إشكالية المواطنة في ظل قيم التكنولوجيا الحديثة
بين حرية المواطن و الأمن السيبراني
Problematic citizenship under modern technology values between citizen freedom and cyber security

خيلية وريدة [1]،

[1] كلية الإعلام والاتصال، جامعة الجزائر3 (الجزائر)، douctoura.warda2012@gmail.com

تاريخ الإرسال: 2019/02/21 تاريخ القبول:2021/04/04 تاريخ النشر: جوان/2021

الملخص:

مع القرن الجديد حلت معطياته ومتطلباته متعددة تواكب تسارع تطورات تكنولوجيا المعلومات والاتصالات الحديثة في عصر الانفجاريات المعرفية والثقافية، وتعقد شبكات الاتصال والتواصل بتكنولوجيا ذات مستوى عال سمح بانفتاح أوسع على القيم الإنسانية العالمية، ما ساهم حتما في إعادة تشكيل الكثير من القيم والمفاهيم كمفهوم المواطنة وحرية المواطن.

فأصبح من حق المواطن أن يستخدم تكنولوجيا المعلومات والاتصالات في جميع مجالات نشاطه اليومي ما جعلها من ابرز سمات العصر الحديث، نظرا لقوة تأثيرها في المجتمع، وبالتالي تأثيرها بشكل مباشر أو غير مباشر على الأمن الوطني وآليات ضمانه، ودخول التكنولوجيا الحديثة في جميع مجالات الحياة البشرية، ما أوجد مخاطر وتهديدات للمواطن وللدولة على السواء.

وفرض هذا الواقع بعض البصمات على النظام الأمني، ما أدى إلى إنشاء مواقع ومنصات جديدة بما في ذلك أدوات جديدة لضمان الأمن، والحفاظ على التوازن بين الأمن الوطني وحرية المواطن لتكفل له حقا أساسيا من حقوق المواطنة. لحماية أمن المواطن و الوطن كان لابد من تأمين البيانات والمعلومـات التي تتداول عبر الشبكات الداخلية أو الخارجية لمستخدمي الأنترنات أفراد ومؤسسات الدولة، لذلك توصلت الدول إلى إنشاء نظام سمي بالأمن السيبراني يهتم بأمن المعلومات على أجهزة وشبكات الحاسب الآلي، والآليات التي يتم من خلالها حماية معدات الحاسب الآلي والمعلومات والخدمات أو أي تغيير أو اختلاف قد يحدث مـن أي تدخـل غير مقصود أو غير مصرح به.

الكلمات المفتاحية: المواطنة ; التكنولوجيا الحديثة ; حرية المواطن ; الأمن السيبراني

Abstract:

Citizens have the right to use information and communication technologies in all areas of daily activity make it one of the most striking features of the modern era, due to the strength of their impact in society, and therefore its impact directly or indirectly on national security guarantee mechanisms. And access to modern technology in all areas of human life, creating serious risks and threats for both ordinary citizens and the State. And the spread of modern technology values imposed on society, to be important technological issues not

المؤلف المرسل: خيلية وريدة ،الايميل: **douctoura.warda2012@gmail.com**

only related to national security and the security of the State, but also concerns related to the need to ensure national security, personal security and integrity of government data and profile. This fact has imposed some imprints on the security system, leading to the creation of new sites and platforms, including new tools to ensure security, and to maintain a balance between national security and citizen freedom to ensure a fundamental right of citizenship. To protect the security of the citizen and the homeland it was necessary to secure data and information circulating through the internal or external networks of users of the Internet individuals and institutions of the state, so the countries reached the establishment of a system called cybersecurity concerned with the security of information on computer devices and networks, and mechanisms through which computer equipment, information and services or any change or difference may occur from any unintentional or unauthorized interference.
KEY WORDS: Citizenship, information security, cyber security, cyber strategy.
unintentionally as a deliberate crime, The legislator has set different penalties for her in terms of the victim's status and cases.
Key words: Libel, punishment, legislator, reprimand

المقدمة:

