السياسات العامة الجزائرية في مجال السيبرانية: الواقع والتحديات

Algerian Public Policies in The Field of Cyber: Reality and challenges

بورياح سلمة *
جامعة امحمد بوقرة بومرداس، الجزائر
s.bouriah@univ-boumerdes.dz

تاريخ الإرسال: 30/ 09/ 2020* تاريخ القبول: 12/21 / 2022 * تاريخ النشر: 31/ /01 / 2023

ملخص:

أضحت السياسات السيبرانية هاجسا بالنسبة للدول وصناع القرار من أجل تحقيق الأمن السيبراني للفرد والدولة على حد السواء، خاصة في ظل الحكومة الإلكترونية والتطورالمتسارع لتكنولوجيا المعلومات والاتصالات. وعليه تهدف هاته الدراسة إلى بحث سبل بناء سياسات عامة جزائرية متكاملة في مجال الأمن السيبراني. وارتأينا الاستعانة بالمنهج التحليلي كمنهج علمي يهدف إلى تحليل وتشريح سياسات الأمن السيبراني الحالية وسبل زيادة نجاعتها. وقد توصلت الدراسة إلى أن بناء سياسات واستراتيجية وطنية في مجال الأمن السيبراني يتطلب تكثيف التعاون بين المؤسسات الحكومية والقطاع الخاص، وتطوير وتنفيذ سياسات قائمة على اقتصاد المعرفة والابتكار والتنافسية والتكوين وتشجيع إنشاء الشركات الناشئة في مجال التكنولوجيا الحديثة لتحقيق السيادة الرقمية.

الكلمات المفتاحية: السياسات العامة، الأمن السيبراني، استراتجية، الجزائر، منظومة معلوماتية.

Abstract:

Cyber policies have become a concern for states and decision-makers in order to achieve cybersecurity for the individual and the state alike, especially in light of e-government and the rapid development of information and communication technology. Accordingly, this study aims to examine ways of building integrated Algerian public policies in the field of cybersecurity. We decided to use the analytical method as a scientific method aimed at analyzing and dissecting current cybersecurity policies and ways to increase their effectiveness. The study found that building national policies and strategy in the field of cybersecurity requires intensifying cooperation between government institutions and the private sector, developing and implementing policies based on knowledge economy, innovation, competitiveness and training, and encouraging the establishment of emerging companies in the field of modern technology to achieve digital sovereignty.

Keywords: *Public Policies, Cybersecurity, Strategy, Algeria, Information System.*

* **بورياح سلمة**

مقدمة:

أضحى الأمن السيبراني جزءا أساسيا من أنظمة الأمن سواء الأمن الاجتماعي أو التربوي أو الصحي، المالي أو الاقتصادي أو السياحي أو العلمي أو المصرفي باعتباره الحلقة الأساسية والأكثر فاعلية في أمن الأفراد والمنظمات والدول. وتحقيق الأمن السيبراني أو على الأقل جزء منه ليس بالهدف الهين بل هو تحد جد صعب في بيئة تكنولوجية جد متسارعة تعرف تهديدات متنوعة في أبعادها وآلياتها، بفعل ازياد الاعتماد على تكنولوجيا المعلومات والاتصالات واتساع مجال الفضاء السيبراني. ما جعله يحتل أهمية كبيرة في السياسات العامة ولدى صانعي القرار.

تعالج هاته الدراسة مسألة السياسات العامة السيبرانية للدولة الجزائرية وهو موضوع جد هام يتعلق بتحدي جديد يضاف إلى تحديات التي تواجه الدولة في تأمين وحماية أمنها المعلوماتي في بيئة تكنولوجية جد معقدة ومتسارعة. وتهدف الدراسة إلى التفكير بصفة جدية في بناء سياسة سيبرانية عامة ناجعة وفعالة، فتحقيق مستوى من الأمن الوطني والقومي يكون بتطوير البُنى السيبرانية وتعزيزها بالخبرات الجديدة وتأهيل المورد البشري. من أجل رفع الكفاءة العلمية والتقنية على المدى الواسع. على هذا الأساس نطرح سؤال البحث التالي، ما هي أفضل السبل لتصميم وتنفيذ سياسات عامة جزائرية فعالة تحقق الأمن السيبراني؟

من خلال السؤال، سنحاول اختبار الفرضية الآتية: يتطلب بناء سياسات عامة جزائرية فعالة في مجال الأمن السيبراني وجود إطار قانوني ومؤسساتي قوي ومتكامل وكذا تكاثف جهود المؤسسات الحكومية والقطاع الخاص وتشجيع المؤسسات الناشئة في مجال التكنولوجيا وتنمية الوعي المجتمعي.

إن الاجابة على سؤال البحث واختبار فرضيته يستدعي الاستعانة بالمنهج التحليلي الذي يساعد على تحليل الموضوع عبر خطة مكونة من ثلاث محاور رئيسية، المحور الأول تناولنا فيه الأمن السيبراني دراسة في المفهوم والأبعاد، المحور الثاني تطرقنا فيه إلى السياسة العامة السيبرانية الأسس والفاعلين، المحورالثالث حللنا محددات السياسات السيبرانية الجزائرية.

1- الأمن السيبراني دراسة في المفهوم والأبعاد.

يرتبط الأمن السيبراني بأمن الفرد والمنظمة والدولة على حد السواء لخصوصيته المرتبطة بالفضاء الرقمي متخطي الحدود وأيضا لارتباطه بشتى نواحي الحياة الحديثة، وهذا ما سنتناوله في هذا المحور بالتعرف على مفهوم الأمن السيبراني وأبعاده.

1-1- مفهوم الأمن السيبراني:

انبثقت عبارة Cyber من أعمال نوربت واينر Norbert Weiner، عندما حاول تطوير نظريته عن رسائل السبرنتيكا Cybernetics والتي تعود إلى اليونانية ومن مشتقاتها معنى الإدارة والحكم. حيث كان يستهدف ضبط البيئة التي يوجد فيها الكائن والتحكم فيها لملائمة احتياجاته. (شلبى، 2002، ص.ص، 145-146). وفي سنة 1834 استعمل الفيلسوف الفرنسي أندري ماري أمبار André-marie Ampére مصطلح Cybernétique في كتابه « Essai sur la philosophie des sciences » حيث كتب أن الحكومة "تحتاج إلى الاختيار بين أنسب التدابير لتحقيق أهدافها" وبالنسبة لـ Ampére ، السيبرنتيك Cybernetics هي فن الحكم"، وهو مؤهل كعلم من الدرجة الثالثة إلى جانب القوة والديبلوماسية. (Baumard, 2017, p2) وفي

عام 1984استخدم مؤلف الخيال العلمي وليام جيبسون مصطلح الفضاء الإلكتروني في روايته The Neuromancer التي تتمحور حول لص البيانات القادر على إجراء اتصالات بين عقله وشبكة عالمية تربط أجهزة الكمبيوتر ببعضها البعض.(Arpagian, 2018, p9) و Cyber معناها افتراضي أو تخيُلي، تم استعمالها لوصف الفضاء الذي يضم الشبكات المحوسبة ومنها اشتقت صفة السيبراني التي تعني علم التحكم الأوتوماتي أو علم الضبط. (بري، 2019، ص17)

أما الأمن السيبراني فهو أمن الفضاء المعلوماتي، وهو تعبير أشمل وأعم من أمن المعلومات. فالمقصود بأمن المعلومات "مجموعة من الإجراءات والتدابير الوقائية التي تُستخدم للمحافظة على المعلومات وسريتها والمحافظة عليها من السرقة أو الإختراق، ومن زاوية أكاديمية هو العلم الذي يبحث في نظريات وأساليب حماية البيانات والمعلومات ويضع الأدوات أو الإجراءات اللازمة لضمان حمايتها". وللمحافظة على أمن البيانات والمعلومات في النظام يجب توفر عناصر السرية، التكامل وسلامة المحتوى، التوافر والإتاحة.(البار، المرجي، 2018، ص ص،1-2) كما يُعرف أيضا بأنه "مجموع الوسائل والأدوات والاجراءات اللازم توفرها لضمان حماية المعلومات من الأخطار الداخلية والخارجية". (الخمايسة، 2017، ص288)

ويُعرف الأمن السيبراني بأنه "مجموع الوسائل التقنية والإدارية التي يتم استخدامها لمنع الإستخدام غير المصرح به وسوء الإستغلال واستعادة المعلومات الإلكترونية ونظم الإتصالات والمعلومات التي تحتويها بهدف ضمان توافر واستمرارية عمل نظم المعلومات وتأمين حماية وسرية وخصوصية البيانات الشخصية ولحماية المواطنين".(البار، المرجي، 2018، ص8) كما يرى نيكولا أرباجان Arpagain Nicoclas أن الأمن السيبراني " يتعلق الأمن في الفضاء السيبراني بالتقنيات والعمليات والسياسات التي تساعد على منع أو تقليل التأثير السلبي للأحداث في الفضاء السيبراني، التي يمكن أن تقع نتيجة لإجراءات متعمدة باستخدام تكنولوجيا المعلومات من قبل فاعل معاد أو خبيث". (Clarck, Berson and Herbert, 2013, p9) أما بالنسبة للتعريفات التي وضعتها الحكومات والدول للأمن السيبراني، فقد عرفت وزارة الدفاع الأمريكية للأمن السيبراني بأنه "جميع الإجراءات التنظيمية اللازمة لضمان حرية المعلومات بجميع أشكالها الإلكترونية والمادية من مختلف الجرائم، الهجمات، التخريب، التجسس، الحوادث." أما الاتحاد الأوربي عرف الأمن السيبراني بأنه "الضمانات والإجراءات التي يمكن استخدامها لحماية المجال السيبراني، سواء في المجال المدني والعسكري، من تلك التهديدات المرتبطة أو التي قد تضر بشبكاتها المترابطة وبنيتها التحتية للمعلومات، ويسعى الأمن السيبراني إلى الحفاظ على توفر ونزاهة الشبكات والبنية التحتية وسرية المعلومات الواردة فيه".
(Christou, 2016, p7) فالملاحظ أن تعريف الدول للأمن السيبراني مختلف من دولة لأخرى حسب أولوياتها وحسب استراتجيتها. كذلك الأمر بالنسبة للجزائر التي عرفت الأمن السيبراني بموجب القانون رقم18-04 وهذا ما سنراه في المحور الثالث.

