الأمن السيبراني كبعد جديد في السياسة الدفاعية الجزائرية

د/ بن مرزوق عنترة
أستاذ محاضر أ كلية الحقوق والعلوم السياسية
بجامعة محمد بوضياف – المسيلة
أ. حرشاوي محي الدين
أستاذ مساعد بكلية الحقوق والعلوم السياسية
بالمركز الجامعي آفلو

مقدمة:

في ظل الأوضاع الأمنية غير المستقرة التي تشهدها المنطقة العربية عموما، ودول الجوار الجزائري خصوصا، ومع تسارع التطورات التكنولوجية الكبيرة التي يشهدها عالم اليوم، لم تعد سياسات الدفاع الجزائرية مقتصرة على مكافحة الإرهاب وحماية سيادة الوطن والمحافظة على استقراره ووحدته من خلال الاعتماد على الطرق التقليدية فقط، بل تجاوزتها لتشمل مسألة حماية أمن الدولة والمجتمع من التهديدات الجديدة التي أفرزتها الثورة التكنولوجية الحديثة، وذلك يتطلب تحقيق الأمن السيبراني باعتباره يمثل أحد أولويات السياسة الدفاعية الجزائرية.

هذه الدراسة ستحاول التطرق إلى موضوع الأمن السيبراني كبعد جديد في السياسة الدفاعية الجزائرية، وذلك من خلال تناول العناصر التالية:

- مفهوم الأمن السيبراني.
- الإرهاب الالكتروني كأحد أخطر التهديدات المحتملة على الأمن الجزائري في ظل الثورة التكنولوجية الحديثة.
- الجهود الجزائرية في مجال تحقيق الأمن السيبراني بين ما هو كائن وما يجب أن يكون.

1- مفهوم الأمن السيبراني:

تعتبر مهمة تحديد المصطلحات أول تحد يواجهه المفكرون ويتعرض له الباحثون في جميع التخصصات وفي شتى الدراسات، وذلك لما تطرحه من إشكاليات تجعل من الصعوبة بمكان الاتفاق على تعريفات واضحة وشاملة وموحدة بين فرقاء المجتمع العلمي يمكن تعميمها على جميع الحقول المعرفية، ويعتبر مصطلح الأمن السيبراني واحدا من هذه المصطلحات التي تعرف تعددا في التعريفات المقدمة لها.

فإذا كان مفهوم الأمن مفهوم واسع، يطال جميع عمليات الدخول، والخروج، والبقاء، أو التصرف، في مكان ما. وعليه، فإنه في الفضاء السيبراني يشمل مختلف قواعد وأصول ضبط الاتصال، وانتقال

المعلومات، وتخزينها وحفظها. كما يشمل أمن المواقع، وامن الأنظمة الالكترونية، وعمليات استثمارها، إضافة إلى امن الاتصالات.[1]

وقد قدمت وزارة الدفاع في الولايات المتحدة الأمريكية تعريفا دقيقا لمصطلح الأمن السيبراني، حيث اعتبرته: "جميع الإجراءات التنظيمية اللازمة لضمان حماية المعلومات بجميع أشكالها (الإلكترونية والمادية)، من مختلف الجرائم، الهجمات، التخريب، والتجسس، والحوادث.[2]

في حين اعتبر الإعلان الأوروبي الأمن السيبراني بأنه يعني: "قدرة النظام المعلوماتي على مقاومة محاولات الاختراق أو الحوادث غير المتوقعة، التي تستهدف البيانات. [3]

وهذا ما ذهب إليه الكاتبان *Martti Lehto,Pekka Neittaanmäki* في كتابهما الموسوم: *Cyber Security: Analytics, Technology and Automation* حيث اعتبرا أن الأمن السيبراني عبارة عن مجموعة من الإجراءات التي اتخذت في الدفاع ضد هجمات قراصنة الكمبيوتر وعواقبها ويتضمن تنفيذ التدابير المضادة المطلوبة.[4]

وهذا ما أكد عليه البروفيسور وأستاذ الاتصالات في جامعة كاليفورنيا ريتشارد كمرر *Richard A. Kemmerer* الذي عرفه بأنه" عبارة عن وسائل دفاعية من شأنها كشف وإحباط المحاولات التي يقوم بها القراصنة"، بينما عرفه إدوارد أمورسو Edward Amoroso بأنه" وسائل 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.. إلخ.[5]

تجدر الإشارة إلى أن لفظة سيبار cyber يونانية الأصل، مشتقة من كلمة ”kybernetes,“، والتي تعني الشخص الذي يدير دفة السفينة steersman ، وتستخدم مجازا لتعبر عن المتحكم governor. [6]وقد استخدمها افلاطون من قبل للتعبير عن الحكم. وهناك من يرجع أصلها إلى منتصف القرن العشرين مع عالم الرياضيات الأمريكي Norbert Wiener's (1894–1964) والذي استخدمها للتعبير عن التحكم الآلي.[7]

ويعتبر Wiener's الأب الروحي المؤسس للسيبرنيتيقية cybernetics وهو صاحب الكتاب الشهير:

Cybernetics or control and communication in the Animal and the machine.

