسية الصين زرعت أجهزة تجسس بمقر الاتحاد الافريقي، http//aljazeera.net، بتاريخ 2018/01/18، تم الاطلاع عليه يوم 2021/05/04.

[68] _ جمال بوازدية، **مرجع سبق ذكر** ، ص 286 .

[69] - **نفس المرجع** ، ص 286 .

يعتبر التعاون الإقليمي والدولي في مجال مكافحة التهديدات السبيرانية بالنسبة للدولة الجزائرية شكلا من أشكال المؤشرات الخمسة التي أقرها الاتحاد دولي للاتصالات السلكية واللاسلكية سابقا.

ب)الآليات المؤسساتية: سنعتمد في هذه الدراسة على الهيئات والمؤسسات التي وضعتها الجزائر في الطليعة في مجال مكافحة الجرائم السبيرانية والتي هي كل من مؤسسة الجيش الوطني الشعبي والدرك الوطني والأمن الوطني.

- **إستراتيجية لجيش الوطني الشعبي في مجال الأمن السبيراني:**

استحدث بتاريخ 11 جوان 2015 على مستوى دائرة الاستعمال والتحضير لأركان الجيش الوطني الشعبي، مصلحة الدفاع السبيراني ومراقبة أمن الأنظمة، وأوكلت لها مهمة حماية المنظومات والمنشآت الحيوية للبلاد ضد كل أنواع الجريمة ا سبيرانية .[70]

تتمحور إستراتيجية الدفاع السبيراني للجيش الوطني الشعبي حول سبعة 7ا) محاور وهي.[71]

أـــ جانب وظيفي وتنظيمي: تكون أعمال الدفاع السبيراني ضمن الجيش الوطني الشعبي موجهة ومنفذة في إطار سلسلة وظيفية أو تنظيمية مكرسة لضمان تجانس وفعالية هذه الأعمال.

ب. ، انب قانوني: تحيين وتعزيز باستمرار الإطار القانوني المتعلق باستعمال تكنولوجيات الإعلام والاتصال عموما وتأمين منظومات الإعلام خصوصا.

ج. جانب الموارد البشرية: تعد جاهزية مورد بشري تقني معتبر وذي كفاءة عالية في مجال الدفاع السبيراني هدفا أساسيا لكي تضمن نجاح دخال هذا المجال في النشاطات العملياتية والتسيير للجيش الوطني.

---

0 – جمال بوازدية، **مرجع سبق ذكر** ، ص 282. .

1 – محمد بوكبشة، الدفاع السبيراني في الجيش الوطني الشعبي ، **مجلة الجيش**، العدد 651 ، أ توبر 2017، ص 65 .

د. جانب تقني: تقوية وتكييف القدرات التقنية للحماية، الكشف والرد على الهجمات السبيرانية باستمرار، مع ضمان يقظة دائمة فيما يخص الطرق والوسائل المستعملة من طرف المهاجمين.

هـ. جانب الوقاية والتحسيس: الوقاية وتحسيس مستخدمي الجيش الوطني الشعبي من المخاطر والتهديدات التي تنجر عن استعمال تكنولوجيات الإعلام و الاتصال في الإطار المهني أو الشخصي بطريقة مستمرة.

و. جانب البحث والتطوير: تعد درجة معتبرة من الاستقلالية التكنولوجية، باستعمال وسائل تقنية خاصة أو مشخصة من طرف هياكل البحث والتطوير للجيش الوطني الشعبي، لاسيما تلك المستعملة للحماية ضد التهديدات السبيرانية عنصرا حاسما في إستراتيجية الدفاع السبيراني.

ز. جانب التعاون: تعزيز التعاون في مجال الدفاع السبيراني مع جيوش الدول الشريكة من أجل السماح للجيش الوطني الشعبي من الاستفادة من الخبرات والوسائل التكنولوجية المتقدمة جدا.

وتجسيدا لذلك باشرت الدولة الجزائرية وفي مقدمتها مؤسسة الدفاع الوطني إلى إعداد برامج خاصة لمجابهة الجريمة الإلكترونية والحد من انتشارها، وإنشاء أجهزة جديدة تنسجم في أدوارها وتجهيزاتها مع المتغيرات الخاصة في هذا المجال، إذ أصبحت الحماية السبيرانية جزء مهما في أي منظومة للدفاع، وقد استطاع الجيش الوطني الشعبي المضي قدما ومسايرة التطورات التكنولوجية والإعلامية الحاصلة في العالم، ومن ثمة تأمين وحماية نطاقه المعلوماتي، وتأمين الفضاء المعلوماتي لكل الناشطين فيه.[72]

وفي سياق ذي صلة، وتعزيزا لإستراتيجية الدفاع الوطني لمكافحة التهديدات السبيرانية، وقصد الإلمام بكافة المستجدات في هذا المجال، وبخاصة تلك التي تعالج موضوع الأمن السبيراني والدفاع كرهان للأمن والدفاع الوطنيين وحماية المنشآت الحساسة ضد لهجمات السبيرانية، تعكف مصلحة الدفاع السبيراني و مراقبة أمن الأنظمة لدائرة الاستعمال والتحضير لأركان الجيش الوطني الشعبي دوريا على تنظيم ملتقيات

[72] - سد ر بارة: **مرجع سبق ذكر** ، ص 64 .

ومحاضرات وورش عمل تطبيقية كالملتقى المنظم بعنوان : "الدفاع السيبيراني؛ مكون أساسي للأمن والدفاع الوطني" يومي 15 و 16 ماي 2017 . [73]

- **إستراتيجية جهاز الدرك الوطني :** اعتمد جهاز الدرك الوطني من أجل مواجهة الجريمة السيبرانية خاصة والجريمة الالكترونية عامة على مراكز وهيئات معينة وهي:

- **مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية:** وقد أنشئ في سنة 2008 ويعتبر الجهاز الوحيد المختص بهذا الصدد في الجزائر، وهدف إلى تأمين منظومة المعلومات لخدمة الأمن العمومي، واعتبر بمثابة مركز توثيق، هذا المركز يعكف على تحليل معطيات وبيانات الجرائم المرتكبة، وتحديد هوية أصحابها سواء كانوا أشخاصا فرادى أو عصابات، وهذا كله من أجل تأ ين الأنظمة المعلوماتية والحفاظ عليها، لاسيما تلك المستعملة في المؤسسات الرسمية والبنوك والبيوت، كما يهدف إلى مساعدة باقي الأجهزة الأمنية الأخرى في أداء مهامها، واستطاعت قيادة الدرك من خلال التكوين المستمر والمتميز لأفرادها والملتقيات الدولية والوطنية وتبا ل الخبرات مع دول أخرى أن توفر القوى المؤهلة وذات الكفاءة من مهندسي الإعلام الآلي، رجال قانون، وهذا من أجل الفهم الصحيح للجريمة المعلوماتية والتصدي لها. [74]

وقد استطاع المركز معالجة أزيد من 100 جريمة الكترونية سنة 2014 ، وما يفوق 500 قضية رقمية خلال سنة 2015 ، منها 300 جريمة تتعلق بمواقع التواصل الاجتماعي "فايسبوك"، 20 جريمة رقمية تعلقت باختراق مواقع رسمية لمؤسسات خاصة وعامة ، استهدف مجرموها أنظمة المعالجة الآلية للمعطيات. [75]

- **المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني:** التابع للقيادة العامة للدرك الوطني، يعتمد في أداء مهامه على الخبرة العلمية والتجارب المخبرية الدقيقة لكل الأدلة المتحصل عليها من مكان ارتكاب الجريمة عامة، من أجل تنوير العدالة وتوجيه الجهات الأمنية كلما تعلق الأمر باستكمال التحقيق. [76]

---

3 - محمد بوكبشة، **مرجع سبق ذكر** ، ص 15 .