وبناءا على ما سبق فإن الأمن السيبراني يهدف للمساعدة على حماية أصول وموارد المنظمات من النواحي التنظيمية والبشرية والمالية والتقنية والمعلوماتية بحيث تسمح بمواصلة مهمتها. والهدف الأكبر هو عدم تضررها تضررا دائما والحد من الضرر الناجم أو سوء الأداء وضمان إستعادة العمليات العادية لحالتها السابقة خلال إطار زمني مقبول وبتكلفة مقبولة في أعقاب وقوع حادث أمني. (دليل، 2006، ص8)

1-2- أبعاد الأمن السيبراني:

إنطلاقا من ارتباط الأمن السيبراني بمقْدرة الدولة على حماية مصالحها وشعبها في مختلف مجالات حياته اليومية ومسيرته نحو التقدم، فإن الأمن السيبراني يطال جميع المسائل الاقتصادية والاجتماعية والسياسية

والإنسانية اضافة إلى ارتباطه بسلامة مصادر الثروة في العصر الحالي من بيانات، معلومات، القدرة على الاتصال والتواصل، باعتباره يتمحور حول الانتاج والإبداع والقدرة على المنافسة. مايجعله متعدد الأبعاد من أبعاد عسكرية، تتجسد خصوصا في الهجمات السيبرانية التي قد تتحول ماديا إلى اندلاع صراعات مسلحة مثل ما وقع بين روسيا وجورجيا. أو اختراق أنظمة المنشآت النووية وإمكانات التلاعب بها كالذي حدث في إيران، أو الاختراقات التي حدثت للبنية التحتية للطاقة من انقطاع التيار الكهربائي وآثاره السلبية على ملايين الأشخاص في كل من البرازيل والمملكة المتحدة. وأبعاد اجتماعية تتجلى في طبيعة الانترنت المفتوح خصوصا عبر الشبكات الاجتماعية، ما يسمح للمواطنين بأن يعبروا على تطلعاتهم السياسية وطموحاتهم الاجتماعية، وذلك بتبادل الأفكار والخبرات، إضافة إلى إمكانات الوصول إلى مختلف المجالات العلمية والثقافية والخدماتية، أيضا وصولها إلى أبعد المناطق وشمولها لمختلف فئات المجتمع. انطلاقا من هذا فإن تحقيق الأمن في الفضاء السيبراني يُعد ضرورة مجتمعية لحمايته من المحتويات غير المشروعة وغير المرغوبة خاصة منها ذات التأثير السلبي على أخلاقيات المجتمع. بالنسبة للأبعاد السياسية فتتمثل في حق الدولة في حماية كيانها ونظامها السياسي ومصالحها الاقتصادية وحقها وواجبها في تحقيق رفاه شعبها.(جبور، 2016، ص29) أما الأبعاد الاقتصادية فترجع إلى الرابطة القوية بين الأمن السيبراني والاقتصاد، خاصة اقتصاد المعرفة. الذي يساهم في تعزيز التنمية الاقتصادية للدول. غير أن ذلك يطرح عدة إشكالات سواء تعلق الأمر بمقدمي الخدمات من شركات وبنوك أو بحماية المستهلكين على الانترنت.(جبور،ص30) من الجرائم السيبرانية التي قد تكون ضارة على العديد من المستويات حيث تؤدي إلى فقدان الملكية الفكرية والمعلومات التجارية مما يقلل القدرة التنافسية للشركات.(أبو زيد، 2019، ص56) كما تؤدي أيضا إلى الاحتيال وتشويه السمعة.

2- السياسات العامة السيبرانية الأسس والفاعلين

تختلف السياسات العامة السيبرانية عن غيرها من السياسات العامة ويرجع ذلك إلى اختلاف بيئتها وكذا الفاعلين المساهمين فيها وهذا ما سوف نوضحه فيما يلي.

2-1- مفهوم السياسات العامة السيبرانية:

في أبسط تعريفاتها تعتبر السياسات العامة السيبرانية "السياسات التي تمكن الدولة من تعظيم الإستفادة من الشبكة المعلوماتية وتفادي مخاطرها".(بري، 2019، ص95) كما تُعرف السياسات العامة السيبرانية على أنها "مجمل القوانين والسياسات، الأدوات، النصوص، المفاهيم، وميكانيزمات الأمن وطرق تسيير الأخطار، والممارسات التكنولوجية المتعلقة بتكنولوجيا المعلومات والإتصالات لحماية الدول والمنظمات والأشخاص".(رضوان، 2016، ص 40) غير أن هاته السياسة ليست مثل باقي السياسات العامة الأخرى أو السياسات القطاعية من حيث وضوح الفاعلين ومجال عملهم، وذلك راجع للفضاء السيبراني الذي يتجاوز الجغرافيا واضعا الحكومة في مشكلة أساسية هي الحماية والعقاب، أي حماية المنشآت وعقاب المجرمين الذين لا يمكن تحديد أماكنهم دائما ما يجعل الأمن السيبراني يمثل تحديا صعبا بالنسبة للحكومات. (Elaine ,Kamarch, 2012, p110)

وقد أصبح الأمن السيبراني يحتل مكانة مهمة في صنع السياسة الحكومية مع بداية القرن العشرين وخصوصا مع بداية العقد الثاني منه مع دمقرطة الانترنت وأدوات التشفير وعمل الحكومات بأنظمة البيانات المفتوحة.(Baumard, 2017, p2) كذلك لأن الانترنت وتكنولوجيا المعلومات والاتصالات غدت ضرورية للتنمية الاقتصادية والاجتماعية وللبنية التحتية الحيوية، باعتبارها مصدر لتحقيق النمو ومحرك للابتكار والرفاهية الاجتماعية والتعبير الفردي. وأيضا بسبب تطور التهديدات السيبرانية وازديادها بوتيرة سريعة، سواءا من قبل الجهات الإجرامية أو من مصادر جديدة، مثل الدول الناشئة والجماعات السياسية، وقد يكون لديها دوافع أخرى غير كسب المال مثل بعض الأنواع إذا كانت أعمال القرصنة مجهولة الهوية، كأن يكون هدفها زعزعة الاستقرار مثل حالة استونيا2007، أو التخريب حالة ستكسنت وحتى العمليات العسكرية. (OCED, 2012, p p,11-12)

وتعتبر مسألة حماية البنية التحتية مسألة بالغة الأهمية في الأمن السيبراني، باعتبار الدولة أصبحت اليوم تعتمد على قطاعات الاتصالات والمال والاقتصاد والطاقة والنقل، التي تعتمد بدورها على المكننة الذاتية والأتمتة أو التحكم الآلي الحاسوبي. ومع تطور تقنيات المعلومات والاتصالات ساهمت في مستوى تقدم الخدمات وخفض التكاليف ورفع الكفاءة ما أدى إلى تطور البنية التحتية، وفي المقابل أدى ذلك إلى تحديات جديدة.(العويضي، 2010، ص101) خاصة تلك المتعلقة بتقنيات والتطبيقات التي تتحكم في البنية التحتية ومدى اعتمادها على الأنظمة المعقدة والثغرات الأمنية التي قد يتسلل منها القراصنة والمخربون، فنجاح القطاعات سواء حكومية أو خاصة في تقديم الخدمات مرتبط باعتماديتها المقبولة أوغير المقبولة. هاته الاعتمادية تنبع من مصدرين أساسين مصدر طبيعي ومصدر بشري، يتجسد المصدر الطبيعي خاصة في الكوارث الطبيعية فهو غالبا ما يتسبب في تعطيل الخدمات المتعلقة بالبنية التحتية مثل انقطاع الكهرباء أو زيادة الأحمال بسبب الضغط أو تأثير الرطوبة على أسلاك الضغط العالي، أما المصدر البشري فهو متعلق بالأخطاء في التصاميم أو التشغيل أو أعطال متعمدة بواسطة ناشطين عدائيين وقراصنة.(العوضي، ص. ص، 102-103) الذين تتنوع مصادر عملهم من الاعتداء على البيانات الرقمية، الدخول غير المشروع إلى الأنظمة المعلوماتية، الاعتراض غير المشروع للبيانات والاتصالات المعلوماتية، الجرائم المخلة بالآداب العامة، الاعتداء على الملكية الفكرية، إنتحال الهوية الإلكترونية، الإحتيال الإلكتروني، المطاردة السيبرانية، جرائم الاتجار بالبشر وبالمخدرات وغسل الأموال الإلكتروني، الجرائم المنظمة والعابرة للحدود.(خوري، رمال،2017، ص7) لذا وجب الاهتمام بالتهديدين الطبيعي والبشري وإعطاءه الأولوية في سياسات عامة طويلة الأمد يأخذ فيها موضوع الاعتمادية موقعه المناسب كهدف مهم للمحافظة على استدامة عمل شبكات البنية التحتية والمنشآت الحيوية والأمنية للدولة والأنظمة المالية والمرافق الحكومية، وذلك من خلال الاستثمار في البحوث العلمية التي تسهم في رفع الاعتمادية في جميع الشبكات الحيوية والإلكترونية والعمل على بناء وإرساء بنية تحتية رقمية قوية.