والذي عرف فيه السيبرنيتيقية cybernetics بأنها " التحكم والتواصل عند الحيوان والآلة.[8] كما أشار في نفس الكتاب إلى مسألة التواصل بين الإنسان والآلة، واعتبر ان السيبرنيتيقية cybernetic هي علم نقل الرسائل بين الإنسان والآلة، أو بين الآلة والآلة.[9] أو هي علم القيادة أو التحكم (control)في الأحياء والآلات ودراسة آليات التواصل communicationn في كل منهما." [10]

غير أنه وبعد الثورة التقنية الهائلة التي انطلقت بعد نهاية الحرب العالمية الثانية، تغير مصطلح الآلات ليحل محله الكمبيوتر.[11]

ولذلك قام وليام جيبسون William Gibson في رواياته عن المستقبل باستخدام كلمة "الفضاء الإلكتروني"، وصارت كلمة سايبر توضع أمام أي شيء وكل شيء مرتبط بشبكة الإنترنت.[12]

وهذا يعني أن مصطلح سيبار أو الفضاء الالكتروني وفي كثير المراجع الفضاء السيبراني، ظهر مع ظهور الانترنت وتعميم استخدام الرقمنة، موازاة مع كم هائل من المصطلحات مثل الفضاء الرقمي، الدفاع الالكتروني، الهجوم الالكتروني، الجريمة الالكترونية وغيرها، في حين أن الآمن السيبراني أو الالكتروني ظهر حديثا وهو يعني: مجمل القوانين السياسية، الأدوات، النصوص، المفاهيم وميكانيزمات الأمن وطرق تسيير الأخطار والممارسات التكنولوجية المتعلقة بتكنولوجيات المعلومات والاتصالات المستخدمة لحماية الدول والمنظمات والأشخاص. كما يعرف على انه الحالة المرغوب فيها لعمل أنظمة المعلومات والاتصالات والتي تمنحها القدرة على المقاومة والتصدي لكل ما ينجم عن الفضاء السيبراني، والذي من شأنه أن يعرض المعلومات المخزنة أو المعالجة أو المنقولة للتلف أو التغيير أو التجسس.[13]

وانطلاقا من ذلك فإن هدف الأمن السبراني هو القدرة على مقاومة التهديدات المتعمدة وغير المتعمدة والاستجابة والتعافي، وبالتالي التحرر من الخطر أو الأضرار الناجمة عن تعطيل آو إتلاف تكنولوجيا المعلومات والاتصالات أو بسبب إساءة استخدام تكنولوجيا المعلومات والاتصالات. [14]وهذا يتطلب حماية الشبكات وأجهزة الكمبيوتر، والبرامج والبيانات من الهجوم أو الضرر أو الوصول غير المصرح به، وبعبارة أخرى فإنه لا يعني أكثر من حماية البيانات.[15]

ونتيجة لأهمية الأمن السيبراني في واقع مجتمعات اليوم فقد جعلته العديد من الدول على رأس أولوياتها، خاصة بعد الحروب الالكترونية التي بدأت تظهر تجلياتها بين بعض الدول الكبرى، في إشارة صريحة إلى نهاية الحروب التقليدية التي كانت تستخدم فيها الأسلحة الثقيلة، والإعلان عن بداية حروب جديدة هي الحروب الالكترونية.

وأمام هذه التحديات فقد بات لزاما على أي دولة تريد المحافظة على أمنها واستقرارها وسيادتها أن تهتم اهتماما بالغا بمسألة تحقيق وتطوير أمنها السيبراني.

والجزائر واحدة من هذه الدول التي بدأت في التوجه نحو الاهتمام بهذا النوع من الأمن لإدراكها أن العالم اليوم تغير، وأن بقائها كقوة عسكرية وإقليمية قوية يتطلب منها بذل جهود كبيرة في مجال الوقاية من مختلف المخاطر السيبرانية التي أفرزتها الثورة التكنولوجية الحديثة.

2- <u>الإرهاب الالكتروني كأحد أخطر التهديدات المحتملة على الأمن الجزائري في ظل الثورة التكنولوجية الحديثة</u>.

تشهد الساحة الأمنية الجزائرية كغيرها من الدول العديد من المخاطر والتهديدات التي فرضتها الثورة التكنولوجية الحديثة، خاصة بعد انتشار وسائل التواصل الاجتماعي والعديد من المواقع الالكترونية التي تحمل أفكارا هدامة تهدد استقرار الوطن ووحدته، وتدعو الى نشر الفوضى والعنف والتطرف

والكراهية والانقسام. ومن أهم المخاطر التي تترتب عن استخدام التكنولوجيا الحديثة على الأمن الجزائري الإرهاب الالكتروني.

ويقصد به " العدوان أو التخويف أو التهديد ماديا أو معنويا باستخدام الوسائل الإلكترونية الصادر من الدول أو الجماعات أو الأفراد على الإنسان في دينه، أو نفسه، أو عرضه، أو عقله، أو ماله، بغير حق بشتى صنوفه وصور الإفساد في الأرض".[16] ويعتبر أحد أخطر التهديدات التي تستهدف أمن جميع الدول بما في ذلك الدولة الجزائرية.