4 - سمير بارة، **مرجع سبق ذكر** ، ص ص 270،271 .

5 - **نفس المرجع** ، ص 271 .

6 - ، **مرجع سبق ذكر** ص 280 .

ومن بين النتائج المتوصل إليها من طرف هذه المصد ح، اتضح أن الجرائم الالكترونية بالجزائر تضاعف بطريقة سريعة جدا، وهذا ما كشفت عنه الأرقام المسجلة التي تم البت فيها، حيث سجلت سنة 2017 أكثر من 2500 جريمة ويتعلق أبرزها 0' % انتهاك الحريات الشخصية والتهديد عبر الانترنت، ونشر صور فاضحة، الابتزاز والقرصنة الالـ ترونية وغيرها. [77]

ا . **إستراتيجية الأمن الوطني:** وفي هذا الصدد تم إنشا :

المصلحة المركزية لمكافحة الجريمة المعلوماتية: التابعة لمديرية الأمن الوطني وتعتمد هذه المصلحة على موارد بشرية لها من الكفاءة المهنية ما يؤهلها لتنفيذ مهامها على المستوى الدولي من خلال ا عامل مع المصالح المختصة (أنتربو · أفريكوم) أو مصالح الشرطة لكبرى الدول، وعلى المستوى الوطني تتواصل هذه الهيئة مع الشرطة العلمية والمكاتب اللامركزية المختصة في الإجرام (الشرطة القضائية).[78] والتي كانت عبارة عن فصيلة شكلت النواة الأولى لتشكيل أمني خاص لمحاربة لجريمة الالكترونية وعلى مستوى المديرية العامة للأمن الوطني والتي أنشأت سنة 011!، ليتم بعدها إنشاء المصلحة المركزية لمحاربة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال بقرار من المدير للأمن الوطني وأضيف للهيكل التنظيمي لمديرية الشرطة القضائية في جانفي 2015!. [79]

ويضاف إلى كل هذه الأجهزة والمراكز والمصالح التابعة للهيئات الثلاث (الجيش الوطني ، الدرك الوطني ، الأمن الوطني)، يضاف إليهم هيئة تابعة مباشرة لوزارة العدل وهي:

الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال ومكافحتها: التي شأت سنة 2009 ووضعت تحت السلطة المباشرة لوزير العدل حافظ الأختام، ولم تدخل حيز التنفيذ إلا بعد صدور المرسوم الرئاسي رقم 61 15 المؤرخ في 08 أكتوبر 2015!. [80]

---

7 – جمال بوازدي **مرجع سبق ذكر** ، ص 280. .

8 – جمال بوازدية: **نفس المرجع** ، ص 280. .

9 – إدريس عطية: **مرجع سبق ذكر** ، ص 14. .

0 – جمال بوازدية: **مرجع سبق ذكر** ، ص 281. .

وكلفت الهيئة باقتراح عناصر الإستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و لاتصال ومكافحتها وتنشيط وتنسيق عمليات الوقاية منها، ومساعدة السلطات القضائية ومصالح الشرطة القضائية في مجال مكافحة هذه الجرائم، من خلال جمع المعلومات والتزويد بها، ومن خلال الخبرات القضائية، وضمان المراقبة الوقائية للاتصالات الالكترونية قصد الكشف عن الجرا م المتعلقة بالأعمال الإرهابية والتخريبية والمساس بأمن الدولة.[81]

وكذلك من أبرز المهام المتصلة بها نذكر.[82]

– استغلال المعطيات المتوفرة بطريقة تسمح بمتابعة كل ما يجري في الفضاء السيبراني من نشاطات غير شرعية وبالتالي توجيه القدرات البشرية والمالية للحد من الثغ ات، مع العلم أن هذا المجال أصبح مفتوحا على كل الاحتمالات في ظل التطور السريع لتكنولوجيا الإعلام والاتصال.

– تعزيز التنسيق بين مختلف الفاعلين في الميدان والتشديد على ضرورة التعاون بين القطاعين العام والخاص والمجتمع المدني، من أجل نشر ثقافة المواجهة لكل الم ارسات التي تخالف القانون في القضاء السيبراني وحماية الحقوق والحريات الأساسية.

– العمل من أجل خلق إطار مركزي للمعلوماتية على شاكلة وحدة بحث، يتم من خلالها جمع المعطيات والإحصائيات في هذا المجال من أجل التحليل المستمر التهديدات واقتراح الحلول المناسبة.

– ا نسيق والتعاون بين مختلف الأجهزة الأمنية، المالية والإدارية التي لها علاقة مباشرة بأنشطة تكنولوجيا الإعلام من أجل تحديد المسؤوليات لغرض مراقبة صارمة بعد حصر المجالات المستهدفة من طرف محترفي الجريمة الالكترونية.

بعد التطرق للإستراتيجية المنتهجة من طرف الدولة الجزائرية في مجال الأمن السيبراني ، ومعرفة أهم العناصر التي تحتويها كان لا بد من عرض الترتيبات والتصنيفات التي تحتلها الجزائر انطلاقا من التصنيفات التي وضعها الاتحاد الدولي للاتصالات السلكية واللاسلكية، والتي ركزت عليها الدراسة انطلاقا من التقرير الصادر ي سنا 2015 .

---

[81] - إدريس عطية: **مرجع سبق ذكر** ، ص 14 .

[82] – جمال بوازدية: **مرجع سبق ذكر** ، ص 281 .

احتلت الجزائر المرتبة 3؛ عالميا من أصل 29 مرتبة في مستوى التأهب في مجال الأمن السيبراني، وذلك حسب الرقم القياسي العالمي في هذا الشأن، وفي ما يلي جدول توضيحي يبين ذلك وفق التقرير الصادر سنة 2015؛.[83]

جدول يبين الترتيب العالمي لمدى إلتزام الدول في مجال الأمن السيبراني :

البلد	الرقم القياسي	الترتيب العالمي
الولايات المتحدة الأمريكية	0,824	01
كندا	0,794	02
استراليا	0,765	03
ماليزيا	0,765	03
عُمان	0,765	03
نيوزيلندا	0,735	04
النرويج	0,735	04
اسرائيل	0,676	06
تركيا	0,647	07
قطر	0,618	08
صر	0,588	09
فرنسا	0,588	09
المغرب	0,559	10
تونس	0,529	11
السودان	0,441	14
الإمارات العربية المتحدة	0,353	17
البحرين	0,294	19
إيران	0,294	19
ليبيا	0,294	19
المملكة العربية السعودية	0.294	19
الأردن	0,206	22

[3] – تقرير الاتحاد الدولي للاتصالات لسنة 015 ، جنيف مكتب تنمية الاتصالات ص ص، من 01 إلى 16 .

الجزائر	**0,176**	**23**
بربادوس	0,176	23
بيلاروس	0,176	23
بليز	0,176	23
البنين	0,176	23
البوسنة والهرسك	0,176	23
بوتسوانا	0,176	23
ملاوي	0,176	23
سوريا	0,176	23
البهاما	0,147	24
موريتانيا	0,147	24
دولة فلسطين	0,147	24
بوروندي	0,118	25
كمبوديا	0,118	25
لبنان	0,088	26
هايتي	0,059	27
العراق	0,029	28
الصومال	0,029	28
هندوراس	0,000	29
ليسوتو	0,000	29

المصدر: تقرير الاتحاد الدولي للاتصالات حول الأمن السبراني و سمات السلامة السيبرانية لسنة 2015 .