2-2- السياسات العامة الدولية في مجال الأمن السيبراني :

يرجع بداية التعاون الدولي في المجال السيبراني إلى عام 2000 حيث تعهد رؤساء الدول في قمة الأرض بتحقيق الأهداف الإنمائية للألفية. ففي المجال السيبراني دعا الهدف الثامن إلى تعاون الدول مع القطاع الخاص من أجل إتاحة فوائد تكنولوجيا المعلومات والاتصالات للذين لديهم فرص قليلة في الوصول إليها. (Obiso and Fowlie, 2012, p81)، وفي 2004 تضمن الإعلان الصادر عن القمة العالمية لمجتمع المعلومات المنعقدة بجنيف، الرغبة في بناء مجتمع معلومات محوره الإنسان وغايته تحقيق التنمية بناءا على مبادئ ميثاق

الأمم المتحدة واحترام الإعلان العالمي لحقوق الإنسان. فمثلا يشير القسم "ب5 "من الإعلان إلى الحاجة إلى تعزيز الثقة في أمن المعلومات وأمن الشبكات، المصادقة الإلكترونية، الخصوصية وحماية المستهلك كشرط لتنمية مجتمع المعلومات وبناء الثقة لدى مستخدمي تكنولوجيا المعلومات والاتصالات.(Domingo and Martinez, 2012, p195) وبناءا على إعلان جنيف ثم قمة تونس لمجتمع المعلومات سنة 2005، وضع الإتحاد الدولي للاتصالات الأهداف المتوخاة لسياسات الأمن السيبراني وهي تعزيز التعاون بين الحكومات في الأمم المتحدة وكل أصحاب المصلحة، وجوب تعاون الحكومات مع القطاع الخاص للوقاية من الجرائم السيبرانية ورفع مستوى الوعي وتشجيع التعليم وتثقيف المواطنين بنظام الخصوصية على الانترنت، اتخاذ الاجراءات المناسبة بشأن الرسائل المزعجة على المستوى الوطني والدولي، تشجيع تكييف القوانين المحلية مع استخدام الوثائق والمعاملات الإلكترونية وغيرها من الأهداف. (Domingo and Martinez, p196)

وفي 17 ماي2007 أطلق الأمين العام للإتحاد الدولي للاتصالات، جدول أعمال الأمن السيبراني العالمي The Global Cybersecurity Agenda من أجل تقديم إطارعمل يمكن من خلاله الاستجابة للتحديات المتنامية للأمن السيبراني، من خلال إشراك كل أصحاب المصلحة من حكومات وقطاع خاص ومجتمع مدني ومنظمات دولية. باعتبار أنه لن تنجح إمكانات تطوير برامج وخدمات الصحة الالكترونية والتعليم الإلكتروني والتجارة الإلكترونية إلا إذا كانت البنية التحتية لتكنولوجيا المعلومات والاتصالات آمنة. وترتكز إستراتيجية الإطارعلى خمسة أركان هي: الإجراءات القانونية - الإجراءات الفنية - الهياكل التنظيمية - بناء القدرات - التعاون الدولي. حيث يجب أولا وضع القوانين الوطنية التي تستند على الاتفاقيات الدولية خاصة الجرائم الالكترونية والهجمات السيبرانية وكيفيات معالجتها، ثم تحديد الحلول التقنية وتطويرها مع مراعاة المعايير العالمية للتقييس التي يضعها الاتحاد الدولي للاتصالات. وأيضا إنشاء الهياكل التنظيمية مثل مراكز التنسيق وفرق الاستجابة لحوادث الكمبيوتر من أجل الاستجابة السريعة للهجمات السيبرانية والتنسيق مع نظرائهم على المستوى الدولي. (Obiso and Fowlie, 2012 , p83)

هاته الاستراتيجية تطورت إلى مؤشر الأمن السيبراني العالمي لقياس مدى نجاعة وفعالية السياسات المنتهجة من قبل الدول في هذا المجال، ولمساعدتها على مقارنة برامجها الخاصة بالأمن السيبراني باستثمارات وبرامج الدول الأخرى. وفي عام 2015 نشرت منظمة التعاون الاقتصادي والتنمية OCED توصية حول إدارة مخاطر الأمن الرقمي لتحقيق الازدهار الاقتصادي والاجتماعي من أجل توفير المعلومات اللازمة لتطوير الاستراتيجيات الوطنية التي تهدف لإدارة الأمن الرقمي ولتحسين الفوائد الاقتصادية والاجتماعية المتوقعة من الانفتاح الرقمي. وتتجسد هاته التوصية في إطار عمل مبني على منهج إدارة المخاطر مكون من ثمانية مبادئ عالية المستوى ومتكاملة هي: زيادة الوعي، اكتساب المهارات والتمكين، مسؤولية أصحاب المصلحة، حقوق الإنسان والقيم الأساسية، التعاون، تقييم المخاطر ودورة العلاج، التدابير الأمنية المناسبة والمتناسبة مع الخطر والنشاط الاقتصادي والاجتماعي المعرض للخطر، الابتكار، الجاهزية وتخطيط الاستمرارية. وخاصية هاته العناصر الثمانية هي تحسين آليات التنسيق داخل الحكومة ومع أصحاب المصلحة غير الحكوميين وتوصي المنظمة أن التعاون بين القطاع الخاص والقطاع الحكومي أساسي لخفض المخاطر السيبرانية.(هاثواي، ص6)

وتعد حماية الفضاء السيبراني أمر جد معقد لأنه يجمع مجالات عديدة في السياسات العامة، بما في ذلك العدالة الجنائية والتكنولوجيا، توحيد المقاييس، التعاون، البحث والتطوير، تنظيم السوق كما يتطلب الأمن السيبراني المشاركة الفاعلة للقطاعين العام والخاص والأفراد.(Robinson, 2012, p160) على سبيل المثال تعتمد المقاربة الأوربية للسياسات السيبرانية على التقسيم الصارم للعمل بين الشق المدني والشق العسكري

للأمن السيبراني. حيث طور الاتحاد الأوربي سياسات مرتكزة على الدفاع المدني في الفضاء السيبراني، تتقاسمها الحكومات مع القطاع الخاص. بينما الدول الأعضاء في الاتحاد تكون مسؤولة عن العمليات العسكرية. أما بالنسبة لسياسات واستراتيجيات الأمن السيبراني في الولايات المتحدة الأمريكية، هي تتبع مقاربة لامركزية للأمن السيبراني حيث تتحكم وزارة الدفاع في متابعة الجريمة، وتكون وزارة الأمن الوطني مسؤولة عن النطاقات بالتنسيق مع القطاع الخاص.(Kamarch, 2012, p117) أما تركيا فقد جعلت الأمن السيبراني ضمن الأجندة اليومية للدولة سنة2010، كما أسست سنة 2012 هيئة الأمن السيبراني بموجب القانون رقم3842 (أوغلو، 2019، ص51) كذلك تونس جعلت استراتيجية تطوير الأمن السيبراني ضمن أولويات الأمن القومي بإعلانها في جويلة 2018 عن إعداد استراتيجية وطنية للأمن السيبراني.(الجمهورية التونسية، 2020، ص3)

2-3- الفاعلين في مجال السياسات العامة السيبرانية:

في أي سياسة عامة نجد مجموعة من الفاعلين الرسمين وغير الرسميين، غير أنه في السياسات العامة السيبرانية الأمر يختلف قليلا ويصعب الفصل فيه لإعتبارات عديدة منها، أنه يُشرف على إدارة الفضاء السيبراني القطاع التجاري بشكل أساسي وهذا الفضاء غير مركزي بطبيعته، كما أنه من الصعب التنبؤ بطريقة استخدام الفضاء السيبراني في المستقبل نظرا لسرعة التغيير والابتكار والتطور التكنولوجي.(الأمم المتحدة، 2015، ص7) ما جعل الدولة ليست الفاعل الأساسي في الجانب المعلوماتي، ويرجع فلوريدي لوتشيانو Luciano Floridi ذلك إلى أربع عوامل رئيسية، العامل الأول هو السلطة فتكنولوجيا المعلومات والاتصالات أدت إلى إضفاء الطابع الديمقراطي على البيانات والقدرة على تجهيزها والتحكم فيها، لأنها تستطيع أن تنشئ وتتيح وتمكن عددا غير محدود من الوكلاء غير التابعين للدولة من الفرد إلى الجمعيات إلى المنظمات الدولية الحكومية وغير الحكومية إلى الشركات متعددة الجنسيات في الساحة السياسية. فالدولة لم تعد الفاعل الوحيد وأحيانا ليست حتى الفاعل الرئيس الذي يستطيع أن يمارس سلطة معلوماتية على عناصر وسيطة معلوماتية أخرى من الأفراد والجماعات. أما العامل الثاني هو الجغرافيا حيث كسرت تكنولوجيا المعلومات والاتصالات حواجز الحدود الإقليمية بجعلها قابلة للإختراق أو في بعض الحالات منعدمة الأهمية تماما. فالتكنولوجيا خلقت مناطق يعمل فيها عناصر وسيطة " وكلاء" ليسوا بالضرورة عناصر بشرية، ما خلق جدلا للدولة التي لا تزال تُحدد هويتها وشرعيتها بالوحدة الإقليمية ذات السيادة بوصفها بلدا. ويرجع العامل الثالث إلى التنظيم، فقد ميعت تكنولوجيا المعلومات والاتصالات الطبولوجيا السياسية، متجاوزة الطرق التقليدية في الإدارة والتمكين، التجميع وإعادة التفكيك وإعادة التجميع المرن والسريع، لجماعات موزعة عند الطلب بشأن مصالح مشتركة، ممثلة في الطبقات الاجتماعية والأحزاب السياسية والانتماء العرقي وعوائق اللغة والعوائق الطبيعية وما شابه ذلك بل هي أيضا تشجع كل ذلك ما يولد جماعات جديدة متنوعة ومتساوية السلطة من المنظمات غير التابعة للدولة والتي من الممكن أن تكون أكثر قوة ونفوذا مقارنة بالدولة ذات السيادة القديمة. وأخيرا تعيد الديمقراطية والتغيرات في السلطة والجغرافيا والتنظيم صياغة الجدل حول الديمقراطية، حيث أصبحت وسائط الإعلام الاجتماعي الجديدة تقود الديمقراطية بما يسمى الديمقراطية الرقمية. (فلوريدي، 2017، ص 220-222) فهاته العوامل الأربعة جعلت مجال المعلوماتية مجالا أو نظاما متعدد الفاعلين من الدولة إلى الأفراد إلى الجمعيات، المنظمات الدولية الحكومية وغير الحكومية إلى الشركات التجارية التي تتولى خاصة إدارة الفضاء السيبراني إلى عناصر وسيطة قد لا يكونوا بالضرورة عناصر بشرية.

وبناءا على ماسبق فإن تبني سياسات عامة سيبرانية قوية تُعد من أهم الخطوات لتأمين البنى التحتية والخدمات السيبرانية الوطنية التي يعتمد عليها المستقبل الرقمي والرفاه الاقتصادي للدولة الحديثة.(هاثواي، ص12) والجزائر قد خطت العديد من الخطوات في سبيل تحقيق ذلك وهذا ما سوف نبحثه في المحور التالي.

3- محددات السياسات السيبرانية الجزائرية:

عملت الجزائر منذ بداية القرن الحالي على مواكبة التغيرات العالمية في مجال السياسات العامة السيبرانية بدءا بتكييف تشريعاتها وقوانينها بما يتماشى مع المعاهدات والاتفاقيات الدولية وأيضا التطورات التكنولوجية، كما أنشأت العديد من المؤسسات إلى جانب تعزيز التعاون الدولي في المجال السيبراني وهذا ما سنراه في هذا المحور.

3-1-المنظومة القانونية:

في إطار مراجعة قوانين الجمهورية لتكييفها مع التطورات التكنولوجية العالمية وأيضا مع المعاهدات والاتفاقيات الدولية التي أبرمتها الجزائر ومن أجل مواكبة عصر المعلومات راجعت الجزائر القوانين التالية:

-القانون رقم 04- سنة 2004 المعدل لقانون العقوبات، خاصة القسم السابع مكرر تحت عنوان المساس بأنظمة المعالجة الآلية للمعلومات، حيث صنف الجرائم المعلوماتية إلى أربعة أنواع: الجرائم التي تمس سرية وسلامة وأمن معطيات النظام، الجرائم المعلوماتية كالتزوير والغش والمساس بالمعطيات، الجرائم المتعلقة بالموضوع كالتصميم، النشر، البحث، التجميع والحيازة، وأخيرا الجرائم الماسة بحقوق المؤلف والحقوق المجاورة. (فولان، 2010، ص32) وفي سنة 2009، أصدرت الجزائر القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، حيث هدف هذا القانون إلى وضع قواعد خاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، كما وضح بعض المصطلحات المرتبطة بتكنولوجيا الاعلام والاتصالات، كالتعريف بالجرائم المتصلة بتكنولوجيا الإعلام والاتصال، ومصطلحات منظومة معلوماتية، معطيات معلوماتية، مقدمو الخدمات، المعطيات المتعلقة بحركة السير أي معطيات متعلقة بالاتصال عن طريق منظومة معلوماتية، والاتصالات الإلكترونية.كما حدد هذا القانون الحالات التي يسمح بها باللجوء إلى المراقبة الإلكترونية في المادة 4، كما ما يلي:

- الوقاية من الأفعال الموصوفة بجرائم الإرهاب والتخريب 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 الإلكترونية.
- في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.

كما حدد هذا القانون أن المحاكم الجزائرية تختص بالنظر في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال المرتكبة خارج الإقليم الوطني عندما يكون مرتكبها أجنبيا وتستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني"أو المصالح الاستراتيجية للاقتصاد الوطني.(القانون رقم 09-04، ص.ص، 5 -6)

وفي سنة 2015 صدر القانون رقم 15-03 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الالكتروني، حيث حدد في مادته رقم 5 أنه يجب أن تتواجد على التراب الوطني كل البيانات والمعلومات ذات الطابع الشخصي التي تم جمعها من مؤدي خدمات التصديق الإلكتروني أو الطرف الثالث الموثوق أو سلطات

التصديق الإلكتروني وكذلك قواعد البيانات التي تحتويها ولا يمكن نقلها إلى خارج التراب الوطني إلى في الحالات التي ينص عليها التشريع المعمول به.(القانون رقم 15-03، ص8)

وفي سنة 2018 صدر القانون رقم 18-04 المحدد للقواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية حيث وضح أن نشاطات البريد والاتصالات الالكترونية تخضع لرقابة الدولة، وأن هاته الأخيرة تمارس صلاحياتها وفق ما يلي:

-ممارسة السيادة طبقا للأحكام الدستورية على كامل فضائها الهيرتيزي .

-الإنفراد بالاستعمال الحصري لطيف الذبذبات اللاسلكية الكهربائية وضمان التخطيط وتقسيمه إلى ذبذبات ومراقبته والإشراف على استعماله من طرف المستعملين في ظل احترام مبادئ الفعالية والرشادة في استعمال الذبذبات اللاسلكية الكهربائية.

- تحديد قواعد شغل الأملاك العمومية والاستفادة من الارتفاقات المرتبطة بانتشار شبكات الاتصالات الإلكترونية وباستعمال الفضاء الهيرتيزي.

-السهرعلى تطبيق اتفاقيات وأنظمة وتوصيات الاتحاد الدولي للاتصالات.(القانون رقم 18-04، ص5)

كما قدم هذا القانون تعريف للأمن السيبراني بأنه: "مجموع الأدوات والسياسات ومفاهيم الأمن والآليات الأمنية والمبادئ التوجيهية وطرق تسيير المخاطر والأعمال والتكوين والممارسات الجيدة والضمانات والتكنولوجيات التي يمكن استخدامها في حماية الاتصالات الإلكترونية ضد أي حدث من شأنه المساس بتوفر وسلامة وسرية البيانات المخزنة أو المعالجة أو المرسلة".(القانون رقم 18-04، ص7) أيضا صدر القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في معالجة المعطيات ذات الطابع الشخصي في ذات السنة، وهدف هذا القانون إلى تحديد قواعد حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي مهما كان مصدرها أو شكلها في إطار احترام الكرامة الإنسانية والحياة الخاصة والحريات العامة وألا تَمسَ بحقوق الأشخاص وشرفهم وسمعتهم. محددا مصطلح معالجة المعطيات ذات الطابع الشخصي التي تعني "كل عملية أو مجموعة عمليات منجزة بطرق أو بوسائل آلية أو بدونها على معطيات ذات طابع شخصي مثل جمع أو التسجيل أو التنظيم أو الحفظ أو الملائمة أو التغيير أو الاستخراج أو الإطلاع أو الاستعمال أو الإيصال عن طريق الإرسال أو النشر أو أي شكل من آخر من أشكال الإتاحة أو التقريب أو الربط البيني وكذا الإغلاق أو التشفير أو المسح أو الإتلاف.(القانون 18-07، ص11) كما أكد المشرع الجزائري على حماية المعطيات ذات الطابع الشخصي للأطفال بإعتبارهم شريحة هامة من المجتمع وأيضا كأفراد لهم حماية خصوصية. حيث جاء في نص المادة 8 " لا يمكن القيام بمعالجة المعطيات ذات الطابع الشخصي المتعلقة بالطفل إلا بعد الحصول على موافقة ممثله الشرعي أو عند الاقتضاء بترخيص من القاضي المختص".