وهذا ما أكده اللواء مناد نوبة، القائد العام للدرك الوطني الجزائري في كلمة له ألقاها بمناسبة افتتاح الندوة الدولية حول "الأمن السيبراني"،حيث قال: "إن الإرهاب الإلكتروني بات من أخطر الجرائم التي تستهدف الجزائر، من خلال تنامي مظاهر الترويج لكل أشكال العنف والإرهاب والتطرف، باستعمال أحدث التقنيات التكنولوجية خاصة شبكات التواصل الاجتماعي والمنتديات الإلكترونية." ولذلك دعا إلى إطلاق خلايا أمنية متخصصة هدفها العمل على "تعزيز إجراءات الرقابة لحماية المواطن الجزائري، وخاصة عنصر الشباب، من مثل هذه الجرائم الإلكترونية الخطيرة جداً على استقرار البلاد." وذلك من خلال قيامها بتعقب وملاحقة كل الأنشطة المتعلقة بالتجنيد للإرهاب والإجرام المنظم العابر للحدود، وتكييفها بالوسائل التكنولوجية العصرية." وذلك يتطلب حسبه ضرورة "التسلح بكل الوسائل التكنولوجية والفعالة لمحاربة إيديولوجيات العنف والتطرف وكل أشكال الجريمة المنظمة والعابرة للأوطان، من خلال اعتماد آليات عملية للتعاون بين كل الشركاء الفاعلين في هذا المجال."[17]

ومن أهم المواقع الإلكترونية التي تدعو إلى التعبئة والتجنيد والدعوة إلى الانضمام إلى التنظيمات الإرهابية مايلي:[18]

موقع النداء : وهو الموقع الرسمي لتنظيم القاعدة بعد أحداث الحادي عشر من سبتمبر عام 2001م، ومن خلاله تصدر البيانات الإعلامية للقاعدة.

ذروة السنام : وهي صحيفة إلكترونية دورية للقسم الإعلامي لتنظيم القاعدة.

صوت الجهاد : وهي مجلة نصف شهرية، يصدرها ما يسمى بتنظيم القاعدة في جزيرة العرب، وتتضمن مجموعة من البيانات والحوارات مع قادة التنظيم ومنظريه.

البتار: وهي مجلة عسكرية إليكترونية متخصصة، تصدر عن تنظيم القاعدة، وتختص بالمعلومات العسكرية والميدانية والتجنيد.

أما التنظيم الإرهابي "داعش" فله أزيد من 50 ألف موقع إلكتروني، 90 ألف صفحة باللغة العربية على موقع التواصل الاجتماعي «فيس بوك»، و40 ألفاً بلغات أخرى، وهذا ما ساهم في تجنيده حوالي 3400 شاب شهرياً عبر حملاته الالكترونية، وهذا حسب تقرير للخبير الأمني في قضايا الإرهاب الرقمي جيف باردين *jeff bardin*.[19]

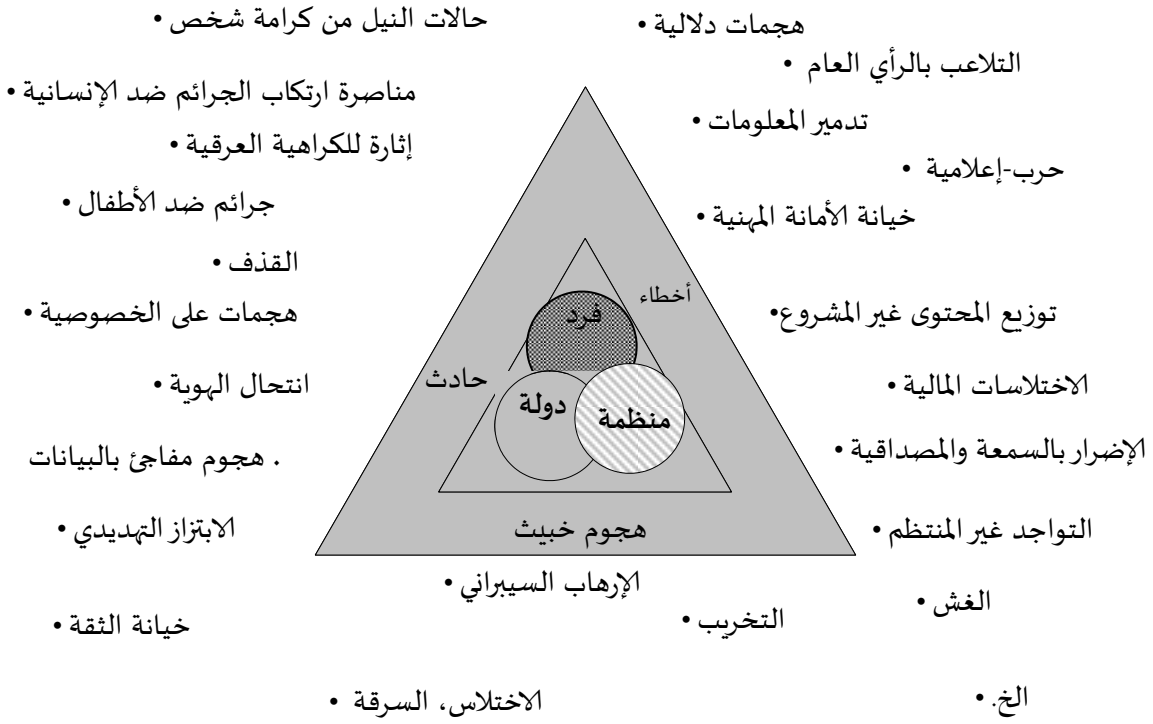
ورغم الخطورة الكبيرة التي تخلفها مثل هذه المواقع الإلكترونية على أمن واستقرار المجتمعات، إلا أن تأثيرها على المجتمع الجزائري كان قليلا.

فقد كشف السيد محمد عيسى وزير الشؤون الدينية والأوقاف، أن التجنيد الإلكتروني لداعش في الجزائر عن طريق شبكة الأنترنيت ومواقع التواصل الاجتماعي لم يتجاوز 100 شاب جزائري[20] ، وهو رقم ضئيل إذا ما قورن بعدد المجندين في دول عربية أخرى.

