مجلة الرواق للدراسات الاجتماعية والإنسانية | ISSN: 2437 - 0363 EISSN 2602-6767 | المجلد 08 / العـدد:02 (2022)، ص 249- 267

الأمن السيبيراني الوطني: قراءة في أهم الإستراتيجيات الأمنية و التقنية لمواجهة الجريمة الإليكترونية بالجزائر.

National Cyber Security : A reading of the most important Security and technical strategies to confront cyber-crime in Alegria.

الدكتور : سمير قلاع الضروس
جامعة غرداية (الجزائر).
Hakimsamir.3816@gmail.com

تاريخ الاستلام: 2022/09/14 تاريخ القبول: 2022/12/07 تاريخ النشر: 2022/12/28

ملخص:

تشكل الدراسات المتعلقة بالأمن السيبيراني والجريمة الإليكترونية إحدى أهم المحاور و الملفات البحثية التي أولى لها الباحثين و الدارسين في الأوساط الأكاديمية ، كما يولي لها النخب و صناع القرار السياسي و الأمني و العسكري إهتماما بالغا وواسعا نظرا لخطورته و تأثيره على سيادة الدول و أمنها ، وعليه سنحاول البحث في هذه الورقة معرفة أهمية الأمن السيبيراني و الجريمة الإليكترونية، محاولين إسقاط هذه المفاهيم على الجزائر من خلال محاولة رصد الأبعاد الإستراتيجية لهذين المفهومين وصولا للبحث في أهم التحديات والإستراتيجيات الأمنية و التقنية لمواجهة الجريمة الإليكترونية التي تحمي الأمن السيبيراني الوطني الجزائري، باعتباره الهدف الذي تسعى تحقيقه النخب العلمية و صناع القرار السياسي و الأمني.

كلمات مفتاحية: الأمن السيبيراني ، الجريمة الإليكترونية، الجزائر ، الإستراتيجية الأمنية.

Abstract:

Studies on cyber security and cyber crime to day are considered one of the most important filrs and themes that reasearchers and political and military decision-makers within the country are interested in due to its sériousness and its impact on the sovereignty of country , Accordingly , we will try to reasearch in this paper the importance of cyber security and cyber-crime , and we trying to drop these concepts on Algeria .

Proceeding from the most important challenges security and technical strategies to confront the cyber-crime that protects the Algerian national cyber security, as it is the goal that the scientific elites and political , security decesions-makers seek to achieve .

Keywords: Cyber security , Cyber crimes, Algeria, Security strategy.

* المؤلف المرسل

1. مقدمة:

أدت نهاية الحرب الباردة إلى بروز العديد من التحولات التي أثرت على طبيعة الدول، نظير التطورات الحاصلة في المشهد الدولي، مما زادت في فاتورة التحديات والتهديدات التي لم يشهدها العالم من قبل، والتي تعرف بالتهديدات اللاتماثلية العابرة للحدود التي لا تعترف بقيمة الحدود ولا بسيادة الدولة الوطنية أو ما يسمى بأطروحة "الدولة القومية"، ومن أبرز هذه التهديدات نجد الحروب البيولوجية والإليكترونية والسيبيرانية، والتي شغلت هذه التهديدات رأي الباحثين و مراكز الفكر و أكبر المؤسسات الإعلامية و المخابر الإستخباراتية والتي توصلت لنقطة محورية هامة مفادها كلما امتلكت الدولة القوة المعرفية والتكنولوجية والمعلوماتية كلما ارتفع مؤشر أمنها القومي والوطني وزادت مكانتها بين الدول في العالم.

ومع انفجار الثورة المعلوماتية ودخول العصر الرقمي في القرن 21 ، وما نتج عنه من معطيات وتداعيات جديدة أنتجت جملة من الجرائم السيبرانية Cyber-crime ما جعلها تشغل بال الساسة والقادة وحتى النخب الأكاديمية في كل الدول بدون استثناء و بالخصوص الجزائر في السنوات الأخيرة التي أصبحت تولي إهتماما واسعا لهذا الموضوع، خاصة بعد ما صنف المختصين بأن الفضاء السيبراني يعتبر بمثابة المجال الخامس في الحروب بعد البر والبحر والجو والفضاء وصولا للفضاء الرقمي السيبيراني وهو ما استدعى بضرورة خلق أطر حماية أمنية للدولة و أنظمة المعلومات والمؤسسات الأمنية والشركات الاقتصادية داخل الجزائر، ما جعلنا نركز في هذه الورقة في البحث على أهم الإستراتيجيات الأمنية و التقنية لمواجهة الجريمة الإليكترونية بالجزائر خاصة الخارجية قصد تعزيز الأمن السيبيراني الوطني. و تأسيسا على هذا نطرح الإشكالية التالية :

- **ما هي أهم الإستراتيجيات الأمنية و التقنية لمواجهة الجريمة الإليكترونية التي تحمي الأمن السيبيراني الوطني بالجزائر؟**

و عليه، تتأسس الفرضية المحورية لهذه الورقة من خلال تحديد طبيعة العلاقة بين الأمن السيبيراني كآلية و الجريمة الإليكترونية كتهديد، فكلما زاد الإهتمام بالأمن السيبيراني كلما نقص التهديد المتعلق بالجريمة الإليكترونية داخل الجزائر. و سنحاول تفكيك هذه الفرضية البحثية بناءا على منهج تحليلي قائم على فهم متغيري الأمن السيبيراني و الجريمة الإليكترونية وصولا لتحليل واقع الأمن السيبيراني وأبعادها الإستراتيجية في الجزائر، و استخلاصا بقراءة لأهم التحديات والإستراتيجيات الأمنية والتقنية لمواجهة الجريمة الإليكترونية التي تحمي الأمن السيبيراني الوطني بالجزائر.