أ يضا صدر القانون رقم 18-05 المتعلق بالتجارة الإلكترونية سنة 2018 ،حدد هذا القانون القواعد العامة المتعلقة بالتجارة الإلكترونية للسلع والخدمات. كما حدد المستهلك الإلكتروني، المورد الإلكتروني والإشهار الإلكتروني وكذا وسيلة الدفع الإلكترونية. وكذا الجرائم والعقوبات المترتبة عنها.

بناءا على هذا نجد أن الجزائر ركزت بشكل أساسي على مكافحة الجرائم السيبرانية بداية من صدور قانون العقوبات 2004، إلى قانون 2009، ثم سنة 2015 أصدرت قانون التوقيع والتصديق الإلكتروني الذي لا يزال يعرف تأخرا ملحوظا في التطبيق أيضا أصدرت قانون حماية المعطيات الشخصية وقانون البريد والاتصالات الإلكترونية، ثم قانون التجارة الإلكترونية سنة 2018. وهو ما يعكس توجهات الدولة الأمنية وأيضا يرجع لتخلف الجزائر في مجال الاقتصاد الرقمي والتجارة الإلكترونية ووسائل الدفع الإلكتروني وكذا تأخر البنوك والمصارف الجزائرية في تطبيق نظام المعاملات الإلكترونية واعتمادها على المعاملات التقليدية.

2-3- المنظومة المؤسساتية :

بتفحص المؤسسات القائمة على الأمن السيبراني بشكل عام نجد في المقدمة المؤسسات التابعة لوزارة الدفاع التي كانت سباقة في إنشاء مؤسسات تعنى بحماية الأمن السيبراني الجزائري بالتركيز أولا على مكافحة الجريمة ثم وضع الاستراتيجيات الدفاعية لتأمين المنشآت الوطنية الرقمية وفق ما يلي:

- **مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية للدرك الوطني**: أنشأ سنة 2008 بهدف تأمين منظومة المعلومات لخدمة الأمن العمومي. ومن ومهامه تحليل المعطيات وبيانات الجرائم المعلوماتية المرتكبة وتحديد هوية أصحابها سواء كانوا أشخاص فرادى أو عصابات لأجل تأمين الأنظمة المعلوماتية والحفاظ عليها، بالإضافة إلى مساعدة الأجهزة الأمنية الأخرى في أداء مهامها.(بارة، 2017، ص435)

- **المصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة لمديرية الأمن الوطني:** أنشأت سنة 2011، ثم أنشأت المصلحة المركزية لمحاربة الجرائم المتصلة بتكنولوجيا الإعلام والإتصال سنة 2015.(بارة، ص437)

- **مصلحة الدفاع السيبراني ومراقبة أمن الأنظمة:** أنشأت بتاريخ 6 نوفمبر 2015 على مستوى دائرة الاستعمال والتحضير لأركان الجيش الشعبي الوطني مهمتها تخطيط وإدراج ومتابعة حالة تقدم تجسيد السياسة الشاملة للدفاع السيبراني لتحقيق الحماية ضد التهديدات السيبرانية المستهدفة لأنظمة المعلومات منظومات الاتصال. كما تساهم هاته الهيئة مع الهيئات الوطنية المعنية إعداد ووضع سياسة وطنية للدفاع السيبراني، إضافة إلى التنسيق مع مختلف الهيئات لتأمين المنشآت الرقمية الحساسة. (بوكبشة، 2017، ص35)

- **المركز الوطني للإشارة والحروب الالكترونية:** الذي أنشأ سنة 2019، وهو تابع لدائرة الإشارة وأنظمة المعلومات والحرب الالكترونية، التابعة لوزراة الدفاع.(غرارمي، 2019، ص8)

وفي مقابل المصالح التابعة لوزارة الدفاع الوطني نجد مجموعة من المؤسسات ذات الطابع المدني أغلبها سلطات ضبط ، أو سلطات رقابية، أو استشارية مستقلة أنشأت بموجب القوانين السابقة الذكر، وهي كالآتي:

- **الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحته**: استحدثت بموجب القانون09-04، حيث تضمن الفصل الخامس منه إنشاء هاته الهيئة. (القانون رقم 09-04، 2009، ص6) دون تحديد تشكيلة هاته الهيئة وتنظيمها حتى صدر المرسوم الرئاسي رقم 15-261 سنة 2015 الذي حدد تشكيلة وتنظيم وسيرها، بجعلها سلطة إدارية مستقلة لدى الوزير المكلف بالعدل تمارس مهامها تحت رقابة السلطة القضائية. ومن مهامها: إقتراح عناصر الإستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، مساعدة السلطات القضائية ومصالح الشرطة القضائية في مجال مكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال بما في ذلك جمع المعلومات والتزويد بها من 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 اخرى.

- تجميع وتسجيل وحفظ المعطيات 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 المعنية بالجرائم المتصلة بتكنولوجيا الإعلام والاتصال.

-المساهمة في تكوين المتخصصين في مجال التحريات التقنية المتصلة بتكنولوجيا الإعلام والاتصال.
- المساهمة في تحديث المعايير القانونية في مجال اختصاصها.(المرسوم الرئاسي 15-261، ص.ص، 16-17)

كما حدد هذا المرسوم أن الهيئة يرأسها وزير العدل ومن أعضائها وزير الداخلية، وزير تكنولوجيا الإعلام والإتصال، قائد الدرك الوطني، المدير العام للأمن الوطني، ممثل عن رئاسة الجمهورية، ممثل عن وزارة الدفاع، قاضيان من المحكمة العليا يعينهما المجلس الأعلى للقضاء. كما تزود الهيئة بقضاة وضباط و أعوان للشرطة القضائية من المصالح العسكرية للإستعلام والأمن والدرك الوطني والأمن الوطني، أيضا تزود بمستخدمي الدعم التقني والإداري من المصالح العسكرية للاستعلام والدرك الوطني والأمن الوطني. والملاحظ أن هاته الهيئة باشرت عملها بمصالحها الإدارية والتقنية فور صدور المرسوم في الجريدة الرسمية في 2015، غير أن تعيين تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال لم يتم حتى سنة 2019، حيث صدر المرسوم الرئاسي رقم 19-172 الصادر بتاريخ 6 يونيو 2019. أبرز ما جاء في هذا المرسوم هو وضع السلطة تحت سلطة وزير الدفاع الوطني، أي تحويل تبعية السلطة من وزارة العدل إلى وزارة الدفاع الوطني. وبالنسبة لتنظيمها فهي تتشكل من مجلس توجيه ومديرية عامة، يرأس مجلس التوجيه وزير الدفاع أو ممثل ينوب عنه ويتشكل المجلس من ممثلي وزارات الدفاع الوطني، الداخلية، العدل، الموصلات السلكية واللاسلكية. تكون مهمة المجلس، التداول حول الاستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها، أيضا التداول حول مسائل التطوير والتعاون مع المؤسسات والهيئات الوطنية المعنية بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال، القيام دوريا بتقييم حالة التهديد في مجال الجرائم المتصلة بتكنولوجيات الإعلام والاتصال للتمكن من تحديد مضامين عمليات المراقبة الواجب القيام بها والأهداف المنشودة بدقة.(المرسوم الرئاسي19-172، ص. ص، 5-6)

-السلطة الوطنية للتصديق الإلكتروني: هي هيئة استشارية أنشأت سنة 2015 تُصنف كسلطة إدارية مستقلة تابعة للوزير الأول، مُكلفة بترقية استعمال التوقيع والتصديق الإلكترونيين وتطويرهما وضمان موثوقية استعمالهما. كما أنها تقدم استشارات بخصوص أي نص تشريعي أو تنظيمي ذي صله بالتوقيع والتصديق الإلكترونين.(القانون رقم 15-03، ص. ص، 9-10) فهي سلطة استشارية.

-السلطة الحكومية للتصديق الإلكتروني: هي سلطة رقابية أنشأت سنة 2015 وهي تابعة للوزير المكلف بالبريد وتكنولوجيات الإعلام والاتصال، مهمتها متابعة ومراقبة نشاط التصديق الإلكتروني وكذا توفير خدمات التصديق الإلكتروني لفائدة المتدخلين في الفرع الحكومي.(القانون رقم 15-03، ص 10)

- **سلطة ضبط البريد وللاتصالات الإلكترونية**: هي سلطة ضبط أنشأت سنة 2018 وهي مُكلفة بضمان ضبط أسواق البريد والاتصالات الإلكترونية لحساب الدولة، كما تسهر على وجود منافسة فعلية ومشروعة في سوقي البريد والاتصالات الإلكترونية باتخاذ تدابير من شأنها ترقية واستعادة المنافسة في هاتين السوقين. ومن مهامها أيضا السهر على احترام متعاملي البريد والاتصالات الإلكترونية للأحكام القانونية والتنظيمية المتعلقة على الخصوص بالبريد والاتصالات الإلكترونية والأمن السيبراني.(القانون رقم 18-04، ص10)

- **السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي**: أنشأت سنة 2018، وهي سلطة إدارية مستقلة، تابعة لرئيس الجمهورية. (القانون 18-07، ص 16) دون أن يفصل القانون في مهامها.