ويمكن تبرير ذلك بنتائج العشرية السوداء التي عاشها الجزائريون نهاية القرن الماضي، وكذا التحصن الجزائري ضد الفكر التطرفي العابر للحدود، إضافة إلى الفشل الذريع الذي منيت به ما يعرف بثورات الربيع العربي، والذي كان له تأثير كبير على ضرورة البحث عن آليات أخرى للتغيير السلمي في المجتمعات بعيدا عن العنف والتطرف بشتى أشكاله.

ولذلك فالانترنت يجب أن تبقى فضاءا لنشر و مشاطرة العلوم و المعرفة و آداة للإبداع و التقارب و التعاون بين الأفراد و الشعوب و الدول، وليس وسيلة وأداة تهديدية تستغلها الجماعات الارهابية من أجل بلوغ أهدافها الاجرامية ونشر أفكارها التطرفية، كما أشار إلى ذلك السيد وزير الشؤون المغاربية و الإتحاد الإفريقي و جامعة الدول العربية, السيد: عبد القادر مساهل في كلمته خلال أشغال الورشة الدولية حول دور الإنترنت و الشبكات الإجتماعية في مكافحة التطرف و الإرهاب الإلكتروني و الوقاية منهما.[21]

ولا تقتصر التهديدات السيبرانية على قضية الإرهاب الالكتروني فقط، وإنما تشمل العديد من المخاطر والتهديدات الأخرى التي لا ترتبط بأمن الدول فقط، بل تشمل المجتمع ككل، فهي متعلقة بأمن الأفراد والمنظمات أيضا، والشكل التالي يوضح ذلك: [22]



شكل يوضح مستويات الأمن السيبراني.

3- الجهود الجزائرية في مجال تحقيق الأمن السيبراني بين ماهو كائن ومايجب أن يكون.

أمام التهديدات والمخاطر المتزايدة التي تخلفها استخدام التكنولوجيا الحديثة في الجزائر فقد بات لزاما اعتماد سياسة أمنية وطنية تضع مسألة توفير الأمن السيبراني على رأس أولوياتها واستراتيجياتها، وذلك من خلال البحث عن آليات وميكانيزمات فعالة يمكن من خلالها إدارة مختلف الحروب السيبرانية سواء باعتماد سياسات وقائية أحيانا أو سياسات علاجية في أحيان أخرى.

وقبل التطرق إلى مختلف الجهود الجزائرية في مجال تحقيق الأمن السيبراني لابد بداية من توضيح الترتيب العالمي للجزائر حسب الرقم القياسي العالمي للأمن السيبراني، حيث احتلت الجزائر المرتبة 23 عالميا من أصل 29 مرتبة في مستوى التأهب في مجال الأمن السيبراني، كماهو موضح في الجدول التالي:[23]

البلد	الرقم القياسي	الترتيب العالمي
الولايات المتحدة الأمريكية	0.824	1
كندا	0,794	2
أستراليا	0.765	3
ماليزيا	0.765	3
عُمان	0.765	3

نيوزيلندا	0.735	4
النرويج	0.735	4
اسرائيل	0.676	6
تركيا	0.647	7
قطر	0.618	8
مصر	0.588	9
فرنسا	0.588	9
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
الجزائر	**0.176**	**23**
بربادوس	0.176	23
بيلاروس	0.176	23
بليز	0.176	23
بنين	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

جدول يوضح الترتيب العالمي للدول حسب الرقم القياسي العالمي للأمن السيبراني.

أما على المستوى العربي فقد احتلت الجزائر المرتبة العاشرة حسب التزامها بتلك التدابير التي يحددها الرقم القياسي العالمي للأمن السيبراني، والشكل التالي يوضح ترتيب مختلف بلدان منطقة الدول العربية: [24]

الدول العربية	قانونية	تقنية	تنظيمية	بناء القدرات	التعاون	الرقم القياسي	الترتيب الإقليمي
عُمان	0.7500	0.6667	1.0000	0.7500	0.6250	0.7647	1
قطر	0.7500	0.8333	0.5000	0.6250	0.5000	0.6176	2
مصر	0.5000	0.5000	0.3750	1.0000	0.5000	0.5882	3
المغرب	0.5000	0.6667	0.7500	0.5000	0.3750	0.5588	4
تونس	1.0000	0.5000	0.6250	0.2500	0.5000	0.5294	5
السودان	0.7500	0.5000	0.5000	0.2500	0.3750	0.4412	6
الإمارات العربية المتحدة	0.7500	0.3333	0.2500	0.5000	12.50	0.3529	7
البحرين	0.7500	0.1667	0.1250	0.3750	0.2500	0.2941	8
ليبيا	0.2500	0.3333	0.3750	0.1250	0.3750	0.2941	8
المملكة العربية السعودية	0.7500	0.3333	0.1250	0.3750	0.1250	0.2941	8
الأردن	0.5000	0.0000	0.5000	0.0000	0.1250	0.2059	9

الجزائر	**0.7500**	**0.0000**	**0.0000**	**0.1250**	**0.2500**	**0.1765**	**10**
سوريا	0.2500	0.3333	0.1250	0.1250	0.1250	0.1765	10
موريتانيا	0.2500	0.1667	0.2500	0.0000	0.1250	0.1471	11
دولة فلسطين	0.2500	0.0000	0.3750	0.1250	0.0000	0.1471	11
لبنان	0.0000	0.0000	0.0000	0.2500	0.1250	0.0882	12
جيبوتي	0.2500	0.0000	0.0000	0.0000	0.1250	0.0588	13
الكويت	0.0000	0.0000	0.0000	0.1250	0.1250	0.0588	13
اليمن	0.2500	0.0000	0.0000	0.0000	0.1250	0.0588	13
جزر القمر	0.0000	0.0000	0.0000	0.0000	0.1250	0.0294	14
العراق	0.0000	0.0000	0.0000	0.0000	0.1250	0.0294	14
الصومال	0.0000	0.0000	0.0000	0.1250	0.0000	0.0294	14

جدول يوضح ترتيب بلدان منطقة الدول العربية حسب الرقم القياسي العالمي للأمن السيبراني.