في ظل التغيرات التكنولوجية العالمية الجديدة، وجدت الدولة نفسها مجبرة على التخلي على النظام التقليدي، واستخدام تكنولوجيا المعلومات والاتصال الحديثة في جميع المجالات من الاقتصاد والسياسة إلى الطاقة النووية، والتقنيات العسكرية والفضائية، بل وتستخدم اليوم في القضايا الأمنية لضمان الأمن القومي. حيث اتجهت إلى استخدام الفضاء السيبراني وتكنولوجيا المعلومات والاتصالات نظرا لتأثيرها المتزايد على الشبكات الاجتماعية وعلى الحياة اليومية التي أوجدت واقعا جديدا للحكومات وللمواطنين على السواء.

أمام تأثير تكنولوجيا المعلومات تغير الهيكل الاجتماعي للمجتمع الحديث، حيث تخلل الواقع الافتراضي جميع مجالات الوجود البشري، سواء في مجال السياسة الخارجية أو في داخلها، ويعمل على تغيير متطلبات التقنيات الأمنية بصفة مستمرة، أدت إلى الانتقال من المجتمع الاجتماعي الواقعي إلى مجتمع الشبكات، تم عبره تخفيض الفضاء الجغرافي والحدود عمليا إلى الصفر.

فرض هذا الواقع بعض البصمات على النظام الأمني، ما أدى إلى إنشاء مواقع ومنصات جديدة بما في ذلك أدوات جديدة لضمان الأمن، والحفاظ على التوازن بين الأمن الوطني وحرية المواطن لتكفل له حقا أساسيا من حقوق المواطنة.

الإشكالية: ما سبل التوازن بين حرية المواطن التكنولوجي الحديث وبين تدخل الجهاز الأمني لحماية الوطن والمواطن من أخطار تكنولوجيا المعلومات والاتصال الحديثة؟

سنعتمد في نقاشنا لهاته الإشكالية على عدد من المحاور:

المحور الأول: المواطنة الأمن السيبراني وأمن المعلومات

1-مفهوم المواطنة(اللغوي والاصطلاحي)

2- مفهوم أمن المعلومات(المصطلح، الأهداف)

3-مفهوم الأمن السيبراني (المصطلح، الأهمية، المجال،الفعالية)

المحور الثاني: الإستراتيجية السيبرانية وحرية المواطن

1-حدود النظام الأمني(التوازن بين حرية المواطن والأمن) 2-الإستراتيجية السيبرانية

3-التهديات والإخطار السيبـرانية، عناصرها وسبل تفاديها 4- القطاعات المستهدفة والبرامج

2- **المحور الأول: المواطنة، الأمن السيبراني وأمن المعلومات**

1.2- مفهوم المواطنة(اللغوي والاصطلاحي)

أولا المفهوم اللغوي: مع القرن الجديد حلت معطياته ومتطلباته متعددة متسارعة تسارع تطورات تكنولوجيا المعلومات والاتصالات الحديثة **في عصر الانفجاريات المعرفية والثقافية، وتعقد شبكات الاتصال والتواصل بتكنولوجيا ذات مستوى عال سمح بانفتاح أوسع على القيم الإنسانية العالمية، ما ساهم حتما في إعادة تشكيل الكثير من القيم والمفاهيم كمفهوم المواطنة.**

كلمة المواطنة في اللغة العربية مأخوذة من كلمة الوطن أي المنزل أو المكان الذي يقيم فيه الفرد، أي أن موطن الإنسان يتحدد بمكان إقامته. حيث يقال في اللغة العربية : "طن يطن وطناً، أي أقام به، و وطن البلد أي اتخذ هذا البلد وطناً له و منه توطن البلد، أي أتخذه وطناً، سواء ولد فيه أم لا"[1].