ويعد هذا الترتيب في هاته الفترة مقبولا على العموم ، و ذلك نظرا للمعطيات الموجودة في تلك الفترة، فالجزائر ورغم بعض الجهود التي كانت تبذل في مجال مكافحة الجرائم و التهديدات الالكترونية عموما فإنها اقتصرت على سن جملة من التشريعات و القوانين، و كذا المصادقة على بعض الاتفاقيات و المعاهدات الدولية و الإقليمية مثل مطابقة التشريعات الداخلية مع الخارجة و المصادقة على الاتفاقية الدولية المبرمة بعاصمة المجر بودابست في 23 نوفمبر 2001 ، و أيضا حتى الهيئات و المنظمات التي

تم تأسيسها مثل الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها و التي تأسست سنة 2009 و لن تدخل حيز التنفيذ إلا في سنة 2015، و من جهة أخرى يلاحظ انه تم إهمال الجوانب التقنية و التنظيمية و بناء القدرات في تلك الفترة.

وفيما يخص ترتيب الجزائر على المستوى العربي فقد احتلت المرتبة العاشرة حسب التزامها بتلك التدبير التي وضعها الرقم القياسي العالمي للأمن السيبراني حسب تقرير سنة 2015 أيضا.[84]

وأما التقرير الصادر عن الاتحاد الدول للاتصالات السلكية واللاسلكية لسنة 2017 فيما يخص الرقم القياسي العالمي للأمن السيبراني فإن الجزائر قد احتلت المرتبة 67 عالميا بتنقيط 0.432 من أصل 164 دولة، و المرتبة 9 عربيا متراجعة بمراتب كثيرة إلى الخلف في الترتيب العالمي.[85]

و يفسر هذا الترتيب التأخر الواضح في تجسيد إستراتيجية وطنية في مجال الأمن السيبراني، فالعمل المنجز في تلك الفترة إضافة إلى القوانين و التشريعات فهو لم يخرج من دائرة المؤسسات الأمنية و هي الجيش و جهاز الدرك و الشرطة، و بالتالي غياب واضح لباقي الدوائر الحكومية و كذا القطاعين العام و الخاص و مختلف فئات المجتمع.

و في التقرير الصادر عن نفس الهيئة لسنة 2018 حول قياس الأمن السيبراني و الذي تغير فيه تصنيف الدول إلى ثلاثة (3) مستويات و هي مستوى عالي، متوسط، منخفض و الذي احتلت فيه الجزائر مرتبة متدنية أي في التصنيف المنخفض، و بالتالي أصبحت بعيدة عن التصنيف العالي و المتوسط و متأخرة عن دول كثيرة رائدة في هذا المجال، حيث احتلت المرتبة 108 عالميا بتنقيط 0.262 و المرتبة 14 عربيا.[86]

---

[4] - الاتحاد الدولي للاتصالات السلكية واللاسلكية، تقرير سنة 2015، **مرجع سبق ذكره**، ص 1.

[85] the International Telecommunication Union (ITU) Global Cybersecurity Index (GCI) , 2017. , Genève. p54.

[86] .,the International Telecommunication Union (ITU) –Global Cybersecurity Index 2018, Genève . p58.

المبحث الثاني: آليات تطوير الإستر تيجية الجزائرية في مجال الأمن السيبراني:

إن نقطة انطلاق الأمن السيبراني تبدأ بتطوير سياسة وطنية لرفع الوعي حول قضايا الأمن السيبراني، و الحاجة لإجراءات وطنية و إلى التعاون الدولي، أما الخطوة الثانية فتتمثل في تطوير المخطط الوطني لتحفيز الأمن السيبراني بهدف تقليص المخاطر و آثار التهديدات السيبرانية و تتضمن المشاركة في الجهود الدولية و الإقليمية بتحفيز الوقاية الوطنية للتعافي من الحوادث السيبرانية.[87]

لذلك لا بد أن تنطلق الحلول في هذا المجال من فهم الطبيعة الخاصة لتقنيات المعلومات و الاتصالات، لا سيما لجزء الخاص بتجاوزها للحدود و للمجتمعات و الأنظمة، كما لطبيعة البنى التحتية نفسها بما يعني الطبيعة غير الملموسة للبيانات و إمكانية تناقضها و اختراق الأنظمة التي تحويها، و يعني هذا بالدرجة الأولى فهم مشترك للإمكانيات التي تقدمها تقنيات المعلومات و الاتصالات بوجهيها السلبي و الايجابي، و وعيا بضرورة إيجاد أرضية مشتركة لمواجهة تحديات بناء الثقة في مجتمع المعلومات انطلاقا من تحقيق بيئة آمنة.[88]

تستوجب عملية تطوير أي إستراتيجية وطنية في مجال الأمن السيبراني المرور عبر جملة أو مجموعة من الـ راحل الهامة التي يجب تطبيقها، وهو ما حاولت الدراسة المقدمة تقديمه بالنسبة للجزائر، والتي ضبطها في أربعة مراحل أساسية وهي:

المرحلة الأولى: إدراك خطورة التهديدات السيبرانية على الأمن القومي لجزا ي

في هذه المرحلة الأولى يعد إدراك حجم وخطورة التهديدات الداخلية والخارجية للأمن القومي شيء مهم جدا لصانع القرار مهما كانت طبيعتها ونوعيتها، فقد تكون هذه التهديدات ملموسة وظاهرة وقد يكون في شق آخر غير ملموسة وأكثر خطورة، وهو ما ينطبق في الوقت الراهن على التهديدات السيبرانية التي تواجهها كل دول العالم.

ويمكن توزيع الأخطار في الفضاء السيبراني انطلاقا من أهدافها على ما يطال الدول وما يطال الأشخاص، ويندرج في إطار الفئة الأولى، كل ما يعرض الأمن القومي

---

[87] – قوي بوحنية: **مرجع سبق ذكر** ، ص 49 .

[88] - **نفس المرجع** ص 54 .

والعسكري والاقتصادي والاجتماعي، ويهدد البيئة التحتية والحرجة للدول وأسواق المال والقطاعات المصرفية والسلم الدولي والمنشآت النووية والمؤسسات الصحية وقطاعات النقل بكل أنواعه البري والبحري والجوي، ورفاه الشعوب. بينما يندرج في الفئة الثانية: سرقة البيانات الشخصية وتسريبها، واستخدامها دون إذن، ودون حق، وسرقة الأموال واختراق أنظمة المعلومات والاعتداء على الملكية الفكرية و لصناعية والعلاقات التجارية كما تشمل هذه الفئة أيضا: الاحتيال والبريد غير المرغوب فيه والجرائم ضد الأطفال والمحتوى غير المشروع، وغيرها الكثير مما يعتبر جرائم سبيرانية ضد الأشخاص وضد الأموال .[89]

بالنسبة للجزائر وكغيرها من معظم دول العالم، فإنها تجاوزت ه ه المرحلة الأولى من إدراك صانع القرار الجزائري مدى خطورة الاستخفاف بالتهديدات السبيرانية المحيطة بالداخل الجزائري، وأنه تهديد يطال المؤسسات العامة والخاصة، الأفراد والجماعات مهما كانت مكانتهم ومناصبهم فهم جميعا معنيين بهذا الموضوع في ظل الانتشار الهائل لو ائل التكنولوجيا والانترنت.

وتختتم هذه المرحلة بأهمية وضع الأشخاص والمؤسسات الكبرى داخل الجزائر في صلب الموضوع وأن تكون القاطرة الأمامية الدافعة نحو تبني الإستراتيجية المعدة.