ومن خلال هذا الجدول يمكن القول أن جهود الجزائرية في مجال تحقيق الأمن السيبراني تبقى ضئيلة، حيث تركزت أساسا في مجال اتخاذ التدابير القانونية دون غيرها من التدابير الاخرى، ويتضح ذلك من خلال صدور القانون رقم 09-04 المؤرخ في 05 أوت 2009، الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، والتي تم فيه تحديد الحالات التي تسمح باللجوء إلى مراقبة الاتصالات الإلكترونية بناءا على ما ورد في المادة 4 التي نصت على مايلي:[25]

- للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة.
- في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.
- لمقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الالكترونية.
- في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.

كما نصت المادة 13 على إنشاء هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وهذا ما تم من خلال صدور المرسوم الرئاسي رقم 15-261 المؤرّخ في 08 أكتوبر سنة 2015، والذي يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم

المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. ومن المهام التي تمارسها الهيئة ما ورد في المادة 4 من المرسوم والتي نصت على مايلي:[26]

– اقتراح عناصر الإستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

– تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

– مساعدة السلطات القضائية ومصالح الشرطة القضائية في مجال مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، بما في ذلك من خلال جمع المعلومات والتزويد بها ومن خلال الخبرات القضائية .

– ضمان المراقبة الوقائية للاتصالات الإلكترونية قصد الكشف عن الجرائم المتعلقة بالأعمال الإرهابية والتخريبية والمساس بأمن الدولة تحت سلطة القاضي المختص وباستثناء أي هيئات وطنية أخرى.

– تجميع وتسجيل وحفظ ا لمعطيات الرقمية وتحديد مصدرها ومسارها من أجل استعمالها في الإجراءات القضائية .

– السهر على تنفيذ طلبات المساعدة الصادرة عن البلدان الأجنبية وتطوير تبادل المعلومات والتعاون على المستوى الدولي في مجال اختصاصها.

– تطوير التعاون مع المؤسسات والهيئات الوطنية ا لمعنية بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

– المساهمة في تكوين المحققين المتخصصين في مجال التحريات التقنية المتصلة بتكنولوجيات الإعلام والاتصال.

-المساهمة في تحديث المعايير القانونية في مجال اختصاصها.

وإضافة إلى الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، فقد أنشأت الجزائر هيئات أخرى تضطلع بأدوار جد هامة في مواجهة مختلف الجرائم الالكترونية منها:[27]

– مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية للدرك الوطني.

– المصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة لمديرية الأمن الوطني.

– المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني.

ويأتي اهتمام الجزائر بإنشاء مثل هذه المؤسسات إلى تزايد معدلات الجرائم الالكترونية التي أصبحت تشكل تهديدا كبيرا على الأمن الوطني، فقد ارتفع معدل الجرائم الالكترونية في الجزائر بشكل كبير خلال السنوات الأخيرة حسب بعض التقارير الأمنية، حيث عرفت الجزائر أزيد من 100 جريمة الكترونية سنة 2014، ليتضاعف هذا العدد خلال السداسي الأول من سنة 2015 إلى أكثر من 200

جريمة الكترونية يتعلق أبرزها بانتهاك الحريات الشخصية، والتهديد عبر الانترنت، ونشر صور فاضحة، الابتزاز، والقرصنة الالكترونية وغيرها.[28]

ونظرا لخطورة هذه التهديدات فقد أولت الجزائر أهمية كبيرة لمسألة تحقيق الأمن السيبراني، خاصة بعد دخول خدمة الجيل الثالث للانترنت وتنامي استخدام شبكات التواصل الاجتماعي، ويظهر ذلك إضافة إلى اهتمامها بالجانب القانوني والمؤسساتي الذي اشرنا إليه سابقا، في تنظيمها لبعض المؤتمرات التي تهتم بهذا الموضوع، فقد نظمت مديرية الإيصال والإعلام والتوجيه لأركان الجيش الوطني الشعبي ملتقى حول: "الجيش الوطني الشعبي ورهانات تداول المعلومة عبر شبكات التواصل الاجتماعي"، وقد أجمع المحاضرون فيه على ضرورة تحلي العقيدة الأمنية الجزائرية بالمزيد من اليقظة والتحكم في التكنولوجيات الحديثة، مع تحصين الأفراد وتحسيسهم بأهميتها ودورها في تطوير الاتصال العسكري، وترقية مستوى تكوينهم في مجال أمن وحماية المعلومة، وكذلك التنبيه بمخاطر سوء استعمالها، إضافة إلى توسيع إشراك فواعل جديدة من خارج المؤسسة العسكرية، والذين بوسعهم المساهمة في صيانة عقيدة الدفاع الوطني، ذلك أن الفضاء الافتراضي أصبح يحتل الميدان الخامس للنزاعات بعد البر والبحر والجو والفضاء.[29]