2. الأمن السيبيراني والجريمة الإليكترونية: قراءة إجرائية ومفاهيمية.

شهدت التحولات الدولية تطورات سريعة وتراكمات خطيرة على الأمن الدولي، ما أدى هذا التحول والتهديد والخطر لتغيير مفهوم الأمن من بعده الكلاسيكي الصلب إلى الأمن اللين اللاتماثلي والرقمي، ومن الإهتمام الأكاديمي لمحاولة فهم التهديد على مستوى الأمن الوطني للدولة ميدانيا إلى محاولة فهم تهديد الدولة في منظومتها الإليكترونية و السيبيرانية، التي أضحت جزء مهم لا يتجزأ من الأمن القومي للدولة، و الذي يُعرّف بأنه" مجموعة من الإجراءات المتخذة في مجال الدفاع ضد الهجمات السيبرانية ونتائجها التي تشمل تنفيذ التدابير المضادة المطلوبة.[1] (قارة، 2019).

ويعتبر الأمن السيبراني من بين التحديات الأمنية المعاصرة التي لاقت إشكالا عويصا في فهمه ومسايرته خاصة بالنسبة للدول ، ما جعلها بعدا مفاهيميا تجدر دراسته من طرف الأوساط الأكاديمية و المعرفية و إيجاد نسق معرفي يسهل على صانع القرار إيجاد الحلول و الإفاق على المستوى الإمبريقي التحليلي .[2] (محمد، 08 جوان 2019)، باعتبار الجزائر من بين الدول التي دخلت مصاف الإدارة الإلكترونية و العالم السيبراني، مما ترتب عليه إنعكاسات أدى بالدولة الجزائرية إلى تبني إصلاحات و إستراتيجية أمنية

لتحقيق أمنها السيبراني في الفضاء السيبيري ، وهذا ما ذهب إليه الكاتبان "ليثو مارتي"Lehto Martti, "نيتانماكي بيكا" Neittaanmäki Pekka كتابهما الموسوم Cyber Security Analytics, Technology and Automation ، حيث اعتبرا الأمن السيبراني بمثابة مجموعة من الإجراءات التي اتخذت في الدفاع ضد هجمات قراصنة الكمبيوتر وعواقبها، ويتضمن تنفيذ التدابير المضادة المطلوبة، بينما عرّفه إدوارد أمورسو Amoroso Edward بأن الأمن السيبيراني وسيلة من شأنها الحد من خطر الهجوم على البرمجيات أو أجهزة الحاسوب أو الشبكات، وتشمل تلك الوسائل الأدوات المستخدمة في مواجهة القرصنة وكشف الفيروسات ووقفها، وتوفير الاتصالات المشفرة[3]".(قارة، الأمن السيبيراني).

وبالتالي فإن الأمن السيبراني في مفهومه العام هي استراتيجية عمل تقوم بها الدول أو بعض الهيئات المختصة في حماية الأنظمة والبرامج من الهجمات الرقمية التي تهدف عادة إلى الوصول إلى المعلومات الحساسة وإعادة تغييرها أو إتلافها أو ابتزاز هذه المؤسسات والدول بمقابل مالي، بالمقابل ينتهج الأمن السيبراني الناجح نهجاً معيناً يتكون عادة من استراتيجيات واجهزة عالية التدفق و أنظمة حماية مرتبطة بأجهزة الكمبيوتر أو البرامج أو البيانات و البيانات المضادة والاحتياطية في حالة أي اختراق التي تنوي بعض الأطراف الوصول إليها من خلال خرق البيانات و كلمات السر [4](لطفي،الجهود الدولية في مجال مكافحة جرائم الارهاب السيبراني: التجربة الماليزية نموذجا، الشتاء 2022،) مما جعل الكثير من الدول خاصة الكبرى كالولايات المتحدة الأمريكية و روسيا ترتبك من كبار الهاكرز و المخترقين في ضرب أنظمة البيانات والمعلومات كقضية ملفات باناما بايبرز Panama Papers التي أحدثت ضجة عالمية و ارتباكا في الأوساط السياسية الأمريكية.

عموما يمكن القول بأن الأمن السيبراني يهتم بأمن الفضاء الإفتراضي والرقمي والتكنولوجي والإتصالي والتواصلي و كل مايتعلق بعالم السايبرانية والذي عرفته الوكالة الفرنسية لأمن أنظمة الإعلامANSSI ، وهي وكالة حكومية مكلفة بالدفاع السيبراني الفرنسي، بأن الأمن السيبيراني هو فضاء التواصل المشكل من خلال الربط البيني العالمي لمعدات المعالجة الآلية للمعطيات الرقمية، كما أن هناك مَن عرّف الفضاء السيبراني بوصفه الذراع الرابعة للجيوش الحديثة، وبالتالي يمكن القول بأن الأمن ينتج عنه مقاربة استباقية دفاعية تتمثل في الردع السيبراني الذي يعرف بأنه" منع الأعمال الضارة ضد الأصول الوطنية في الفضاء والأصول التي تدعم العمليات الفضائية"، ويرتكز الردع السيبراني على ثلاث ركائز هي (ROHIT CHATTERJEE، 2021.)[5]، و هي كالتالي: مصداقية الدفاعCredible Defense ، القدرة على الانتقام An Ability to Retaliate، والرغبة في الانتقام.A Will to Retaliate . ومن أبرز النماذج ظاهرة الويكيليكس "Wikileaks" الذي نجح في نشر ملايين الوثائق السرية للإدارة الأمريكية وقنصلياتها، ما خلق مشاكل دبلوماسية بين الولايات المتحدة الأمريكية وحلفائها و أسس لحروب الإنترنت والحرب السيبرانية cyber war من خلال التأسيس لمفهوم الأمننة the process of securitization ، من خلال دعم القدرات التكنولوجية في مقاومة التهديدات المتعمدة وغير المتعمدة والاستجابة و حماية الشبكات وأجهزة الكمبيوتر[6] (What is Cyber Security؟، 2021/11/9)، والبرامج والبيانات من الهجوم أو الضرر أو الوصول غير المصرح به خاصة تلك الأجهزة الحكومية الرسمية التي تحمل معطيات أمنية حول الوطن والمواطن.