و يعرف قاموس علم الاجتماع مفهوم المواطنة بأنه:"مكانة أو علاقة اجتماعية تقوم بين فرد طبيعي ومجتمع سياسي."[2] و يعرفه علم النفس بأنه : "شعور بالانتماء و الولاء للوطن و القيادة السياسية، و هي مصدر الإشباع للحاجات الأساسية، و حماية الذات من الأخطار المصيرية"[2] و تعرف دائرة المعارف البريطانية المواطنة بأنها: "علاقة بين الفرد والدولة، كما يحددها قانون تلك الدولة بما تتضمنه من حقوق"[3]

ثانيا المفهوم الاصطلاحي: يبنى مفهوم المواطنة على شرطين، يمكن من خلالهما التوصل إلى كشف دلالة مفهوم المواطنة كمصطلح:

1-كون مصطلح المواطنة قد اكتسب مفهومه في فضاء معرفي محدد ضمن ظروف تاريخية محددة.

2-أن مصطلح المواطنة قد تفاعل مع مصطلحات أخرى، و من ثم توضح اختلافه عن تلك المصطلحات. فمصطلح المواطنة قد تداخل و مفهوم "الوطنية" الذي يعني حب الوطن" Le Patriotisme" باللغة الفرنسية. فالمصطلح إذن يحمل في مضمونه:

1-أحاسيس متعددة كالإحساس بالحب والتعلق بالوطن، و كل ما تنتجه تلك الأحاسيس من استجابات عاطفية للمواطن تجاه وطنه.

2-يحمل في مضمونه أيضا صفة "المواطن" بما تحمله الكلمة من حقوق و واجبات وطنية يتعلمها المواطن عن طريق التربية الوطنية التي يكتسبها من الأسرة و المدرسة و المسجد، و من نشاطات دور الثقافة و الشباب، و عبر ما تقدمه وسائل الإعلام المسموعة، و المرئية و المقروءة إذا التزمت كل تلك المؤسسات بتأدية وظيفتها التربوية بوطنية، **لأن مصطلح المواطنة يتضمن معاني حب الوطن و يتضمن في نفس الوقت التزامات أخلاقية واجتماعية لابد على المواطن أن يؤديها تجاه المجتمع الذي يعيش فيه,**

فحسب نظرية "العقد الاجتماعي" لـ "Jean jaque rousseau" للمواطن حقوق إنسانية يجب أن تقدم إليه وهو في نفس الوقت يحمل مجموعة من المسؤوليات الاجتماعية ملزم بتأديتها"4 باعتبارها واجبات يفرضها عليه انتماؤه إلى الوطن.

يعتبر مصطلح المواطنة قيما و سلوكيات تحددها شروط تربوية وأدبية وأخلاقية، و تكوين و ذوق حضاري وتراث، لكنها جميعا مرتبطة بقيم وثوابت المجتمع الذي يعيش فيه المواطن.

من تلك القيم نذكر:

1-القيم الأساسية الراسخة في المجتمع و مثله العليا.

2-روح المشاركة الفعلية في تسيير شؤون المجتمع بصفة عامة، سواء على المستوى الوطني أو على المستوى الخارجي. و من ثمة يمكن أن ينبثق عن مصطلح المواطنة مصطلح آخر و هو مصطلح "المواطن الفعال" الذي يشارك بصفة فعلية و فعالة رسميا أو تطوعا من أجل رفع المستوى الحضاري للوطن. فعلى الرغم من درجة الوضوح التي وصل إليها مفهوم المواطنة في الفكر الغربي المعاصر إلا أن الوعي العربي يشهد بعض التداخل بين مفهوم المواطنة و بين مفاهيم متعددة كالانتماء و الديمقراطية.