المرحلة الثانية: الإعداد والتخطيط للإستراتيجية الجزائرية في مجال الأمن السبيراني

تبدأ هذه المرحلة بادراك صانع القرار في الجزائر بأهمية سن جملة من التشريعات والنصوص القانونية التي تتلاءم وتتناسب مع مجال الأمن السبيراني، وهو ما تجسد فعلا على أرض الواقع كخطوة أولية، ويليها بعد ذلك كخطوة ثانية تعيين الهيئات والمؤسسات الرائدة التي خول لها مسؤولية إدارة مخاطر التهديدات السبيرانية وبالتالي صياغة وإصدار قوانين وأنظمة، وكذا برامج محددة لعمل هذه الهيئات والمؤسسات كي تأخذ الطابع الرسمي والشرعي.

وعلى اعتبار أن موضوع الأمن السبيراني يأخذ في طياته أساس الطابع الأمني فقد أوكلت المهمة في الجزائر لكل من مؤسسة الجيش الوطني الشعبي؛ وكذا جهاز الدرك الوطني، وسلك الأمن الوطني ووزارة العدل، وهي المؤسسات الرائدة التي اعتمدت عليها

[9] - منى جبور الأشقر؛ **مرجع سبق ذكر** ، ص 14 .

الدولة في هذا الخصوص. حتى تتمكن الهيئات من السيطرة على مختلف الجوانب المتعلقة بعملية تحقيق الأمن السبيراني وفق ما تم رسيمه في الإستراتيجية الوطنية، توجهت المؤسسات السيادية (رئاسة الجمهورية، وزارة الدفاع المؤسسات الأمنية، الوزارات) إلى تنظيم دورات تكوينية وسخرت لها كافة الوسائل المادية والبشرية، كما استنجدت الجزائر بخبراء دوليين لتمكين الإطارات الناشطة في المجال من جه ع الأسلاك لمعرفة أفضل الممارسات في تكنولوجيا الأمن والسياسات العامة للأعمال الالكترونية المعمول بها في الخارج، كما تم بعثات للحضور والمشاركة في المؤتمرات الدولية للاستفادة من الخيرات التي تهدف إلى إصدار التوصيات المناسبة لأمن وسلامة المعلومات في الفضاء الس بيراني .[90]

المرحلة الثالثة: التجسيد الفعلي للإستراتيجية الجزائرية في مجال الأمن السبيراني

تشكل هذه المرحلة حجر الزاوية بالنسبة لأي إستراتيجية، ليس فقط بالنسبة لموضوع أو مجال الأمن السبيراني فحسب بل لأي موضوع يحتاج لخطط بناء سياسات أو استراتيجيات، إذ أن هذه المرحلة وإذا ربطناها بالمؤشرات الخمسة التي وضعها الاتحاد الدولي للاتصالات السلكية واللاسلكية قد تضم في طياتها كل المؤشرات التقنية والتنظيمية وبناء القدرات وأخيرا مؤشر التعاون الدولي، وبالتالي ما يلاحظ على التخطيط الإستراتيجي الجزائري مجال الأمن السبير ني لم يخرج عن دائرة المؤشر القانوني بالدرجة الأولى.

وينبغي أن توفر الإستراتيجية التوجيه العام للأمن السبيراني للبلد، وان تعبر عن رؤية واضحة ونطاق واضح، وأن تحدد الأهداف التي يتعين بلوغها في إطار زمني محدد، وأن تحدد أولويات هذه الأهداف من حيث الأثر على لمجتمع والاقتصاد والبنية التحتية. وعلاوة على ذلك ينبغي لها أن تحدد مسارات العمل الممكنة، وأن تحفز جهود التنفيذ، وأن تدفع تخصيص الموارد اللازمة لدعم جميع هذه الأنشطة. وقد تتضمن الإستراتيجية أيضا بعض النتائج التي تم التوصل إليها في مرحلة الجرد والتحليل .[91]

[90] - جمال بوازدية، **مرجع سبق ذكره**، ص 1284.

[91] - ، دليل وضع إستراتيجية وطنية للأمن السبيراني إلتزام إستراتيجي بالأمن السبيراني الإتحاد الدولي للاتصالات السلكية واللاسلكية ب ت ن)، ص 13 .

إن الأمن السيبراني ليس تحديا تقنيا فحسب بل قضية معقدة متعددة الأوجه تمتد جوانبها إلى ما هو أبعد من الازدهار الاقتصادي والاجتماعي إلى مجالات مثل إنفاذ القانون والأمن الوطني والدولي والعلاقات الدولية والمفاوضات التجارية والتنمية المستدامة وما إلى ذلك.[92]

يمثل تحدي إعداد بنية تحتية صلبة وقوية في الجزائر بمثابة حجر الركيزة للسلطات، ليس فقط في مجال تكنولوجيا الاتصال والمعلومات فحسب بل للرقي والرفاه من كافة الكوارث والتهديدات والأخطار التي تتربص بالأمن الوطني ومنها خطر التهديدات السيبرانية التي لا يمكن ر عها ومواجهتها إلا عبر قاعدة تكنولوجية صلبة مهيئة ومعدة لتجاوز أحلك الصعوبات والامتحانات، خاصة وأن قطار التطورات التكنولوجية لا يمكن له أن يتوقف عند أي بلد لازالت الأساليب التقليدية والبدائية هي المسيطر على كافة مناحي الحياة فيه وما فائدة سن القوانين والنص وص التنظيمية التجسيد الفعلي للمشاريع على أرض الواقع لا يزال بعيدا أو يسير بوتيرة بطيئة.

وأصبح للبيئة الرقمية أهمية حرجة بالنسبة للحكومات ومؤسسات الأعمال والأفراد وتواجه هذه المجموعات مخاطر الأمن السيبراني وتتقاسم درجة من المسؤولية في إدارتها، وذلك تبعا لدور كل منها ولئن كانت المهمة صعبة، فإن تحديد جميع أصحاب المصلحة المعنيين وإشراكهم أمر ضروري لوضع إستراتيجية الوطنية للأمن السيبراني والنجاح في تنفيذها، ويساعد ذلك على فهم احتياجات أصحاب المصلحة ومعارفهم وخبراتهم الفريدة، مما يسهل التعاون من أجل تحقيق أهد ف الإستراتيجية.[93]

الحصول على أفضل الوسائل التكنولوجية، الاعتماد على الكفاءات والإطلاع على أفضل طرق الحماية تعتبر حلقة وصل صلبة لتفادي الثغرات ومقاومة الاختلافات ولتحقيق هذه المهمة أصبح من الضروري على السلطات الاستثمار في الجانب التقني وتشجيع المبادرات ، هادفة لتطوير سياسات أمن وحماية البنية المعلوماتية، خاصة إذا علمنا أننا على عتبة تجسيد مشروع الحكومة الإلكترونية التي أصبحت مطلب للمواطن لتحسين الخدمات.[94]

---

[2] – الإتحاد الدولي للاتصالات للإتصالات السلكية و اللاسلكية وآخرون ؛ **مرجع سبق ذكر** ، ص 30 .

[3] – **نفس المرجع** ص 31 .

[4] – جمال بوازدية: **مرجع سبق ذ ر** ، ص 283 .

ومن ابرز العناصر الأساسية التي يجب أن تركز عليها الإستراتيجية الجزائرية في مجال الأمن السبيراني هو ن يكون الهدف الأسمى لها حماية كافة مكونات المجتمع والكل مساهم في صياغة والدفاع عن هذه السياسات والاستراتيجيات ومعنى هذا هو إشراك القطاعين العام والخاص، بدءا من أن تكون قضايا التكنولوجيا والمعلوماتية ليست حكرا على بعض الوزارات والدوائر الحكومية فقط بل يجب ن تتوسع لكافة الوزارات، فنلاحظ مثلا أن وزارات مثل البريد وتكنولوجيا المعلومات والاتصالات ووزارة التربية الوطنية والثقافة و أيضا وزارة الاستشراف كلها تكاد مغيبة في هذا الشأن إلا من بعيد، أيضا لا يمكن نسيان دور كثير من المؤسسات سواء كانت عمومية أو خاصة في جزائر، حيث يجب أن تلعب الدور المحوري في مجال الأمن السبيراني مثل المؤسسات الإعلامية مهما كان نوعها، وكذا المؤسسات البنكية والمصرفية والتي لها دور أساسي في اقتصاد الرقمنة والمعرفة والتي لها دور أساسي في اقتصاد الرقمنة والمعرفة.