عموما فإن أهمية الأمن السيبراني يقوم على تامين المعلومات الحساسة البالغة لأهمية الدول الأفراد على حد سواء المعرضة للخطر والاختراق والاستيلاء كي تحافظ على الأمن الوطني وحفظ وحماية السرية والخصوصية للبيانات الشخصية للمواطنين ، من

خلال تعزيز حماية أنظمة التقنيات التشغيلية على كافة الأصعدة ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات وما تحويه من بيانات، والتصدي لهجمات وحوادث امن المعلومات التي تستهدف الأجهزة الحكومية ومؤسسات القطاع العام والخاص وتوفير بيئة أمنة موثوقة للتعاملات في مجتمع المعلومات، ومقاومة البرمجيات الخبيثة، ما تستهدفه من أحداث أضرار بالغة للمستخدمين وصولا للحد من التجسس والتخريب الإلكتروني على مستوى الحكومة والأفراد.[7](شلوش ،2018).

3. واقع الأمن السيبيراني و أبعادها الإستراتيجية في الجزائر.

ما يمكن أن نؤكده في دراستنا هذه بأن الجزائر أصبحت تولي أهمية بالغة وواسعة للأمن السيبيراني خاصة لدى المؤسسات و الأجهزة الأمنية باعتبارها مطلبا ضروريا لكل الدول دون استثناء، و مطلبا أكثر إلحاحا للدول التي أصبحت توظف البعد التكنولوجي والرقمي و الإفتراضي في تسييره للشأن العام محليا داخليا إقليميا و دوليا، لأنه يتعلق بالحماية من المخاطر المحتملة عن طريق مصادر خارجية من خلال الإنترنت بالدرجة الأساس ، كون الكثير من الأطراف تسعى لضرب إستقرار الدول و سلامة أراضيها من خلال الإختراقات الرقمية و التكنولوجية ، والجزائر ليست ببعيدة عن هذه التهديدات.

و تأسيسا على ما سبق يمكن القول بأن الأمن السيبيراني أضحى مركز اهتمام النخب السياسيين و صناع القرار حيث أصبح يعمل مختصو الأمن السيبراني على ضمان عدم السماح لأحد غير مصرح له بالدخول والوصول إلى المعلومات كالأشخاص الغرباء على أي هيئة و مؤسسة حفاضا على بعض المارقون الذين يمارسون الجرائم الإلكترونية يقومون بنشر الفيروسات و الغاية منه هو حماية الحاسب كله من المصادر الخارجية وأمن المعلومات ، فهو يهتم بحماية كل ما يتعلق بالمعلومات ضمن الحاسب أو خارجه وليس

حماية الحاسب كله من أي خطر خارجي محتمل كالسرقة والاختراق، ويمنع أي شخص غير مصرح له بالوصول إليها من ذلك.

وفي ما يخص أهم الأبعاد الإستراتيجية التي تنتج عن الأمن السيبراني في الجزائر فإنه يطال جميع المسائل الاقتصادية والسياسية والعسكرية والاجتماعية والإنسانية، وعليه فإنه قبل الحديث عن هذه الأبعاد سنحاول البحث عن انعكاسات الأمن السيبيراني على الفضاءات الرقمية الجزائرية في مجابهة المخاطر والتحديات السيبرانية من خلال تكييف المنظومة الأمنية مع التحولات الجيواستراتيجية الإقليمية والعالمية، فالتهديدات السيبرانية أصبحت بشكل غير مسبوق من أكثر القضايا أهمية وإلحاحا بالنسبة للأمن الوطني الجزائري فقد عقدت عدة مؤسسات رسمية أمنية عسكرية عدة ندوات ولقاءات في السنوات الأخيرة من أجل بحث و فهم الأمن السيبيراني ومخاطر الجريمة الإليكترونية وانعكاسها على الأمن الوطني الجزائري، ولذا وجب دعم استراتيجية الامن والدفاع الجزائرية مع الأخذ بعين الاعتبار درجتها من الأكثر إلى الأقل جدية، وتكييفها حسب المتطلبات المستقبلية لمواجهة التهديدات حسب درجة خطورتها، والتركيز في بناء هذه المنظومة الأمنية على احتمال ما سيقوم به الفاعلون الاخرون، كون الدولة من خلال قطاع التعليم العالي أولت إهتماما بالغا وواسعا لتخصصات المتعلقة بالإعلام الآلي و الإقتصاد الرقمي و السيبيرانية وهذا من أجل التعاطي مع كل التهديدات وفق منطق علمي إستباقي قائم على مبدأي التوقع والاحتمال من خلال التركيز على الأبعاد الإسترانتيجية للأمن السيبيراني في الحفاظ على المنظومة الأمنية الجزائرية وهم كالتالي:

1.3 البعد العسكري وضرورة تقوية المنظومة الأمية الإليكترونية: من خلال ربط الوحدات العسكرية ببعضها البعض عبر العالم الافتراضي، وهذا ما يسهل عملية تبادل المعلومات الذي ينعكس إيجابا على تحقيق الأهداف العسكرية وحماية القدرات

الدفاعية وحتى الهجومية للدولة، والترسانة العسكرية والنووية للدولة من خلال مجموعة البرامج التقنية والتكنولوجية، التي تسهر من أجلها الوحدات الإليكترونية بالاعتماد على تقنيين ساميين ذو تكوين عالي في المعلوماتية ، وبالتالي ربط القوة العسكرية بالتطور التكنولوجي مهم جدا ولكن الأهم هو آليات الحماية والدعم الرقمي لأمننة هذا التطور.[8] (Martti)

2.3البعد الاجتماعي وتأمين منصات التواصل الاجتماعي من المخاطر الخارجية: ساهمت صفحات التواصل الاجتماعي في خلق فضاء تواصلي غير عادي ومسبوق ما جعل أسهم المخترقين ترتفع من خلال البحث عنهم واستخدامهم في خلق برامج مضادة ضد هيئات ومؤسسات وفتح باب الحروب الافتراضية بين الجماعات البشرية داخل الدولة خاصة الدول التي تحمل إيديولوجيات و هويات متناقضة، حيث تمثل مشاركة جميع شرائح المجتمع في هذه الحروب خطرا على الأمن العام للدولة و فرصة لهذه الجماعات من أجل الاطلاع على الأفكار والمعلومات المختلفة ، وعليه فلابد من العمل على توعية المواطن بهذه المخاطر لتحقيق الأمن السيبراني في بعده الاجتماعي.[9](الأمن السيبيراني :الهجمات السيبرانية. ماي 2021).

3.3 البعد السياسي وهدف تحقيق الحكومة الإليكترونية: تشكل السياسة عصب الحياة لدى الدول والمجتمعات، ما يجعل الكثير من الصراعات السياسية الحاصلة في ارض الواقع تتحول إلى صراعات إفتراضية من جهة ما يخلق نوع من الحروب لكسب الطرف الآخر، خاصة في السنوات الأخيرة أين أصبح توظيف القوة السيبيرانية سلاح مهم للتغلب على الخصم السياسي، من خلال تنفيذ لأجندات وسياسات خاصة من خلال ضرب المنظومة التكنولوجية .[10] (الزهراني، شتاء 2017).

4.3البعد الاقتصادي والتوجه نحو الإقتصاد الرقمي: أصبح رهان الجزائر والشركات الإقتصادية الكبرى والمؤسسات الأمنية والعسكرية تعمل على تطوير قدراتها العلمية

والسيبيرانية من أجل تجنب أي محاولات اختراق خاصة في ظل الصراعات الإقليمية للجزائر مثلا مع الجارة المغرب ما يجعل الجزائر تركز وتهتم بشكل كبير على حفاظها على الأمن الإليكتروني والرقمي داخل مؤسساتها الرسمية بالجزائر ومكافحة ما يسمى بالجريمة الإليكترونية[11] (مرعي، 9. أغسطس 2016)، وهذه الجريمة غاليا تأتي من طرف دول تختلف مع الجزائر في توجهاتها السياسية و الإيديولوجية، وعلى صعيد البورصة والتداولات المالية من خلال حماية لرقم الأعمال الذي تحوز عليه الجزائر، ما جعل هذه الأخيرة ترتبط بالأمن السيبراني ارتباطاً وثيقاً بالأمن بالدرجة الأولى و الاقتصاد بعدها، فالتلازم واضح بين اقتصاد المعرفة وتوسع استخدام تقنيات المعلومات والاتصالات والتي تتيح تعزيز التنمية الاقتصادية لبلدان كثيرة عبر إفادتها من فرص الاستخدام التي تقدمها الشركات الدولية والشركات الكبرى التي تبحث عن إدارة كلفة إنتاجها بأفضل الشروط[12] (الزهراني.).

وبالتالي يمكن القول بأن هذه الأبعاد الإستراتيجية السالفة الذكر وجب التركيز عليها و الإهتمام بها بشكل دقيق خاصة البعدين العسكري الذي يعتبر الواجهة الأمنية للدولة و البعد الإقتصادي من خلال تعزيز نظام التأمين للحفاظ على المعلومات الخاصة بالدولة بعيدا عن أي خطر للإختراق، و قصد تمكين هذه الأبعاد الإستراتيجية وجب تكوين وخلق جيل رقمي يفهم و يستوعب المخاطر الأمنية الناتجة عن الجرائم الإليكترونية.

4. أهم التحديات والإستراتيجيات الأمنية والتقنية لمواجهة الجريمة الإليكترونية التي تحمي الأمن السيبيراني الوطني بالجزائر.