- **منظومة وطنية لأمن الأنظمة المعلوماتية**: أنشأت بموجب المرسوم الرئاسي رقم 20-05 الصادر بتاريخ 20 جانفي2020. وبموجب المادة 2 المنظومة أداة الدولة في مجال أمن الأنظمة المعلوماتية وتشكل الإطار التنظيمي لإعداد الإستراتيجية الوطنية لأمن الأنظمة المعلوماتية وتنسيق تنفيذها، وهي تابعة لوزارة الدفاع

الوطني. وتتكون المنظومة من مجلس وطني لأمن الأنظمة المعلوماتية ووكالة لأمن الأنظمة المعلوماتية. الملاحظ أن المشرع لم يستعمل مصطلح سيبرانية بل استعمل أمن الأنظمة المعلوماتية هاته الأخيرة التي سبق له تعريفها في قانون09-04، والمنظومة تتكون من هيئتين واحدة عسكرية وهي الهيئة العليا التي تضع الاستراتيجة والأخرى مدنية مستقلة ماديا ومعنويا ذات طابع تنفيذي.

مجلس وطني لأمن الأنظمة المعلوماتية: يُكلف بإعداد إستراتيجية وطنية لأمن الأنظمة المعلوماتية والموافقة عليها وتوجيهها. كما يتولى أيضا مهام البت في عناصر الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية المقترحة من قبل الوكالة وتحديدها، دراسة مخطط عمل الوكالة وتقرير نشاطاتها والموافقة عليها، دراسة التقارير المتعلقة بتنفيذ الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية والموافقة عليها، الموافقة على اتفاقات التعاون والاعتراف المتبادل مع الهيئات الأجنبية في مجال أمن الأنظمة المعلوماتية، الموافقة على سياسة التصديق الإلكتروني للسلطة الوطنية للتصديق الإلكتروني، الموافقة على تصنيف الأنظمة المعلوماتية، اقتراح ملائمة الإطار الهيكلي أو التنظيمي الخاص بأمن الأنظمة المعلوماتية. كما يبدي المجلس رأيا مطابقا في أي مشروع نص تشريعي أو تنظيمي ذي صلة بأمن الأنظمة المعلوماتية. يرأس المجلس وزير الدفاع، ويتكون المجلس من ممثل عن كل من، رئاسةالجمهورية، الوزير الأول، الخارجية، الداخلية، العدل، المالية، الطاقة، الاتصالات، التعليم العالي. كما يحضر رئيس الوكالة بصفة استشارية.(المرسوم الرئاسي 20-05، ص 6)

وكالة أمن الأنظمة المعلوماتية: تُكلف بتنسيق تنفيذ الإستراتيجية الوطنية لأمن الأنظمة المعلوماتية. وهي مؤسسة عمومية ذات طابع إداري تتمتع بالشخصية المعنوية والإستقلالية المالية. تشمل مهامها تحضير عناصر الإستراتيجية الوطنية في مجال أمن الأنظمة المعلوماتية وعرضها على المجلس، تنسيق تنفيذ الإستراتيجية الوطنية المحددة من المجلس. أيضا من مهامها إجراء تحقيقات رقمية في حالة الهجمات أو الحوادث السيبرانية التي تستهدف المؤسسات الوطنية، تقديم المشورة والمساعدة للإدارات والمؤسسات والهيئات العمومية والخاصة من أجل وضع إستراتيجية وطنية، ضمان اليقظة التكنولوجية في مجال أمن الأنظمة المعلوماتية، اقتراح مشاريع نصوص تشريعية أو تنظيمية في مجال أمن الأنظمة المعلوماتية بعد الرأي المطابق للمجلس، تنشيط وتوجيه البحث في مجال أمن الأنظمة المعلوماتية. تدير الوكالة لجنة توجيه وتُزود بلجنة علمية، وتحتوي الوكالة مركز وطني عملياتي لأمن الأنظمة المعلوماتية ومديريات ومصالح تقنية وإدارية موضوعة تحت سلطته، وتتكون لجنة التوجيه من ممثلي وزارات: الدفاع، الخارجية، الداخلية، العدل، المالية، الطاقة،التعليم العالي، الصناعة، الاتصالات، التجارة، مصالح الأمن. وممثلي سلطات البريد والاتصالات الإلكترونية، التصديق الإلكتروني، حماية البيانات ذات الطابع الشخصي، السلطة الحكومية للتصديق الإلكتروني. وعلى سبيل الاستشارة مدير الوكالة. أما اللجنة العلمية للوكالة تتكون من 10 أعضاء يتم اختيارهم لمدة ثلاث سنوات قابلة للتجديد من طرف لجنة التوجيه، يتم اختيارهم من بين أساتذة والباحثين والخبراء في مجال أمن الأنظمة المعلوماتية. تستشار اللجنة العلمية في المسائل ذات الطابع العلمي تندرج ضمن نشاطات البحث والتطوير في مجال أمن الأنظمة المعلوماتية. (المرسوم الرئاسي 20-05، ص، 7- 9)

ومن بين ما جاء به القانون أن تُلزم المؤسسات والإدارات والهيئات العمومية والمتعاملون الخواص بتعيين مسؤولهم المكلف بأمن الأنظمة المعلوماتية في أجل أقصاه سنة ابتداءا من تاريخ نشر المرسوم.(المرسوم الرئاسي 20-05، ص 10) وهذا الأمر الإيجابي ويعتبر خطوة جيدة نحو إرساء التعاون بين القطاع العام والخاص في مجال أمن السيبراني. لأن هاته الخطوة تعزز تحقيق الأمن السيبراني كما أنها تكشف جوانب القصور والخلل في أمن الأنظمة المعلوماتية. كما أنه يدعم بناء سياسة سيبرانية متكاملة بين كل الإدارات والمؤسسات عمومية وأيضا القطاع الخاص.

3-3- المنظومة الاستراتيجية :

فالتحديات الراهنة للجزائرتستوجب بناء وإرساء بنية تحتية رقمية قوية للإندماج في البيئة العالمية في ظل تحديات ترافق هاته الخدمة مثل، معايير أمن المعلومات، إنقطاع الانترنت أو ضعف خدماتها، العقود التي تفرضها الشركات مُوردة الخدمات، والتي تتسبب في إعاقة حركة البيانات والخدمات. وهذا لا يتأتى إلا بوضع استراتيجية شاملة لكل القطاعات تتضح معالمها فيما يلي.

- **في مجال الأمن والدفاع الوطني:** أولى مخطط عمل الحكومة 2020 أهمية كبيرة للدفاع السيبراني، وذلك بالعمل على تطوير الاستراتيجية المتعلقة بالسيطرة والاستقلال الذاتي في المجال السيبراني. لمجابهة هيمنة القوى الكبرى في الفضاء الرقمي، من حماية نقل البيانات الرقمية الشخصية وكذا أمن السلطات الرقمية مرورا بأنظمة التشغيل بأكملها وخدمات الانترنت وصولا إلى الأجهزة من أجل تحقيق السيادة الرقمية.(فضيل شريف، 2020، ص 47)

- **في مجال تعزيز القدرات**: تعمل الوكالة الفضائية الجزائرية على المساهمة في تعزيز السيادة الوطنية في مجال التكنولوجيا الفضائية والاتصالات، حيث أشرفت على تطبيق البرنامج الفضائي الوطني2006-2020 الذي تكلل بإطلاق ستة أقمار صناعية، ألسات-1سنة 2002 وألسات- A2 سنة 2010، وألسات B1 وألسات –B2 وألسات N1 التي أطلقت سنة 2016 ثم إطلاق القمر الصناعي المخصص للاتصالات ألكوم سات-1 في ديسمبر2017. كما وضعت الجزائر استراتيجية فضائية وطنية 2020-2040 من بين أهدافها تأمين الاتصالات المؤسساتية والعمل على سد الهوة الرقمية ومنح الفرصة للمواطن ليكون طرفا فاعلا في المجتمع العالمي للمعلومات.(جنادي، 2019، ص.ص، 56-57)

اضافة إلى تشجيع المؤسسات الناشئة، فهي التي تعمل على انتاج وتوطين التكنولوجيا وتساهم في تحقيق السيادة الرقمية للبلاد والتخلص من المؤسسات الأجنبية المسيطرة على التكنولوجيا، وتحقيق سيادة رقمية لا يتحقق إلا بتكنولوجيا وطنية وليست مستوردة. والدولة حاليا تعمل على تشجيع و تسهيل كل السبل لمثل هاته المؤسسات، حيث أنشأت وزارة خاصة بها، فبموجب المرسوم التنفيذي 20-54 المحدد لصلاحيات وزير المؤسسات الصغيرة والمؤسسات الناشئة واقتصاد المعرفة من صلاحياته، ترقية وتطوير الحاضنات والحظائر السيبيرانية والأقطاب التكنولوجية وأقطاب الابتكار وأقطاب التنافسية. كما أنه مكلف بموجب المادة 6 من نفس المرسوم بإعداد واقتراح بالتنسيق مع القطاعات المعنية السياسة والاستراتيجية الوطنية لاقتصاد المعرفة التي تضع ترقية وتطوير المعرفة والابتكار والتكنولوجيات الجديدة لاسيما منها تكنولوجيات الرقمنة في صلب شروط التنمية وتنفيذها ومتابعتها، والتركيز على قطاعات الاقتصاد الرقمي والتعليم والتكوين اضافة إلى السهر على إنشاء أقطاب ابتكار والأقطاب التنافسية لاسيما الحظائر السيبرانية والأقطاب التكنولوجية والحظائر التكنولوجية بالاتصال مع القطاعات المعنية.(المرسوم التنفيذي 20-54، ص 8) وهذا مؤشر إيجابي سوف يساعد الشباب على خلق مؤسساته الناشئة خاصة في المجال الرقمي .