إن بناء الثقة في النظام لبيئي الرقمي الوطني، حيث تتوفر حماية حقوق المستعملين ومصالحهم وضمان أمن البيانات والأنظمة، أمر ضروري لاستغلال الإمكانات الكاملة للفرص الاجتماعية والسياسية والاقتصادية التي يوفرها استخدام تكنولوجيا المعلومات والاتصالات، ويجب أ ن تمكن الإستراتيجية السياسات , العمليات والإجراءات على المستوى الوطني من أجل تقديم خدمات حيوية آمنة (بما في ذلك الحوكمة الالكترونية والتجارة الالكترونية والمعاملات المالية الرقمية، وغيرها) تدعمها تكنولوجيا المعلومات والاتصالات ويستخدمها المواطنون، ومن شأن هذا النهج أن يغرس مبدأ الثقة ! بين عموم السكان فحسب، بل كذلك داخل المنظمات العامة والخاصة التي تقدم للمواطن خدماتها المتعلقة بتكنولوجيا المعلومات والاتصالات.[95]

وهذا يقودنا حتما إلى نقطة جوهرية وحساسة في هذا الشأن ألا وهي مسألة الاستثمار في العنصر البشري وقضية بناء القدرات، فلا ي كن أن تتقدم أي إستراتيجية وطنية وتتطور دون إعطاء وإتاحة مساحة كافية للمبادرات الفردية والجماعية وكل أشكال الإبداع في جانب تكنولوجيا المعلومات والاتصال،وأن يكون هذا العنصر أو المواطن مهما كان محترفا أو هاوي مصدر تطوير للإستراتيجية الوطنية الشاملة في مجال ا' من السبيراني عوض أن يكون مصدرا للتهديدات التي تحيط بالأمن القومي للدولة وهو أمر يقودنا حتما إلى أهمية أن تبنى الأهداف والسياسات من قاعدة التنشئة الأسرية والاجتماعية

[95]- الإتحاد الدولي للاتصالات السلكية و اللاسلكية وآخرون : **مرجع سبق ذكر** ، ص 4 .

السليمة، خاصة إذا علمنا بأن كل الأسر اليوم في الجزائر وكغيرها من الدول تتعامل وإلى حد الإ مان أحيانا بالهواتف النقالة وشبكات الانترنت ومواقع التواصل الاجتماعي، دون إدراك ما هي السلبيات والايجابيات من وراء ذلك على الوجه الحقيقي، وبالتالي عملية النوعية والتحسيس أمر مهم للغاية من أجل إيجاد ثقافة أسرية ومجتمعية في تكنولوجيا المعلومات والاتصالات.

وينبغي أن تعترف الإستراتيجية بالطبيعة غير المحدودية للأمن السيبراني وأن تسلط الضوء على ضرورة التعاون مع أصحاب المصلحة، لا على المستوى الوطني فحسب وإنما على المستوى الدولي أيضا والالتزامات الدولية مع أصحاب المصلحة من القطاعين العام والخاص عنصر أساسي في سهيل الحوار البناء وتطوير آليات الثقة والتعاون وإيجاد حلول مقبولة متبادلة للتحديات المشتركة واستحداث ثقافة عالمية للأمن السيبراني.[96] وأن تعبر الإستراتيجية عن التزام بالتعاون الدولي بشأن الأمن السيبراني والاعتراف بالمسائل السيبرانية كعنصر متأصل في السياسة ا خارجية للبلد، ولهذه الغاية من المهم تشجيع تنمية واستخدام الكفاءات والمهارات التي تركز على المسائل السيبرانية (الدبلوماسية السيبرانية) لاستكمال وضع هياكل تنظيمية محددة وإنشاء بعض المكاتب المتخصصة أو الموظفين المدربين اللذين يكون محور اهتمامهم المشاركة الدا وماسية في المسائل السيبرانية.[97]

ويطرح أشكال في مسألة أو مؤشر التعاون الدولي، فبقدر ما هو مفيد جدا لدولة مثل الجزائر من أجل الاحتكاك بالدول والمنظمات التي هي متقدمة ورائدة في مجال الأمن السيبراني، واكتساب الخبرات والتعلم من التجارب، بقدر ما هو سلاح ذو حدين بالنسبة للسيادة الوطنية والأمن القومي، فقد يكون مسار التعاون مع بعض الأطراف والجهات الخارجية مغلفا بأجندات خطيرة على الداخل الوطني، خاصة وأن التعامل مع التكنولوجيا والمعلومات والرقمنة يتطلب اليوم الكثير من الحيطة والحذر واليقظة المستمرة ممن هم أقوى منا في هذا الشأن.

المرحلة الرابعة: التقييم الدوري للإستراتيجية الجزائرية في مجال الأمن السبيراني من طرف صانع القرار

[6] – الإتحاد الدولي للاتصالات السلكية و اللاسلكية وآخرون : **مرجع سبق ذكر** ص 48

[7] - . **نفس المرجع**، ص 49

تعد هذه الخطوة درجة عالية من وعي صانع القرار الجزائري بأن السياسة أو الإستراتيجية المعتمدة في مجال الأمن السيبراني، وبما أنها ترتبط ارتباطا وثيقا بل هي صلب التطورات التكنولوجية الحاصلة في العالم، فهي إذا دائما في حاجة ماسة للمراجعات والتحيين والتقييم المستمر، إذ أن كل دول العالم أضحت تعتمد على التحولات العميقة في تكنولوجيا المعلومات والاتصالات في عملية البناء والتشييد وبدون قاعدة تكنولوجية صلبة لا يمكن التنبؤ بنجاح أو تقدم عملية تطوير الأمن السيبراني.

ومن بين الميزات التي تتصف بها الدول المتطورة أو المتقدمة في مجال الأمن والدفاع السيبراني نجد أن النهج القائم في هذا الشأن هو عبارة عن وضع آليات وضوابط تعمل بشكل دائم مثل خلية النحل تراجع السياسات وتقيم النتائج المحصل عليها سابقا وتخطط للمستقبل بشيء من الحيادية بحيث يتحمل كل طرف من أطراف المعادلة مسؤوليته أمام باقي الأطراف.

وأول شيء يحتاج دائما إلى التقييم الدوري والمستمر في مسألة الإستراتيجية الجزائرية للأمن السيبراني، هو الجانب لقانوني، إذ أن تسارع الأخطار الإلكترونية وتعدد مصادرها وجهاتها يوحي دائما إلى صانع القرار بفكرة أساسية وجوهرية مفادها أن باب الاجتهاد والسعي نحو تطوير المنظومة التشريعية والقانونية في الجزائر أمر حتمي اعتمادا على نقطتين هامتين هما: أولا: مواكبة التحولات مختلفة الحاصلة في العالم بأسره. وثانيا: ضرورة مراعاة الخصوصيات التي يتميز بها المجتمع المحلي من أجل مراعاة واحترام كافة أطياف المجتمع ومكوناته.