كما أبرزنا في المحورين السابقين بضرورة الإهتمام بالأمن السيبيراني الذي أصبح عنصرا هاما من عناصر تقوية أمن الدول، خاصة و أن العالم كله أصبح يتجه نحو الفضاء السيبيراني خاصة مع التطورات الدولية[13] (Geers، 2010)، وما تبعها من

إجراءات إحترازية أثناء وباء كورونا وسيتجه أكثر بعد الوباء في السنوات القادمة، ما يحعل كل الدول بما فيها الجزائر قريبة من أي تهديد سيبيراني كون الجزائر ليست معزولة عن جملة من التحديات التي تعاني منها بقية الدول وبالخصوص تلك الدول التي تعتمد على الفضاء الرقمي كوسيلة هامة للتواصل و التنسيق و التعاون وحتى في الإستخدامات اليومية داخليا أو خارجيا، وعليه يمكن حصر مجموعة من التحديات الأساسية التي تعاني منها الجزائر كدولة وهي كالاحتيال الرقمي والافتراضي بتوظيف معطيات وبيانات تكنولوجية توهم الآخر قصد التخطيط لجرائم إليكترونية، واستخدام أجهزة الكمبيوتر وشبكة الإنترنت للحد من سرقة البيانات والمعلومات الخاصة والرسمية وكل القضايا المتعلقة بجرائم القرصنة و إنشاء مواقع للبرامج المقرصنة .[14] (الزهراني، امرجع سبق ذكره)

وفي إطار السياسات التي وجب انتهاجها الجزائر خاصة في السنوات الأخيرة مع تزايد الحروب الإليكترونية يجب على الجزائر ومنظومة الأمن الوطني الجزائري أن تركز بشكل كبير على تكوين إطارات عالية المستوى في مجال السيبيرانية و الهاكرز و تعزز إستراتيجياتها في مجال التكوين في الهجمات السيبرانية والردع السيبيراني كآلية إستباقية و ووقائية أمنية جزائرية، للحفاظ على منظومات المعلومات الوطنية و خاصة أن الجزائر مؤخرا إنخرطت في عالم الرقمنة و الحكومة الإليكترونية ، كون يمكن للهجمات السيبرانية التي تأتي من أطراف داخلية أو أجنبية أن تسبب في دمار هائل يمس الأمن القومي للدولة، وهذا ما يجب أن تحذر منه الجزائر في السنوات المقبلة لأن الأمن الوطني و القومي أصبح يرتبط بالأمن الإليكتروني و الرقمي للدول من خلال استهداف أنظمة المعلومات المؤسسات الرسمية السياسية و المالية و النقدية و الإقتصادية و الأمنية بالخصوص.

ومنه أصبح لزاما على الجزائر أن تتبنى سياسات عالية الدقة و الإحتراف في مجال الردع الرقمي و الهجمات السيبيراني كآلية وميكانيزم للحفاظ على مقومات الأمن القومي الوطني من خلال تطوير من قدرات وظائف شبكة الكمبيوتر، ومحاولة استغلال نقاط ضعف الدول التي تسعى إختراق المنظومة الأمنية الإليكترونية من خلال نظام المعلومات الذي هو إتاحة المعلومات وضمان سلامة الدولة ومعرفة خبايا على الدول الأخرى. ولعل أبرز أنواع الهجمات و الدفاع الذي يندرج في إستراتيجية وقائية و استباقية أمن المعلومات ما يلي[15] (البهي، 2017):

- **الهجمات السرية :** وتعد أحد أنواع التجسس باستخدام وسائل التكنولوجيا الفائقة؛ كالهجمات السيبرانية المتطورة التي تطلق من قبل الدول أو الجماعات الإجرامية التي تقع ضمن هذه الفئة.
- **الهجمات المتكاملة:** تتمثل في تخريب نظم معلومات الخصم المدنية أو العسكرية الهامة. فيمكن أن ينطوي التخريب على التلاعب بالبيانات داخل نظم المعلومات التي يمكن أن تشوه وعي العدو عن طريق نشر معلومات خاطئة داخل أنظمة ذكائه، أو إخفاء أنشطة محددة قد تكون تحت المراقبة.

وعلى ضوء ما سبق، يمكن تحديد أهم الإستراتيجيات و الإجراءات الأمنية مواجهة الجريمة الاليكترونية و تأمين الأمن السيبيراني من خلال تقوية الأجهزة الخاصة بالأمن الإليكتروني علما أن الجزائر حاليا تحوز على[16] (بارة، 2017):

1.4 مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية للدرك الوطني: والذي تأسس سنة 2008 حيث عالج العديد من القضايا المتعلقة بالتهديد الإليكتروني و قضايا الإختراق و الهاكرز الذي تؤرق أنظمة المؤسسات الأمنية و الإقتصادية بالخصوص.

2.4 المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني ببوشاوي الجزائر العاصمة والتي تختص في التحري و التحقيقات المتعلقة بالجرائم الجنح والجنايات والتي تعتمد على وسائل تقنية عالية الدقة والمستوى.

3.4 المصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة للأمن الوطني التي أنشئت سنة 2011 والتي عالجت هي أيضا الكثير من الجرائم خاصة تلك المتعلقة بصفحات التواصل الإجتماعي ، و بعدها تم إلحاقها لمديرية الشرطة القضائية سنة 2015 قصد التحري أكثر في الجرائم التي تهدد الأمن الوطني كالقضايا التالية [17] (عز الدين، نوفمبر 2015)، التهديد و جرائم المساس بالنظام العام و الإعتداء على الحياة الخاصة للمواطن والإرهاب و الجريمة الإليكترونية و قضايا تحريض القصر على الفسق و الدعارة وجرائم المساس بأنظمة المعلومات و الهاكرز ، إهانة هيئة نظامية و رموز الدولة و النصب و الإحتيال و التحرش الجنسي ضد القصر.