-في مجال التعاون الدولي: شاركت الجزائر في العديد من الندوات والمؤتمرات الدولية في مجال سياسات الأمن السيبراني. اضافة إلى تنظيمها العديد من التظاهرات الدولية منها ندوة دولية حول الأمن السيبراني تحت شعار "الخدمات العمومية والأمن العمومي" 27 و28مارس2018 كان من بين توصياتها إنشاء هيئة جامعة لمكافحة التهديدات السيبرانية. وتشجيع إطلاق حاضنة وطنية لدعم الشركات الجزائرية الناشئة في مجال أمن المعلومات لتطوير تكنولوجيا جزائرية ضامنة لفضاء سيبراني وطني آمن.(https://bit.ly/3l57vDB) كما احتضنت الجزائر أشغال الطبعة السابعة للقمة الإفريقية الموسومة بـ"الأمن السيبراني في عصر التحول الرقمي

في إفريقيا" 10جوان 2019، عالجت أمن الإعلام الآلي والتكنولوجيا، الاقتصاد الرقمي، الدفع الإلكتروني، الحياة الخاصة، التهديدات السيبرانية وغيرها من المواضيع. (https://bit.ly/33fAcrF)

- **في مجال التدابير التقنية:** أنشأت الجزائر CERT.DZ وهو مركز الاستجابة لطوارئ الحاسوب Computer Emergency Reponse Team(CERT) يعتبر أداة أساسية لحماية المعلومات الحساسة، بالعمل على رصد المخاطر المعلوماتية المستجدة مثل الفيروسات وبرامج التجسس ومكامن الضعف في الأنظمة التشغيلية والتعامل معها وإعطاء الحلول والتدابير بشأنها. كما يهدف إلى تمكين الأفراد والشركات من استباق الهجمات السيبرانية وتفادي الأضرار قبل وقوعها.(الأمم المتحدة، 2015، ص20) غير أن دوره لا يزال مقتصرا على التعامل مع المؤسسات العمومية والخاصة ولم يتوسع إلى التعامل مع المواطنين بتنفيذ برامج توعية شاملة لهم.

وبتحليل موقع الجزائر سنة2017، في مؤشر الأمن السيبراني العالمي الذي تقوم به مؤسسة ABI للبحوث والاتحاد الدولي للاتصالات. (انظر الجدول رقم 1 في الملاحق) نجد أن الجزائر لا تزال متأخرة خاصة في مجال التدابير التقنية لأنها لم تنشأ بعد فريق وطني للاستجابة للحوادث الأمنية الحاسوبية CIRT، الذي يعمل على توفيرالحماية الأمنية لتحديد التهديدات السيبرانية ومكافحتها والاستجابة لها وإدارتها وتعزيز الأمن السيبراني في الدولة، على أن تقترن هاته القدرة بعملية جمع المعلومات الخاصة بها بدلا من عملية الإبلاغ عن الحوادث من مصادر أخرى. إضافة إلى التأخر في المعايير والمقاييس المعتمدة من قبل الحكومة أو التي تحظى بتأييدها لأجل تنفيذ معاييرالأمن السيبراني المعترف بها دوليا داخل القطاع العام وداخل البنى التحتية الأساسية حتى لو كان القطاع الخاص يقوم بتشغيلها. وتشمل هاته المعايير على سبيل المثال لا الحصر تلك التي تضعها وكالات كل من المنظمة الدولية للتوحيد القياسي(ISO)، الاتحاد الدولي للاتصالات(ITU)، فريق مهام هندسة الاتصالات(IETE)... وغيرها. اضافة إلى إصدار الشهادات يعنى وجود أطر معتمدة من الدولة أو تحظى بتأييدها من أجل منح الشهادات واعتماد وكالات حكومية وطنية ومهنيي القطاع العام بموجب معايير الأمن السيبراني المعترف بها دوليا. وتتضمن هاته الشهادات والاعتمادات على سبيل المثال لا الحصر، معرفة أمن الحوسبة السحابية، التحليل الجنائي في مجال الأمن السيبراني، شهادة هندسة البرمجيات... وغيرها. (Global cybersecurity Index, 2015, p 32)

فالجزائر حسب المؤشر، لم تصل إلى مرحلة آمنة في مؤشرات الأمن السيبراني للدولة، باستثناء الجانب التشريعي والمؤسساتي اللذين وصلت إلى مرحلة مقبولة فيهما وهذا راجع للإجراءات التي اتخذتها الدولة والتي ذكرناها سابقا، غير أن الإجراءات المتخذة ليست في مجال بناء القدرات خاصة تنظيم الدورات التدريبية المحترفة، والصناعات الموطنة والبرامج التعليمية، فهي بحاجة إلى بذل المزيد من المجهودات. وفيما يتعلق بالإجراءات التنظيمية لا تزال غير كافية من وضع استراتيجة واضحة المعالم وخطة شاملة للتنفيذ، تراعي الاحتياجات التي تتطلبها حماية البنى التحتية للمعلومات على الصعيد الوطني. كذلك بخصوص الشراكة بين مؤسسات القطاع العام وبين القطاع العام والقطاع الخاص فإنها تحتاج المزيد من الجهود لتطويرها.

بناءا على ما سبق يمكن القول أن الأمن السيبراني لم يدخل بعد في صلب العديد من الاستراتيجيات التكنولوجية الوطنية والصناعية، حتى وإن تعددت جهود الدولة إلا أنها عامة تتسم بالانتقائية والتشتت. فسياسة عامة قوية في مجال الأمن السيبراني تتطلب تكامل جهود العديد من القطاعات العدل، المؤسسات التعليمية والوزارات وشركات القطاع الخاص ومطوري التكنولوجيا، وكذا الشراكات بين القطاعين العام والخاص ضمن

الدولة نفسها. كما يتطلب إشراك المجتمع المدني وحملات التوعية للمواطنين. فقد أظهرت إحصائيات عالمية أن أغلب الهجومات السيبرانية الناجحة تدخل ضمن تسمية "الهندسة الاجتماعية" التي تستغل نقائص مردها السلوكات البشرية،(بوكبشة، 2017، ص3) خاصة النساء والأطفال، لذا يجب القيام بعمليات تحسيسية بصفة مستمرة لترسيخ ثقافة الاستعمال الأمثل للتكنولوجيا الحديثة وخاصة المواقع الإلكترونية ومواقع التواصل الاجتماعي.

الخاتمة:

تطرقنا في هاته الدراسة إلى مفهوم السياسات العامة السيبرانية باعتبارها سياسات متميزة عن باقي السياسات العامة الأخرى لوحودها في بيئة تكنولوجية جد متطورة وسريعة التغير وأيضا لصعوبة تحديد الفاعلين فيها. ما يطرح مشكلا بالنسبة للدول خاصة النامية منها وبالنسبة للجزائر تطرقنا الى معالم السياسات العامة السيبرانية فيها من الجانب القانوني والمؤسساتي والاستراتيجي والتقني وخلصت الدراسة إلى أنه لابد من بذل المزيد من الجهود في سبيل بناء سياسات متكاملة وفعالة خاصة في مجال بناء تكنولوجيا وطنية ومستقلة، وتكثيف التعاون والتنسيق بين مختلف المؤسسات الحكومية والخاصة كل حسب قطاعه وأيضا تنمية الوعي المجتمعي بمخاطر الفضاء السيبراني.

وقد توصلت الباحثة لمجموعة توصيات:

- تعديل مرسوم إنشاء المجلس الأعلى للأمن، بما يسمح بإدراج الأمن السيبراني ضمن الأولويات الوطنية وأن تكون هناك هيئة وطنية عليا لمتابعة كل ما يتعلق به.

-تحديث السياسة العامة للحكومة في قطاعات الاتصالات وتكنولوجيا المعلومات بما يسمح وتوفير خدمات جديدة ومتطورة للمواطنين والشركات.

-خلق بيئة مشجعة داعمة للشباب من أجل الاستثمار في تطوير وتوسيع الشبكات والاتصالات.

-تعزيز التعاون بين القطاع الحكومي والقطاع الخاص في تبادل المعلومات ووجهات النظر والتدريب ودراسة مكامن الضعف والقوة.

-خلق تخصصات جامعية في العلوم الإنسانية والإجتماعية والعلوم التكنولوجية لمواكبة التطورات المتسارعة في هذا التخصص.

-تنظيم الندوات وورشات العمل بالتعاون بين الجامعات والمؤسسات الوطنية والدولية ذات الصلة بالأمن السيبراني من أجل تبادل الخبررات.

-إنشاء مراكز أبحاث تعنى بالأمن السيبراني في الجزائر.