ورغم هذه الجهود التي تبذلتها الجزائر في مجال تحقيق الأمن السيبراني إلا أنها تبقى في نظرنا بحاجة إلى القيام بالعديد من الإجراءات، التي يمكن أن نوردها فيمايلي:

– إقامة العُدة العسكرية السيبرانية بتكليف عدد كبير من الأفراد العسكريين بمهمة القتال الافتراضي استجابة للتهديد الجديد للحرب السيبرانية، ويمكن أن يشمل هذا التحول السياسي إنشاء فرق حربية للإنترنت تكون مكرسة لتحقيق الأمن السيبراني، ويمكن دمجها في وكالات استخبارات أخرى، أو حتى إنشاء قطاعات جديدة تماماً ضمن الهيكل العسكري المكرس للنشاط السيبراني. وتقام هذه العدة العسكرية الجديدة لدمج وإعداد الموارد العسكرية من أجل جميع أنواع عمليات الفضاء السيبراني. ويمكن أن تكون أيضاً مسؤولة عن تأمين الشبكات الخاصة التي تشغّل جزءاً كبيراً من العمليات العسكرية، وإن كان تركيزها في المقام الأول على حماية الشبكات العسكرية وتسيير العمليات العسكرية في الفضاء السيبراني.[30]

– تكوين نخب وطنية مختصة في مجال الأمن السيبراني، مع ضرورة إجراء مؤتمرات علمية يشارك فيها مختلف المختصين العالميين من أجل الاستفادة من خبراتهم.

– الاستفادة من تجارب الدول الرائدة في مجال تحقيق الأمن السيبراني، والتعرف على أفضل التقنيات العالمية المنتهجة في مكافحة الجرائم الالكترونية من قرصنة وتجسس وإرهاب الكتروني...إلخ

– اعتماد سياسة وقائية بنشر ثقافة الأمن السيبراني وزيادة الوعي المجتمعي بمختلف المخاطر والتهديدات التي تفرضها الثورة التكنولوجية الحديثة، وتحصين أفراد المجتمع ضد كل الأفكار الهدامة

التي تنشرها مختلف المواقع الالكترونية ووسائل التواصل الاجتماعي، وذلك من خلال حجب تلك المواقع وملاحقة المؤيدين لها.

– التعاون الإقليمي والدولي بتيسير تبادل المعلومات في مجال مكافحة الإرهاب الالكتروني والدعوة إلى تحقيق الأمن والسلم الدوليين ومنع تحول الفضاء السيبراني الى ميدان للحروب والنزاعات بين الدول.

– تحديث البنية التحتية لتقنية المعلومات والاتصالات وحمايتها، وتحديد نقاط القوة والضعف الموجودة في التشريعات القانونية المتعلقة بمكافحة جرائم المعلومات، والعمل على تجاوز عقبات تطبيقها.

خاتمة:

في الأخير وانطلاقا من كل ما سبق يمكن القول أن مسألة تحقيق الأمن السيبراني في الجزائر يعد أحد أهم التحديات الجديدة للسياسة الأمنية الجزائرية التي فرضتها التطورات التكنولوجية المتسارعة، ورغم الجهود المبذولة في سبيل تحقيق ذلك إلا أن المراتب التي تحتلها الجزائر عربيا ودوليا تشير إلى أنها بحاجة إلى المزيد من الجهود، وهذا حتى يمكن لها أن تنجح في مجال مكافحة مختلف المخاطر التي يفرزها الفضاء الالكتروني، والتي يأتي على رأسها الإرهاب الالكتروني وغيره من التهديدات التي يمثل الانتصار عليها انتصارا جديدا للسياسة الأمنية الجزائرية التي أثبتت نجاعتها في المكافحة خارج الفضاء الالكتروني ولن تدخر أي جهد في إثبات مكانتها في هذا الفضاء الذي لا يعترف لا بالحدود ولا بالقيود.

قائمة المراجع:

الكتب باللغة العربية:

– الاتحاد الدولي للاتصالات، **دليل الأمن السيبراني للبلدان النامية**. جنيف: مكتب تنمية الاتصالات، 2009.

– (ـــــ،ـــــ)، **البحث عن السلام السيبراني**. جنيف: الاتحاد الدولي للاتصالات، يناير 2011.

– (ـــــ،ـــــ) ، **تقرير حول الرقم القياسي العالمي للأمن السيبراني وسمات السلامة السيبرانية**. جنيف: الاتحاد الدولي للاتصالات، مكتب تنمية الاتصالات، أفريل 2015.

الكتب باللغة الأجنبية:

- *Daniel Ventre,* ***Cyberattaque et cyberdéfense.*** *Paris ; La Voisier, 2011.*

- *Joanna F. DeFranco,* ***What Every Engineer Should Know About Cyber Security and Digital Forensics****.Boka Raton : CRC press, 2014.*

-*Marc Delplanque,* ***Gouvernance globale: gouvernement du monde****. France : Éditions Bénévent, 2004, P105.*

-*Martti Lehto,Pekka Neittaanmäki,* ***Cyber Security: Analytics, Technology and Automation****. Switzerland : Springer International Publishing, 2015.*

- *Norbert Wiener*, ***The Human Use of Human Beings: Cybernetics and Society***. *London : Free Association Books, 1989.*

- *Norbert Wiener*, ***Cybernetics or control and communication in the Animal and the machine***. *2nd ed, Cambridge, Massachusetts : the M.I.T. press, 1985.*