4.4 الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال حيث تشكلت هذه الهيئة بمقتضى المرسوم الرئاسي رقم 261-15 وهي سلطة إدارية مستقلة لدى وزير العدل، تعمل تحت إشراف ومراقبة لجنة مديرية يترأسها وزير العدل وتضم أساسا أعضاء من الحكومة معنيين بالموضوع ومسؤولي مصالح الأمن وقاضيين من المحكمة العليا يعينهما المجلس الأعلى للقضاء ، حيث كلفت هذه الهيئة بإقتراح عناصر الإستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات العالم والاتصال ومكافحتهما وتنشيط وتنسيق عمليات الوقاية منها، ومساعدة السلطات القضائية ومصالح الشرطة القضائية في مجال مكافحة هذه الجرائم، من خالل جمع المعلومات والتزويد بها ومن خلال الخبرات القضائية، وضمان المراقبة الوقائية للاتصالات الإلكترونية، قصد الكشف عن جرائم المتعلقة بالأعمال الإرهابية والتخريبية والمساس بأمن الدولة وقد نص سابقا على إنشاء هذه الهيئة المادة 13 من القانون 09/04 المؤرخ في أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم

المتصلة بتكنولوجيا الإعلام و الإتصال ومكافحتها من خلالها تنشأ هيئة وطنية وتنظيمها وكيفيات سيرها عن طريق التنظيم.[18] (عطية، بدون عدد)

وعليه أصبح لزاما اليوم أكثر من أي وقت مضى بضرورة تركيز العمل القضائي والتنسيق الأمني والعسكري في مكافحة الجرائم الداخلية وتعزيز دور الثقافة السيبيرانية و التكوين العالي في مجال حفظ أنظمة المعلومات و الأمن السيبيراني لدى منتسبي مؤسسات الدولة كجهاز العدالة، مؤسسة الدرك الوطني و الأمن الوطني، إلا أن الجزائر أصبح لزاما عليها التركيز و الاهتمام بما يحيطها من تهديدات إقليمية ودولية. وهذا من خلال الإعتماد على مجموعات من الإستراتيجيات الضرورية لتقوية المنظومة السيبيرانية الجزائرية و التي تتمثل في ما يلي[19]: (جبور الاشقر.)

- إلزامية تفعيل جدار الحماية fire well من خلال البصمة الإليكترونية والتوقيع الرقمي و تقوية أنظمة الباسوورد Password وهي تقنيات تفيد تعزيز الحماية وعدم الاختراق وعدم تزوير الرسائل الإلكترونية من خلال وضع سياسة أمنية عالية الدقة للمؤسسات والأجهزة التي تؤشر لوجود مواقع إرهابية و إجرامية خاصة في المؤسسات الإقتصادية والبنوك و البورصة و المؤسسات الرسمية خاصة الوزارات ومؤسسة الرئاسة وكل الهيئات الرسمية التي تحوز على الأرقام و الإحصائيات كمجلس المحاسبة و المجلس الوطني الاقتصادي الاجتماعي والبيئي والبرلمان بغرفتيه.

- وضع برامج للحماية من الفيروسات و هذا كله بمراسيم تنظيمية و يمكن للدولة أن تدعم هذه العملية بتخفيض أسعار هذه البرامج فمثلا في الجزائر نجد أن أسعار الحماية من الفيروسات ليست في متناول الحميع . كتطبيق KESPERSKEY في كل الأجهزة و الحواسيب.

- تفعيل الإجراءات القانونية الخاصة بمكافحة الهاكرز و اختراق الأنظمنة قانونيا و إرساء ترسانة قانونية تحمي المواطن والشركة والدولة، و هذا العمل من صلاحيات المصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة للأمن الوطني ومركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية للدرك الوطني، وعلى الصعيد الدولي وجب على الدولة توقيع كل الاتفاقيات التي بامكانها حماية الأنظمة الرقمية والافتراضية داخل الدولة من خلال رسم سياسات دولية تفرض عقوبات صارمة على مرتكبي جرائم الإنترنت إذ يستلزم التدخل الحكومي والدولي نظرا للأخطار الكبيرة التي تعترض الدول والمؤسسات[20]. (الصادق، ماي 2017)

- خلق جيل رقمي قائم على تكوينه جيدا في مجال التربية الإليكترونية والسيبيرانية باعتبارها ضرورية وملحة للأجيال القادمة نظرا لمعادلتها الحياتية في الاجيال المقبلة، من خلال العمل على توعيتهم في آليات استخدام الأنترنت ونصحهم بخطر الجرائم الإلكترونية وكل ما يترتب عليها من مخاطر و أبعاد أمنية وسياسية و اقتصادية واجتماعية كما ذكرناها سابقا، إضافة بالتركيز على التكوين القوي والفعال لكل الباحثين داخل الجامعات من خلال تشجيع مراكز البحث والفرق العلمية و مراكز التكوين الجزائرية و الإطارات و الأجهزة الأمنية .