- العمل على رفع الوعي المجتمعي بالمخاطر السيبرانية، والعمل من أجل ضمان الاستخدام المسؤول والآمن للتكنولوجيات الحديثة والتطبيقات الرقمية الحديثة.

-المراجع باللغة العربية:

1-الكتب:

- بري، محمود. (2019). السيبرنطيقا-السيبرانية علم القدرة على التواصل والتحكم والسيطرة. بيروت، دار العتبة العباسية المقدسة.

- جبور، منى الأشقر.(2016). السيبرانية هاجس العصر. القاهرة: جامعة الدول العربية، مركز البحوث القانونية والقضائية.

- الخمايسة، صدام محمد طالب.(2017). الحكومة الذكية ما بعد الحكومة الإلكترونية، دبي، قنديل للطباعة والنشر والتوزيع.
- العويضي، فريج بن سعيد. (2010). حروب تقنية المعلومات، السعودية: (د.د.ن).

- فلوريدي، لوتشيانو. (2017). الثورة الرابعة كيف يعيد الغلاف المعلوماتي تشكيل الواقع الإنساني. ترجمة: لؤي عبد المجيد السيد، الكويت: عالم المعرفة.

2- المقالات:

-أبو زيد، عبد الرحمن عاطف. (2019). الأمن السيبراني في الوطن العربي دراسة حالة المملكة العربية السعودية، مجلة آفاق سياسية، (العدد48) ، شهر أكتوبر، ص، 55-61.

-أوغلو، أرسين هاجموت. (2019). سياسات الاستخبارات والأمن السيبراني في تركيا، مجلة رؤية تركية، ربيع(العدد8)، ص،43 -59.

-بارة، سمير.(2017). الدفاع الوطني والسياسات الوطنية للأمن السيبراني في الجزائرالدور والتحديات، مجلة دفاتر السياسة والقانون، المجلد (العدد)، الجزائر،جامعة قاصدي مرباح ورقلة، ص، 426-442.

-بوكبشة، محمد. (2017). الأمن والدفاع السيبراني أولوية قصوى، مجلة الجيش، أكتوبر(العدد 651)، الحزائر: وزارة الدفاع الوطني، ص، 32-37.

-جنادي، إسماعيل. (2019). البرنامج الفضائي الوطني تعزيز السيادة الوطنية، مجلة الجيش، ديسمبر، (العدد677)، الجزائر: وزارة الدفاع الوطني، ص 56-59.

-رضوان، ج. (2016). الأمن السيبراني أولوية في استراتيجيات الدفاع، مجلة الجيش، جانفي(العدد 630)، الجزائر: وزارة الدفاع الوطني، ص ص،40-41.

-غرارمي، عبد الغني.(2019). الحروب المستقبلية هي بالأساس حرول إلكترونية، مجلة الجيش، نوفمبر(العدد 676)، الجزائر: وزارة الدفاع الوطني، ص8-9

-فضيل شريف، سهام. (2020). السيادة الرقمية الجزائرية. ترجمة: لعجوزي سهام، مجلة الجيش، مارس (العدد280) الجزائر: وزراة الدفاع الوطني، ص46-47.

-فولان، محمد. (2010). الحماية القانونية لتكنولوجيا الإعلام. مجلة المحكمة العليا، العدد1، الجزائر: المحكة العليا.

3- النصوص القانونية:

- القانون 09-04. (2009). المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 47، الصادرة بتاريخ 08أوت 2009.

- القانون15-04. (2015). المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، الجريدة الرسمية، العدد06، الصادرة بتاريخ 10فيفري2015.
- القانون 18-05. (2018). المتعلق بالتجارة الإلكترونية، الجريدة الرسمية، العدد28، الصادرة بتاريخ 16ماي 2016.
- القانون18-04. (2018). المتضمن القواعد العامة التعلقة بالبريد والاتصالات الإلكترونية، الجريدة الرسمية، العدد27، الصادرة بتاريخ 13ماي2018.
- المرسوم الرئاسي19-172. (2019). المحدد لتشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها وتنظيمها وكيفيات سيرها، الجريدة الرسمية، العدد37، الصادرة بتاريخ 09جوان2019.
- المرسوم الرئاسي20-05. (2020). المتعلق بوضع منظومة وطنية لأمن المعلوماتية، الجريدة الرسمية، العدد04، الصادرة بتاريخ 26 جانفي2020.
- المرسوم التنفيذي16-135. (2016). المحدد لطبيعة السلطة الحكومية للتصديق الحكومي وتنظيمها وشكلها، الجريدة الرسمية، العدد26، الصادرة بتاريخ 28 أفريل2016.
- المرسوم التنفيذي 20- 54 . (2020). المحدد لصلاحيات وزير المؤسسات الصغيرة والمتوسطة والمؤسسات الناشئة واقتصاد المعرفة، الجريدة الرسمية، العدد12، الصادرة بتاريخ 25فيفري2020.

4- المؤتمرات :

- الخوري،جنان. رمال محمد. (2017). مؤتمر الأمن والدفاع السيبراني تحديات وآفاق. بيروت، الجامعة اللبنانية والوكالة الجامعة للفرنكفونية.

5-التقارير :

- الإتحاد الدولي للإتصالات. (2006). دليل الأمن السيبراني للدول النامية.

- الجمهورية التونسية. (2020). الاستراتيجية الوطنية للأمن السيبراني، رئاسة الجمهورية التونسية: مجلس الأمن القومي.

- الأمم المتحدة.(2015). الأمان في الفضاء السيبراني ومكافحة الجرائم السيبرانية في المنطقة العربية توصيات سياساتية، نيويورك.

6- المواقع الإلكترونية:

-البار، عدنان مصطفى. المرجي، خالد علي. أمن المعلومات والأمن السيبراني. 2018، تاريخ التصفح : 10 أكتوبر 2019. https://bit.ly/30h2jom

-هاثاواي، ميليسا، إدارة الخطر السيبراني الوطني. تاريخ التصفح: 25أكتوبر2019 https://bit.ly/33ctmmP

- الأمن السيبراني في عصر التحول الرقمي الإفريقي موضوع نقاش بالجزائر العاصمة، 10جوان 2019، تاريخ التصفح 24 أفريل 2020. https://bit.ly/33fAcrF

-الندوة الدولية حول الأمن السيبراني: الدعوة إلى إنشاء هيئة تقنية تحت سلطة رئاسة الجمهورية، وكالة الأنباء الجزائرية، 29 مارس 2018. تاريخ التصفح: 24 أفريل 2020. https://bit.ly/3l57vDB

- المراجع باللغة الأجنبية:

-Books:

Baumard, Philippe.(2017). Cybersecurity in France. Springer

Arpagain , Nicoclas.(2018). La cybersécurité, Press universitaires de France, paris.

Christou, George. (2016). Cybersecurity in the European Union resilience and adaptability in governance policy. Palgravr Macmillan , UK.

Obiso Marco , Fowle Gray.(2012)Toward A global Approch to Cybersecurity. in Anderasson kim, cybersecurity public sector Threats and responses , taylor and francis group, USA .

Domingo , Icnacio Alamillo. Martinez, Agusti cerrillo.(2012). A local Cybersecurity Approach : the case of catalana . in Anderasson kim, cybersecurity public sector Threats and responses , taylor and francis group, USA.

Kamarck, C. Elaine.(2012). The Cybersecurity Policy Challenge : The Tyranny of Geography. in Anderasson kim, cybersecurity public sector Threats and responses , taylor and francis group, USA.

Robinson, Neil. (2012). European Cybersecurity Policy. in Anderasson kim, cybersecurity public sector Threats and responses , taylor and francis group, USA.

Rapport:

-International Telecommunication Union.(2015). Global Cybersecurity Index.

-International Telecommunication Union.(2017). Global Cybersecurity Index.

-OECD.(2012).Cybersecurity policy making at a turning Point.

الملاحق:

جدول رقم 01: ترتيب الجزائر وفق مؤشر الأمن السيبيراني العالمي لسنة 2017 .

تشريعات الجرائم السيبرانية	
تشريعات الأمن السيبراني	
التكوين في المجال السيبراني	
الإجراءات التشريعية	
المقاييس الوطنيةCIRT/CERT/CSIRT	
المقاييس الحكوميةCIRT/CERT/CSIRT	
المقاييس القطاعيةCIRT/CERT/CSIRT	
مقاييس المنظمات	
مقاييس المحترفين	
حماية الأطفال	
الإجراءات التقنية	
الاستراتيجية	
الوكالات المسؤولة	

تحديد معايير مرجعية وطنية	
الإجراءات التنظيمية	
هيئات التقييس	
الممارسات السيبيرانية الجيدة	
برامجR&D	
حملات التوعية العامة	
دورات تدريبية احترافية	
برامج التعليم	
آليات التحفيز	
الصناعات الموطنة	
بناء القدرات	
الاتفاقيات الثنائية	
الاتفاقيات المتعددة الأطراف	
الشراكة الدولية	
الشراكة العمومية مع الخواص	
الشراكة بين الوكالات الحكومية	
التعاون	
GCIمؤشر الأمن السيبيراني العالمي	

Source : International Telecommunication Union.(2017). Global Cybersecurity Index, p 31.