بالإضافة إلى تقييم التقدم المحرز في جميع المقاييس المتفق عليها، من المهم أيضا إجراء تقييم دوري للنواتج ومقارنتها بالأهداف المحددة، وهذا أمر بالغ الأهمية لفهم ما إذا كانت أهداف الإستراتيجية تتحقق أم ما إذا كان ينبغي النظر في اتخاذ إجراءات أخرى وكجزء من هذه العملية، يتعين أيضا إعادة تقييم بيئة المخاطر الأوسع بانتظام لفهم ما إذا كان ثمة تغييرات خارجية تؤثر على نواتج الإستراتيجية، وعلى صعيد الواقع، تكون هذه العملية بمثابة لمسات مراجعة خفيفة لمواصفات تقييم المخاطر السيبرانية التي تهدد البلد.[98]

[98] – الإتحاد الدولي للاتصالات السلكية و اللاسلكية وآخرون ، **مرجع سبق ذكر** ، ص 7!.

وفي نهاية المطاف ينبغي أن تكون التقارير الصادرة طوال دورة الحياة الإستراتيجية هي الأساس للاستعراض الشامل للإستراتيجية وطنية للأمن السبيراني وفقا للجدول الزمني المحدد أثناء مرحلة الاستهلال، وينبغي ألا تقتصر هذه المراجعة الشاملة على النظر في التقدم المحرز والتغيرات في البيئة الخارجية فحسب، بل ينبغي أيضا أن تعيد تقييم الأوليات والأهداف الخاصة بالحكومة.[99]

المبحث الثالث : تقييم نقدي لإستراتيجية الجزائر في مجال الأمن السبيراني

سيعتمد تقييم الإستراتيجية الجزائرية في مجال الأمن السبيراني على أمرين هما : **أولا** تقييم من جانب النقاط الايجابية التي يمكن استنتاجها بما أن هناك مجهودات و سياسات انتهجت في هذا الشأن من طرف صانع القرار و كل الفاعلين و المهتمين و كذا المعنيين بهذا الموضوع سواء كانوا مؤسسات أو أفراد أو جماعات، و**ثانيا** التقييم من حيث النقائص و السلبيات التي ظهرت و لا تزال على الجهود التي بذلتها الدولة الجزائرية من أجل ترقية العمل المنجز سواء كان من الجانب النظري أو التطبيقي على أرض الواقع، و بالتالي معالجة الخلل و إدراك العجز و النقائص يعتبر في حد ذاته هدف أساسي من أجل تفادي الوقوع في نفس الأخطاء مستقبلا، و كل هذا نظرا لحساسية و خطورة التعامل ببساطة وسهولة مع موضوع الأمن السبيراني لما له من تداعيات متعدد و متراكبة ـ ى مسألة الأمن القومي.

/ الايجابيات :

- من الناحية القانونية تعتبر المنظومة التشريعية في الجزائر ذات قيمة مهمة، إذ أن الجهود المبذولة في مجال القوانين والتشريعات المتعلقة بتكنولوجيا الاتصال والمعلومات و كل ما يدخل في ضمنها ذا قيمة نوعية.
- توسع دائرة المهتمين بموضوع الأمن السبيراني من الأجهزة الأمنية الثلاث (مؤسسة الجيش الوطني الشعبي ـــــ جهاز الدرك الوطني و سلك الأمن الوطني) إلى مشاركة مؤسسات و هيئات دراسية تعالج هذا الموضوع، و بالتالي المساهمة بفعالية في تطوير الإستراتيجية الوطنية للدفاع السبيراني و إن كان من الجانب النظري فقط.

[99] - **نفس المرجع** ، ص 17 .

- الاهتمام المتزايد إعلاميا و والتحسيس بخطورة التهديدات السبيرانية على الأمن القومي الجزائري من قبل بعض وسائل الإعلام التي تحاول تسليط الضوء على الظاهرة كخطر يتربص بكل فئات المجتمع الجزائري.
- المحاولات الحثيثة التي تقوم بها كل من مؤسسة الجـ ش الوطني الشعبي و جهاز الدرك الوطني و سلك الأمن من أجل التكيف مع كل المستجدات الواردة عبر العالم فيما يخص التهديدات الأمنية و التي تمس في جانب منها الشق السبيراني الذي أضحى يهدد أمن و سلامة كل دول العالم.
- الانخراط والتعاون الإقليمي والدولي الذي تبديه الجز ئـــر اتجـــاه بعـــض الـــدول و المنظمات والهيئات الإقليمية والدولية الرغبة في تبادل الزيارات والخبرات عبر تنظيم لقاءات متعددة.

! / السلبيات :

يمكن أن نلخص السلبيات الظاهرة على الإستراتيجية الجزائرية في مجال الأمن السبيراني و التي يجب على صانع القرار تصحيحـ ا و تفاديها مستقبلا في ظل المعطيات العامة حول خطورة و حساسية التقليل من شأن الموضوع و التي يمكن تلخيصها في النقاط التالية :

- إذا اعتمدنا على المؤشرات الخمسة التي وضعها الاتحاد الدولي للاتصالات و هي القانونية و التقنية، التنظيمية، و بناء القدرات، التعاون الـ ولي و أسقطناها على حالة الجزائر فنجد بأن الجهود المنتهجة في هذا الشأن اقتصرت فقط على المؤشر الأول و هو القانوني و بعض المحاولات المحتشمة في المؤشر الأخير و هو مؤشر التعاون الدولي.
- اقتصار إستراتيجية الجزائر في مجال الأمن السبيراني على بعض المؤسسات و دوائر الحكومية و عدم شمولها لكافة المؤسسات و الهيئات و المنظمات التي تتواجد في المجتمع الجزائري أي أنها إستراتيجية تأخذ في طياتها الطابع الرسمي بين دوائر مغلقة فقط و تهمش فئات واسعة من هواة التكنولوجيا و المختصين في مجال الإعلام الآلي.

- غياب سياسات واضحة ستقطب العقل البشري الجزائري و تجعله ينخرط في المنظومة الكلية للسياسة الداخلية و الخارجية للبلاد، و هو ما أهدر طاقات بشرية و نخب هامة.
- غياب بنية تحتية متطورة في جانب التكنولوجيا و الإعلام و الاتصال و هو ما يعرض البلد لأخطار متعددة الجوانب من الكوارث الطبيعية إلى البيئية وصولا نحو تقهقر و تراجع عوامل الانفتاح على العالم الخارجي، خاصة و أن هذا الأخير أصبح يعد بمثابة قريبة رقمية عالمية واحدة.
- تواضع النظم الحمائية و قاعدة البيانات و المعلومات التي تتوفر عليها المؤسسات الجزائرية خاصة كانت أم عامة، و على رأسها مؤسسات الحساسة في جهاز الدولة مثل الدوائر الحكومية و البنوك و المصارف و المؤسسات الإعلامية و هو ما يسهل من عمليات الاختراق و القرصنة في عدة مرات.
- غياب ثقافة التحسيس و التوعية بأهمية الدفاع و الأمن السبيراني لدى فئات واسعة من الشعب الجزائري، الذي يعتبر غلب أفراده أن التهديدات و المشاكل التي تحملها التكنولوجيا مجرد أخطار و مشاكل عادية و كل ذلك بسبب غياب برامج و آليات لدى صانع القرار نحو فئات المجتمع المختلفة.

خاتمة

إن ما يتم استخلاصه من هذه الدراسة المتعلقة بموضوع الأمن السبيراني و الذي هو يندرج ضمن المفهوم الأوسع للأمن بصفة عامة، و كل القضايا المتعلقة به و التي تشكل جوهر و أساس وجود البشر لما يمثله هذا العنصر الحيوي من أهمية قصوى في حياتهم مهما حدث له من تحول و تغير في مفهومه و مكوناته و كذا عناصره.