5. خاتمة:

وكحوصلة عامة لموضوعنا هذا يمكن القول بأن الأمن السيبيراني يعتبر بعد مهم من أبعاد الأمن التي حددها تقرير التنمية البشرية للأمم المتحدة و هو الأمن الذي يأتي مباشرة بعد الأمن الإنساني، ما يجعلنا نقر بأن قوة الدولة في حفاظها على كل عناصر الأمن و أبعادة الإستراتيجية وبالخصوص الأمن القومي مهما كانت مساحتها وعدد سكانها والأمن الإنساني بكل أبعاده ومستوياته والأمن السيبيراني إلا أنه يبقى الإهتمام

بالمقدرات الدفاعية السيبيرانية و حفظ أمن المعلومات عنصر مهم وجب على الجزائر التركيز عليه في السنوات القادمة لأنه أصبح أمر مهم من أجل مواجهة الحروب الإليكترونية التي أصبحت تزداد يوميا مع اهتمام العالم والدول والمؤسسات والحكومات والهيئات بالفضاء الإليكتروني والرقمي خاصة بعد مرحلة الوباء لأن العالم الذي سيأتي مستقبلا حسب تقديرات خبراء تكنولوجية الإعلام و الإتصال سيكون عالما رقميا إفتراضيا و سيبيرانيا بامتياز، ما يجعل للجزائر بضرورة رسم إستراتيجية مهمة وضرورية للحد من الجريمة الإليكترونية و اختراق المنظومة الاليكترونية للدولة التي تعتبر عنصر هام من عناصر السيادة بالنسبة للدولة.

6. الهوامش:

1- فارس قارة ، الأمن السيبيراني ، متحصل على المقال من موقع الموسوعة السياسية والمنشور يوم 12 مارس 2019، من خلال الرابط الاليكتروني التالي :
https://politicalencyclopedia.org/dictionary/%D8%A7%D9%84%D8%A3%D9%85%D9%86%20%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%

2- صخري محمد ، الأمن السيبراني: الإستراتيجية الجزائرية للأمن و الدفاع في الفضاء السيبيري، مقال متحصل من الموقع الاليكتروني الموسوعة الجزائرية للدراسات السياسية والاستراتيجية ، منشور يوم 08 جوان 2019 عبر الرابط الاليكتروني التالي:
https://www.politics-dz.com/%D8%A7%D9%84%D8%A3%D9%85%D9%86-6

3- فارس قارة ، الأمن السيبيراني ، مرجع سبق ذكره.

4- وفاء لطفي، الجهود الدولية في مجال مكافحة جرائم الارهاب السيبراني: التجربة الماليزية نموذجا، جامعة القاهرة، مجلة كلية الإقتصاد والعلوم السياسية، المقالة 5، المجلد 23، العدد 1 - الرقم المسلسل للعدد 90، الشتاء 2022، الصفحة 178-151 .

5- ROHIT CHATTERJEE, "Difference Between Cybersecurity & Information Security", Published in analytics india mag, 5/3/2020, Retrieved 16/11/2021. p 03 .

6- What is Cyber Security? Definition and Best Practices", itgovernance, Retrieved 9/11/2021. Edited.by web site : https://www.itgovernance.co.uk/what-is-cybersecurity

7- شلوش، نورة ، القراصنة الإلكترونية في الفضاء السيبراني : التهديد المتصاعد لأمن الدول، العراق : مجلة مركز بابل للدارسات الإنسانية المجلد 8 العدد 2018،2. ص 66.

8- Lehto Martti , Neittaanmäk Pekka .Cyber Security: Analytics, Technology and Automation. Switzerland : Springer International Publishing, 2015,published in web site : https://www.pdfdrive.com/cyber-security-analytics-technology-and-automation 27098885.html

9- تقرير منشور من طرف مركز سيتا التركي للدراسات السياسية ، الأمن السيبيراني :الهجمات السيبرانية.. حروب غير مرئية منشور في 10 ماي 2021 ومتحصل على التقرير بشكل مفصل عبر الرابط الإليكتروني التالي:

HTTPS://WWW.IFEGYPT.ORG/NEWSDETAILS.ASPX?PAGE_ID=1244&PAGEDETAILID=1324#:~:TEXT=%D9%88%D9%82

10- يحي مفرح الزهراني، الأبعاد الإستراتيجية و القانونية للحرب السيبيرانية، السعودية : مجلة البحوث والدراسات ، جامعة نايف للعلوم الأمنية، العدد 23 ، السنة 14، ستاء 2017، ص 226.

11- اسراء جبريل رشاد مرعي، الجرائم الإلكترونية : الأهداف – الأسباب – طرق الجريمة ومعالجتها، برلين: المركز الديمقراطي العربي، مقال منشور في موقع المركز يوم 9. أغسطس 2016، متحصل على المقال من خلال الرابط الاليكتروني التالي : https://democraticac.de/?p=35426

12- يحي مفرح الزهراني، مرجع سبق ذكره، نفس الموقع الاليكتروني.

13- Kenneth Geers, The Challenge of Cyber Attack Deterrence, *Computer Law & Security Review*, No. 26, 2010, pp. 298-303.

14- يحي مفرح الزهراني، مرجع سبق ذكره، ص 244.

15- رغدة البهي، الردع السيبراني: المفهوم والإشكاليات والمتطلبات، Cyber Deterrence: The Concept, Dilemmas and Requirements، برلين : المركز الديمقراطي العربي، مقال

منشور يوم 21 فيفري 2017، مجلة العلوم السياسية والقانون، متحصل على المقال من خلال الرابط الاليكتروني التالي :

https://democraticac.de/?p=43837#_ftn34

16- سمير بارة، الأمن السيبيراني في الجزائر السياسات و المؤسسات ، المجلة الجزائرية للأمن الإنساني ،العدد الرابع ، جويلية 2017، ص 270.

17- عز الدين عز الدين، الإطار القانوني للوقاية من الجرائم المعلوماتية ومكافحتها ، قيادة الدرك الوطني ، مداخلة بالملتقى الوطني الأول حول الجريمة المعلوماتية بين الوقاية و المكافحة ، جامعة محمد خيضر بسكرة 16 نوفمبر 2015، ص30.