-*Sandro Bologna, Bernhard Hämmerli, Dimitris Gritzalis*, ***Critical Information Infrastructure Security***. *Berlin ; Springer, 2013.*

الرسائل الجامعية باللغة الأجنبية:

- *Hyun jean Lee, The Screen as Boundary Object in the Realm of Imagination.* ***A Thesis presented to the academic faculty, In partial fulfillment of the requirements for the degree Doctor of Philosophy in the School of Literature, communication and culture***. *Georgia Institute of Technology, May 2009.*

المجلات والدوريات العلمية:

– محمد مختار، هل يمكن أن تتجنب الدول مخاطر الهجمات الالكترونية. **دورية اتجاهات الأحداث**، الصادرة عن مركز المستقبل للأبحاث والدراسات المتقدمة، العدد06، يناير 2015.

– ج. رضوان، الأمن السيبراني: أولوية في استراتيجيات الدفاع. **مجلة الجيش** الصادرة عن مؤسسة المنشورات العسكرية، العدد 630، جانفي 2016.

– ب. بوعلام، ملتقى حول: "الجيش الوطني الشعبي ورهانات تداول المعلومة عبر شبكات التواصل الاجتماعي". **مجلة الجيش** الصادرة عن مؤسسة المنشورات العسكرية، العدد 630، جانفي 2016.

– الهام غازي، الوقاية ومكافحة الجريمة المعلوماتية في التشريع الجزائري. **مجلة الجيش** الصادرة عن مؤسسة المنشورات العسكرية، العدد 630، جانفي 2016.

الملتقيات والمؤتمرات العلمية:

– أيسر محمد عطية، "دور الآليات الحديثة للحد من الجرائم المستحدثة: الإرهاب الالكتروني وطرق مواجهته". **ورقة مقدمة في الملتقى العلمي: الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية**. عمان خلال الفترة 02–04 سبتمبر 2014.

الجرائد اليومية:

[1] زولا سومر، عيسى: 100 شاي جزائري التحقوا بداعش. **جريدة المساء**، العدد 6061، الصادر بتاريخ 17 ديسمبر 2016.

الوثائق الرسمية:

الجمهورية الجزائرية الديمقراطية الشعبية، قانون رقم 09-04 المؤرخ في 14 شعبان 1430،الموافق 05 أوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، **الجريدة الرسمية**، العدد 47، الصادرة بتاريخ 25 شعبان 1430 الموافق 16 أوت 2009.

[1] الجمهورية الجزائرية الديمقراطية الشعبية، مرسوم رئاسي رقم 15-261 مؤرّخ في 24 ذي الحجة عام 1436، الموافق 8 أكتوبر سنة 2015، والذي يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، **الجريدة الرسمية**، العدد 53، الصادرة بتاريخ 24 ذو الحجة 1436 الموافق08 أكتوبر 2015.

المواقع الإلكترونية:

- إيهاب شوقي، الإرهاب الالكتروني وجرائمه. من موقع:
http://www.assakina.com/awareness-net/rebounds/81251.html
- جهاد ملحم، السوبرنية ضد قوانين الفيزياء !!!! ما هي السوبرنية؟. من موقع:
http://wehda.alwehda.gov.sy/node/393079

وكالة الأنباء الجزائرية، الارهاب الالكتروني: "الجزائر حريصة على حماية أمنها". من موقع:
http://www.algpress.com/article-50021.htm

- محمود خليل، 50ألف موقع إلكتروني لداعش.. والإرهاب يحاصر الإنترنت. من موقع:
http://www.alittihad.ae/details.php?id=64991&y=2015&article=full
- منى الاشقر جبور، الأمن في الفضاء السيبيري: الأمن المعلوماتي والأمن القانوني. من موقع:
xa.yimg.com/kq/groups/.../ÇáÃãä+Ýí+ÇáÝÖÇÁ+ÇáÓíÈíÑí.doc
- الخليج اونلاين، تخصيص خلايا أمنية لتعقب الإرهاب الإلكتروني في الجزائر . من موقع:
alkhaleejonline.net

الهوامش :

1. منى الاشقر جبور، الأمن في الفضاء السيبيري: الأمن المعلوماتي والأمن القانوني. من موقع:
xa.yimg.com/kq/groups/.../ÇáÃãä+Ýí+ÇáÝÖÇÁ+ÇáÓíÈíÑí.doc
2. *Daniel Ventre, **Cyberattaque et cyberdéfense.** Paris ; La Voisier, 2011, P103.*
3. منى الاشقر جبور، الأمن في الفضاء السيبيري: الأمن المعلوماتي والأمن القانوني. الموقع السابق الذكر.
4. *Martti Lehto,Pekka Neittaanmäki, **Cyber Security: Analytics, Technology and Automation**. Switzerland : Springer International Publishing, 2015, P25.*
5. محمد مختار، هل يمكن أن تتجنب الدول مخاطر الهجمات الالكترونية. **دورية اتجاهات الأحداث**، الصادرة عن مركز المستقبل للأبحاث والدراسات المتقدمة، العدد06، يناير 2015، ص 05.
6. *Norbert Wiener, **The Human Use of Human Beings: Cybernetics and Society**. London : Free Association Books, 1989, P15.*
7. *Joanna F. DeFranco, **What Every Engineer Should Know About Cyber Security and Digital Forensics**.Boka Raton : CRC press, 2014, P40.*
8. *Norbert Wiener, **Cybernetics or control and communication in the Animal and the machine**. 2nd ed, Cambridge, Massachusetts : the M.I.T. press, 1985.*
9. *Hyun jean Lee, The Screen as Boundary Object in the Realm of Imagination. **A Thesis presented to the academic faculty, In partial fulfillment of the requirements for***

the degree Doctor of Philosophy in the School of Literature, communication and culture. *Georgia Institute of Technology, May 2009, P41.*