ففي ظل التسارعات و التجاذبات الرهيبة لعناصر الإعلام الآلي و تكنولوجيا الاتصالات و المعلومات، التي جعلت من العالم كله و من يسكنه بمثابة قرية واحدة موحدة، تبرز لنا في هذا الشأن أهمية مجال الأمن السبيراني كتحد يفرض نفسه بقوة في الحياة لا غنى لنا عنه بما أن أغلب خيوط العلاقات التي تربط بين الدول و الكيانات مجموعات و أفراد هي خيوط تكنولوجيا بحتة تستلزم منا جميعا الحيطة و الحذر في التعامل مع بعضنا البعض.

و في الجزائر و كغيرها من الدول كان لزاما عليها التوجه نحو تبني مقاربة معينة في مجال الدفاع السبيراني على غرار مقاربتها الأمنية التي اعتمدت في سبيل مكافحة الإرهاب سابقا، و هذا إدراكا من صانع القرار بأهمية إيلاء أهمية قصوى لهذا المجال الحيوي الذي تتشابك فيه عناصر التكنولوجيا و دفعا نحو التصدي الحازم لمختلف التهديدات الموجودة والمحتملة في هذا الشأن و بالتالي شكل الأمن السبيراني الجزائري قطعة أساسية من ساليب الإستراتيجية الدفاعية ككل.

و للوقوف على مدى نجاعة هذه السياسات و الإستراتيجية المعتمدة في الجزائر، كان من المهم إسقاطها على مؤشرات و تقارير إحدى أهم المؤسسات و الهيئات الدولية التابعة للأمم المتحدة و المتخصصة في هذا الشأن ألا و هي الاتحاد الدولي للاتصالات السلكية و اللاسلكية، وذلك من خلال المؤشرات الخمسة التي تم وضعها في هذا الخصوص والتي من خلالها يمكن قياس مدى التزام الدول وحالة تأهبها لمعايير وسمات السلامة السبيرانية و هو ما أظهرت الدراسة التي أسقطت على الجزائر مدى تقدمها أو تراجعها أو حتى أخرها مقارنة مع هذه المعايير و المؤشرات الموضوعة.

- الإسراع في تطوير مختلف التشريعات و القوانين وفق التحولات الحاصلة في ميدان تكنولوجيا الاتصال و المعلوماتية، و التي يمكن من خلالها حماية الأمن القومي الجزائري مع الحرص على التطبيق الصارم للقوانين الخاصة في هذا المجال الصعب و الحساس.
- إعداد إستراتيجية وطنية في مجال الأمن السيبراني شاملة لكافة مكونات المجتمع الجزائري دون استثناء وعدم اقتصارها على بعض الدوائر الحكومية و الأجهزة الأمنية.
- ضرورة الاستثمار في العنصر البشري و استقطابه مهما كانت صفته و جعله عنصر بناء لا معول هدم للأمن القومي و عدم تركه فريسة للمتربصين بأمن الجزائر خاصة الجماعات الإرهابية التي تستهدف الشباب.
- تحرير المبادرات الفردية و الجماعية في مجال استغلال تكنولوجيا الاتصال و المعلومات، و هو ما يتيح لمنتسبي القطاع الإبداع و مواكبة كافة التطور ت و التحولات الحاصلة عالميا.
- تعدد أساليب و مناهج التحسيس و التوعية حول مجال الأمن السيبراني داخل كافة مكونات المجتمع الجزائري من الأسرة إلى المدرسة إلى غاية الوصول نحو مؤسسات العمل، و هو ما يخلق ثقافة مجتمعية ملمة بكل مكونات و أبعاد الأمن السيبراني و ج ل ذلك أداة من أدوات حماية المصلحة العليا للوطن.
- تحسين تدفق شبكة الانترنت في كافة ربوع الجزائر مما يتيح لمستخدميها حرية التصرف و الاطلاع الجيد على المعلومات و من مصادرها الرسمية سواء كانت محلية أو إقليمية أو دولية.
- حرية الاطلاع على المعلومة من طرف المواطنين و التي كانت حكرا على دوائر حكومية معنية و مسئوليها، و هو ما يعزز الثقة بين السلطة و المواطن عوض أن يبحث عنها هذا الأخير من مصادر أخرى قد تضلله أو تستخدمه لأغراض و غايات هدامة.
- إقرار جملة من القوانين الصارمة في مجال مكافحة الجرائم الالكترونية التي تنتشر بـ رعة و تتزايد كل يوم داخل المجتمع الجزائري سواء عن قصد أو جهل من طرف بعض مستخدمي الأدوات التكنولوجية.

- تكوين جيش الكتروني يضم مختلف محترفي مجال التكنولوجيا في الجزائر يعد بمثابة النخبة التي تمثل القاطرة الأمامية أو جدار الصد أمام أي اختراق يهدد الأمن ا ومي للبلاد.
- تطوير البنية التحتية لكل المدن الجزائرية في مجال تكنولوجيا الاتصال و الإعلام.
- جعل مسألة الأمن السيبراني و تطويره أولوية من أولويات العمل الدبلوماسي وفي أجندة السياسة الخارجية للجزائر مثله مثل الدبلوماسية الرقمي و الدبلوماسية الاقتصادية ...الخ.
- الاستفادة من تجارب و خبرات الدول الرائدة في مجال الأمن السيبراني من خلال تبادل الزيارات و تنظيم الندوات و الملتقيات العلمية.
- تكثيف التعاون الدولي مع مختلف الدول و المصادقة على الاتفاقيات الدولية الصادرة عن هيئة الأمم المتحدة و المنظمات الإقليمية و الدولية مثل جامعة الدول العربية و الاتحاد الإفريقي و غيرها في مجال تكنولوجيا الإعلام و الاتصال عموما، و موضوع الأمن السيبراني على وجه الخصوص، و كل ذلك طبعا بما يحفظ خصوصيات المجتمع الجزائري و صون سيادة الوطن و الأمن القومي للبلاد.

قائمة المراجع

les références

قائمة المراجع والمصادر

القوانين :

1( ) الجمهورية الجزائرية الديمقراطية الشعبية، القانون رقم 9 4( ) المؤرخ في 14 شعبان عام 1430 الموافق 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 47 .

*** التقارير الدولية:**

2( ) تقرير حول الرقم القياسي العالمي للأمن السيبراني وسمات السلامة السيبرانية جنيف: الإتحاد الدولي للاتصالات مكتب تنمية الاتصالات، أفريل 2015.

3( ) الإتحاد الدولي للاتصالات السلكية واللاسلكية، تقرير قياس الأمن السيبراني لسنة 2017

4( ) تقرير عن تنفيذ الخطة الإستراتيجية للإتحاد الدولي للاتصالات وأنشطته للفترة 2018 2019، جنيف من 30 إلى 20 جوان 2019 .

تقارير باللغة الأجنبية :

05) Global Cybersecurity Index (GCI) , **2017.** Genève**.** the International Telecommunication Union (ITU)

06) Global Cybersecurity Index 2018, Genève .the International Telecommunication Union (ITU)

*** الكتب:**

7( ) البصيلي جاسم محمد، الحرب الإلكترونية أسسها وأثرها في الحروب، د ط، المؤسسة العربية للدراسات والنشر، 1989.

8( ) البدانية ذياب، الأمن وحرب المعلومات، عمان: دار الشروق للنشر والتوزيع 2002 .

9( ) الطائي جعفر حسن جاسم، جرائم تكنولوجيا المعلومات رؤية جديدة للجريمة الحديثة ، ، عمان: دار البداية 007! .