18- إدريس عطية ، مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري ، جامعة العربي تبسي: مجلة المصداقية، بدون عدد ، ص114.

19- جبور منى الأشقر ، الأمن السيبراني: التحديات ومستلزمات المواجهة، مرجع سبق ذكره، ص05.

20- عادل عبد الصادق، أنماط الحرب السيربانية وتداعياتها على الأمن العالمي، مجلة إتجاهات النظرية، البنك العربي الإفريقي، 14ماي 2017 ،ص38.

7. قائمة المراجع:

- **المقالات:**

1. الزهراني، يحي مفرح، (شتاء 2017). الأبعاد الإستراتيجية و القانونية للحرب السيبيرانية، السعودية : مجلة البحوث والدراسات ، جامعة نايف للعلوم الأمنية، العدد 23 ، السنة 14. بارة، سمير ، (جويلية 2017) الأمن السيبيراني في الجزائر السياسات و المؤسسات ، المجلة الجزائرية للأمن الإنساني ،العدد الرابع .
2. عطية ، إدريس ، مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري ، جامعة العربي تبسي: مجلة المصداقية، بدون عدد .
3. عبد الصادق، عادل، أنماط الحرب السيربانية وتداعياتها على الأمن العالمي، مجلة إتجاهات النظرية، البنك العربي الإفريقي، (ماي 2017) .

4. لطفي، وفاء، الجهود الدولية في مجال مكافحة جرائم الارهاب السيبراني: التجربة الماليزية نموذجا، (شتاء 2022). جامعة القاهرة، مجلة كلية الإقتصاد والعلوم السياسية، المقالة 5، المجلد 23، العدد 1 - الرقم المسلسل للعدد 90،
5. نورة ، شلوش، (2018) .القراصنة الإلكترونية في الفضاء السيبراني : التهديد المتصاعد لأمن الدول، العراق : مجلة مركز بابل للدارسات الإنسانية المجلد 8 العدد 02 ،

- **المداخلات:**

6. عز الدين عز الدين، (16 نوفمبر 2015). الإطار القانوني للوقاية من الجرائم المعلوماتية ومكافحتها ، قيادة الدرك الوطني ، مداخلة بالملتقى الوطني الأول حول الجريمة المعلوماتية بين الوقاية و المكافحة ، جامعة محمد خيضر بسكرة .
7. شقر، منى، (2012) .الأمن السيبراني: التحديات ومستلزمات المواجهة، جامعة الدول العربية، ورقة بحثية المركز العربي للبحوث القانونية والقضائية، اللقاء السنوي في امن وسلامة الفضاء السيبراني.

- **مواقع الانترنيت:**

8. فارس قارة ، الأمن السيبيراني ، (12 مارس 2019) ، متحصل على المقال من موقع الموسوعة السياسية ، من خلال الرابط الاليكتروني التالي :
https://politicalencyclopedia.org/dictionary/%D8%A7%D9%84%D8%A3%D9%85%D9%86%20%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A
9. صخري محمد ، (08 جوان 2019) ، الأمن السيبراني: الإستراتيجية الجزائرية للأمن و الدفاع في الفضاء السيبيري، مقال متحصل من الموقع الاليكتروني الموسوعة الجزائرية للدراسات السياسية والاستراتيجية ، عبر الرابط الاليكتروني التالي:
https://www.politics-dz.com/%D8%A7%D9%84%D8%A3%D9%85%D9%86-6
10. رغدة البهي، (21فيفري 2017)، الردع السيبراني: المفهوم والإشكاليات والمتطلبات، برلين : المركز الديمقراطي العربي مجلة العلوم السياسية والقانون، متحصل على المقال من خلال الرابط الاليكتروني التالي :

https://democraticac.de/?p=43837#_ftn34

11.تقرير منشور من طرف مركز سيتا التركي للدراسات السياسية ، الأمن السيبيراني :الهجمات السيبرانية.. حروب غير مرئية منشور في 10 ماي 2021 ومتحصل على التقرير بشكل مفصل عبر الرابط الإليكتروني التالي:
HTTPS://WWW.IFEGYPT.ORG/NEWSDETAILS.ASPX?PAGE_ID=1244&PAGEDETAILID=1324#:~:TEXT=%D9%88%D9%82

12. اسراء جبريل رشاد مرعي، (9 أغسطس 2016) الجرائم الإلكترونية : الأهداف – الأسباب – طرق الجريمة ومعالجتها، برلين: المركز الديمقراطي العربي، مقال منشور في موقع المركز ومتحصل عليه من خلال الرابط الاليكتروني التالي :
https://democraticac.de/?p=35426

13. ROHIT CHATTERJEE(2021)"Difference Between Cybersecurity & Information Security", Published in analytics india mag, 5/3/2020, Retrieved 16/11/2021.

14. Kenneth Geers, (2010) The Challenge of Cyber Attack Deterrence, *Computer Law & Security Review*, No. 26,.

15. What is Cyber Security? Definition and Best Practices", itgovernance, Retrieved 9/11/2021. Edited.by web site :
https://www.itgovernance.co.uk/what-is-cybersecurity

16. Lehto Martti , Neittaanmäk Pekka (2015) .Cyber Security: Analytics, Technology and Automation. Switzerland : Springer International Publishing, ,published in web site :
https://www.pdfdrive.com/cyber-security-analytics-technology-and-automation27098885.html