10. Marc Delplanque, ***Gouvernance globale: gouvernement du monde****. France : Éditions Bénévent, 2004, P105.*

11. جهاد ملحم، السوبرنية ضد قوانين الفيزياء !!!! ما هي السوبرنية؟. من موقع:
http://wehda.alwehda.gov.sy/node/393079

12. *Joanna F. DeFranco, op cit, P40.*

13. ج. رضوان، الأمن السيبراني: أولوية في استراتيجيات الدفاع. **مجلة الجيش** الصادرة عن مؤسسة المنشورات العسكرية، العدد 630، جانفي 2016، ص ص 40-41.

14. *Sandro Bologna, Bernhard Hämmerli, Dimitris Gritzalis,* ***Critical Information Infrastructure Security****. Berlin ; Springer, 2013, P 02-03.*

15. *Joanna F. DeFranco, op cit, P40.*

16. أيسر محمد عطية، "دور الآليات الحديثة للحد من الجرائم المستحدثة: الإرهاب الالكتروني وطرق مواجهته". **ورقة مقدمة في الملتقى العلمي: الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية.** عمان خلال الفترة 02-04 سبتمبر 2014، ص 09.

17. الخليج اونلاين، تخصيص خلايا أمنية لتعقب الإرهاب الإلكتروني في الجزائر . من موقع:
alkhaleejonline.net

18. إيهاب شوقي، الإرهاب الالكتروني وجرائمه. من موقع:
http://www.assakina.com/awareness-net/rebounds/81251.html

19. محمود خليل، 50ألف موقع إلكتروني لداعش.. والإرهاب يحاصر الإنترنت. من موقع:
http://www.alittihad.ae/details.php?id=64991&y=2015&article=full

20. زولا سومر، عيسى: 100 شاي جزائري التحقوا بداعش. جريدة المساء، العدد 6061، الصادر بتاريخ 17 ديسمبر 2016، ص 04.

21. وكالة الأنباء الجزائرية، الارهاب الالكتروني: "الجزائر حريصة على حماية أمنها". من موقع:
http://www.algpress.com/article-50021.htm

22. الاتحاد الدولي للاتصالات، **دليل الأمن السيبراني للبلدان النامية**. جنيف: مكتب تنمية الاتصالات، 2009،ص08.

23. الاتحاد الدولي للاتصالات، **تقرير حول الرقم القياسي العالمي للأمن السيبراني وسمات السلامة السيبرانية.** جنيف: الاتحاد الدولي للاتصالات، مكتب تنمية الاتصالات، أفريل 2015، ص ص 01-06.

نتج الرقم القياسي العالمي للأمن السيبراني (GCI) عن شراكة تعاونية بين القطاع الخاص ومنظمة دولية من أجل وضع قضية الأمن السيبراني في صدارة البرامج الوطنية. والرقم القياسي GCI ،وهو مشروع مشترك بين مؤسسة ABI للبحوث والإتحاد الدولي للاتصالات، يقدم رؤية من أجل دمج الأمن السيبراني ضمن اهتمامات الدول ذات السيادة.

والرقم القياسي GCI المتجذر في البرنامج العالمي للأمن السيبراني للاتحاد يتناول مستوى الالتزام في خمسة مجالات:

التدابير القانونية.

التدابير التقنية.

التدابير التنظيمية.

بناء القدرات.

-التعاون الدولي.

24. المرجع نفسه، ص11.

25. الجمهورية الجزائرية الديمقراطية الشعبية، قانون رقم 09-04 المؤرخ في 14 شعبان 1430،الموافق 05 أوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، **الجريدة الرسمية**، العدد 47، الصادرة بتاريخ 25 شعبان 1430 الموافق 16 أوت 2009، ص 06.

26. الجمهورية الجزائرية الديمقراطية الشعبية، مرسوم رئاسي رقم 15-261 مؤرّخ في 24 ذي الحجة عام 1436، الموافق 8 أكتوبر سنة 2015، والذي يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، **الجريدة الرسمية**، العدد 53، الصادرة بتاريخ 24 ذو الحجة 1436 الموافق08 أكتوبر 2015، ص ص 16-17.

27. ب. بوعلام، ملتقى حول: "الجيش الوطني الشعبي ورهانات تداول المعلومة عبر شبكات التواصل الاجتماعي". **مجلة الجيش** الصادرة عن مؤسسة المنشورات العسكرية، العدد 630، جانفي 2016، ص 39.

28. الهام غازي، الوقاية ومكافحة الجريمة المعلوماتية في التشريع الجزائري. **مجلة الجيش** الصادرة عن مؤسسة المنشورات العسكرية، العدد 630، جانفي 2016، ص 43.

29. ب. بوعلام، المرجع السابق الذكر، ص ص 38-39.

30. حمدون إ. توريه، "الاستجابة الدولية للحرب السيبرانية". في كتاب: الاتحاد الدولي للاتصالات، **البحث عن السلام السيبراني**. جنيف: الاتحاد الدولي للاتصالات، يناير 2011، ص82.