0) حجازي عبد الفتاح بيومي، جرائم الكمبيوتر والانترنت و تشريعات العربية(دراسة مقارنة مع تطبيق على نظام مكافحة جرائم المعلوماتية في المملكة العربية السعودية) القاهرة، .2009

1) حسني محمد نصر وعبد الله الكندي، الإعلام الدولي(النظرياد – الاتجاهاد – الملكية) ، ! ، الإمارات العربية المتحدة: دار الكتاب الجامعي .2011

2) منصور شادي عبد الوهاب، حروب الجيل الخامس أساليب التفجير من الداخل على الساحة الدولية، ، ، القاهرة: المستقبل للأبحاث والدراسات المتقدمة، العربي للنشر والتوزيع 019! .

3) موسى مصطفى محمد، الإرهاب الإلكتروني(دراسة قانونية – أمنية – نفسية – اجتماعية) ، ،مصر:سلسلة اللواء الأمنية في مكافحة الجريمة الإلكترونية 009! .

*** المجلات والمقالات العلمية:**

4) البهي رغدة، الردع السيبراني: المفهوم والإشكاليات والمتطلبات، مجلة الدراسات الإعلامية المركز الديمقراطي العربي، العدد الأول، جانفي 018! .

5) بارة سمير، الأمن السيبراني في الجزائر السياسات والمؤسسات، المجلة الجزائرية للأمن الإنساني، العدد الرابع 017! .

6) بوحنية قوي، الأمن السيبراني والصيانة في المنظمات والحكومات دراسة في المؤشرات والتطبيقات، مجلة مصداقية، المدرسة العليا العسكرية للإعلام والاتصال المجلد الأول، العدد الأ ل، ديسمبر 019! 04

7)بوكبشة محمد، الأمن والدفاع السيبيراني أولوية قصوى، مجلة الجيش، العدد 651 أكتوبر 017! .

8) بوازدية جمال، الإستراتيجية الجزائرية في مواجهة الجرائم السيبيرانية التحديات والآفاق المستقبلية، مجلة العلوم القانونية والسياسية، العدد ، أفريل 019! .

9) بوغرارة يوسف، الأمن السيبيراني: الإستراتيجية الجزائرية للأمن والدفاع في الفضاء السيبيراني، مجلة الدراسات الإفريقية وحوض النيل، المركز الديمقراطي العربيالمجلد 1 العدد ؛ ، سبتمبر 018؛ .

0؛) ج. رضوان، الأمن السيبراني أولوية إستراتيجيات الدفاع، مجلة الجيش، العدد 30ز جانفي .2016

1؛) جنادي إسماعيل، الأمن السبيراني التحدي القادم للإتحاد الإفريقي، مجلة الجيش العدد 63ز ، أكتوبر 018؛ .

2؛) حمزاوي جويدة، المقاربات النظرية للأمن: من الأمن القومي إلى الأمن الإنساني مجلة الدراسات الإستراتيجية والعسكرية، المركز لديمقراطي العربي للدراسات الإستراتيجية والسياسية والاقتصادية، برلين، المجلد الثاني، العدد السادس، مارس 020؛ .

3؛)مقلد إسماعيل صبري، ثورة المعلومات وحروب المستقبل المحتملة،مجلة آفاق المستقبل، العد 5 ، جويلية أوت سبتمبر 012؛ .

4؛) مؤيد عبد اللطيف سامر ، الحرب في الفضاء الرقمي رؤية مستقبلية، مجلة رسالة الحقوق، السنة السابعة، العدد الثاني، .2015

5؛) عطية إدريس، مكانة الأمن السبيراني في منظومة الأمن الوطني الجزائري، مجلة مصداقية، المدرسة العليا العسكرية للإعلام والاتصال، المجلد الأول، العدد الأول، سبتمبر 019؛ .

6؛) غازي إلهام ، الدفاع السبيراني، مجلة الجيش، العدد 63ز ، أكتوبر 018؛ .

7؛) القانون رقم 9 4ا) المؤرخ في 14 شعبان عام 1430 الموافق 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهور ة الجزائرية الديمقراطية الشعبية العد 47 .

*** الملتقيات والندوات:**

8؛) بن مرزوق عنترة وحرشاوي محي الدين، الأمن السبيراني كبعد جديد في السياسة الدفاعية الجزائرية، مداخلة بالملتقى الدولي الثاني حول سياسات الدفاع الوطني بين الالتزامات السيادية والتحديات الإ يمية، جامعة قاصدي مرباح ورقلة 0؛ 1؛ جانفي 2017.

9؛) طاجين فريدة، سياسات الدفاع الماليزية في ظل التهديدات الأمنية للبيئة الرقمية: الواقع والتحديات، مداخلة قدمت *بالملتقى الدولي الثاني حول سياسات الدفاع الوطني بين الالتزامات السيادية والتحديات الإقليمية، جامعة قاصدي مرباح* ورقلة 0؛ 1؛ جانفي 2017؛ .

0؛) بودح سارة ، مذكرة لنيل شهادة الماستر الأكاديمي في تخصص العلوم السياسية بعنوان: الإستراتيجية الجزائرية في الإنفاق على التسلح في ظل التهديدات الأمنية الجديد 010 2014؛)السنة الجامعيا 2014؛ 2015؛ .

1؛) جبور منى الأشقر، ا من السبيراني: التحديات ومستلزمات المواجهة، اللقاء السنوي الأول للمختصين في أمن وسلامة الفضاء السبيراني، بيروت، لبنان، 7؛ 28 أوت 2012.

2؛) الاجتماع الإقليمي التحضيري للمؤتمر العالمي لتنمية الاتصالات 2010 لمنطقة الدول العربية، دمشق سوريا 7 19 جانفي 2010؛ .

3؛) الوثائق الصادرة عن القمة العالمية لمجتمع المعلومات جنيف 003؛ و تونس 2005 الإتحاد الدولي للإتصلات 006؛ .

4؛) دليل لوضع إستراتيجية وطنية للأمن السبيراني إلتزام إستراتيجي بالأمن السبيراني مشاركة جماعية لكل من : الإتحاد الدولي للاتصالات، البنك الدولي، أمانة الكومنولث منظمة الكومنولث للإتصلات ، مركز التميز التعاوني للدفاع السبيراني التابع لحلف الأطلسي.(ب ت ن).

5؛) الصباحي نسرين ، الحروب السبيرانية وتحديات الأمن العالمي، ملف نشر بالمركز العربي للبحوث والدراسات، سبتمبر 2017.

6) المؤشرات الأساسية لتكنولوجيا معلومات والاتصالات، لجنة الأمم المتحدة الاقتصادية والاجتماعية لغربي آسيا الإسكوا، 2010 .

7) إرشادات الإسكوا للتشريعات السبيرانية(مشروع تنسيق التشريعات السبيرانية لتحفيز مجتمع المعرفة في المنطقة العربية) لبنان 2012 .

8) ليون برخو، الهاكطولوجيا ودورها في تفسير الهجمات الإلكترونية وتأثيرها على الممارسة الصحفية، دراسة إعلامية في مركز الجزيرة للدراسات، قطر، 2017 . http//studies aljazeera.net

9) موقع الجزيرة ، حسب " لوموند" الفرنسية الصين زرعت أجهزة تجسس بمقر الاتحاد الافريقي، http//aljazeera.net ، بتاريخ 18 /1 /2018 ، تم الاطلاع عليه يوم 4/ 5/ 2021.

10) كحال كمال، لمخاطرها العالمية ... الجزائر تمنع تداول البيتكوين بنهاية 2017 العربي الجديد http://alaraby.co.uk ، تم الاطلاع عليها بتاريخ 4/ 5/ 2021.

11) بلحيمر عمار، وزير الاتص ل الناطق الرسمي للحكومة، في حوار مع جريدة الشروق اليومي، بتاريخ 5 فيفري 2021 حول التهديدات السبيرانية.

فهرس الجداول

الفهرس