فالانتماء مفهوم ذو طبيعة نفسية اجتماعية فلسفية، ناتجة عن عملية جدلية تبادلية بين الفرد والمجتمع أو الجماعة التي يفضلها المنتمي. والمجتمع أو الجماعة ضروريان للعالم الذي ينتمي إليه الفرد، لأنه بحاجة إلى التجمع و الارتباط بالآخر. والانتماء هو حاجة أساسية (إنسانية وطبيعة سيكولوجية) للبناء النفسي للإنسان. و يعتبر الفرد أن جماعة الانتماء هي مصدر فخر واعتزاز له، لذلك يفضل أن تصبح كيانا كبيرا وقويا، بالتالي "ينبغي أن يكون الفرد متوافقا مع جماعة الانتماء ليحقق التفاعل الإيجابي ضمنها"5. لكن انتماء الفرد و توحده مع الجماعة لابد أن يكون ضمن إطار ثقافي مشترك وعناصر ثقافية معينة كاللغة والفكر والفن. حيث "يشار إلى جماعة الانتماء بـ"الجماعة المرجعية" لأنها تعتبر معياراً لتقدير ذاته، ومصدرا لتقويم أهدافه الشخصية"6 لذلك ينبغي على الفرد الاقتناع أولا بمعايير الجماعة و مبادئها و التمسك بها حتى يعمل على نصرتها والدفاع عنها، والتضحية في سبيلها إذا لزم الأمر، مقابل أن توفر الجماعة للفرد حاجياته، كالحماية والأمن والمساعدة. لكن في حال فشل الجماعة أو المجتمع في توفير تلك الحاجيات- نظرا لتأثره بالظروف الاجتماعية والسياسية والاقتصادية السائدة- فإن انتماء الفرد قد يضعف فيتملكه الشعور بالعزلة، و ينتابه الشعور بأن المجتمع ينكر عليه إشباع حاجاته، ما يدفعه إلى اتخاذ موقف سلبيا و عدائي نحو المجتمع ليلجأ إلى انتماءات بديلة ذات عواقب سلبية على الفرد والمجتمع معـا. فكلمـا زاد عطاء المجتمع لإشبـاع حاجات الفرد، كلما زاد انتماء الفرد إليه، والعكس صحيح.

لأن الفرد عندما يتخذ مواقف سلوكية إيجابية تجاه جماعة الانتماء، فإن هذه المواقف تعبر عن قوة الانتماء، أما إذا اتخذ مواقف سلوكية سلبية، فإنها تعبر عن ضعف الانتماء.

مما سبق يمكن أن نستخلص تعريفاً نظرياً للانتماء فنقول: أن الانتماء هو "اتجاه إيجابي مدعم بالحب يستشعره الفرد تجاه وطنه ، مؤكداً وجود ارتباط وانتساب نحو هذا الوطن باعتباره عضواً فيه، ويشعر نحوه بالفخر والولاء، ويعتز بهويته وتوحده معه، ويكون منشغلاً ومهموماً بقضاياه، واعيا ومدركا لمشاكله، وملتزماً بالمعايير والقوانين، والقيم الإيجابية التي تعلي من شأنه وتنهض به، محافظاً على مصالحه وثرواته، مراعياً للصالح العام، ومشجعاً ومسهماً في الأعمال الجماعية، ومتفاعلاً مع الأغلبية ولا يتخلى عن الوطن وإن اشتدت به الأزمات"[7] والانتماء منه ما هو حقيقي و ما هو مزيف، و منه ما هو انتماء لفئة معينة. وهناك حقيقة لابد أن نوضحها وهي أن الدولة الحديثة –بغض النظر عن النظام السياسي– لا تستطيع حل جميع المشاكل البسيطة على المستوى المحلي في جميع المجالات الاجتماعية والاقتصادية والبيئية، فتجبر المواطن على تحمل المسئولية الاجتماعية باعتبارها آلية لتشكيل الذات الفردية والاجتماعية لموضوعاتها، ما يؤثر تأثيراً فعالاً على حل القضايا الاجتماعية الأكثر تعقيدًا والمتعلقة بتنمية المجتمع ككل، وبالعلاقة بين الدولة والفرد.

فالإجراء العكسي والتنظيم الذاتي للمواطن لا يستوجب إن يتحدد فقط بالاحتجاج والدفاع عن حقوقهم بل يتم التعبير عنها أيضا عن طريق رفع مستوى التعليم الذاتي في مجال تكنولوجيا المعلومات,

كما أن "**المشاركة النشطة للمواطن والهيئات الحكومية والمنظمات العامة – في نظام ضمان الأمن الوطني والقومي– تساهم في توفير أمن أكثر فعالية على جميع المستويات، ولهذا فأن الثقافة السياسية والإستراتيجية للمجتمع لها دور مهم في تشكيل النظام الأمني، يترتب على هذا أن الدول والمجتمعات المهتمة بالحفاظ على التوازن بين الحرية والأمن هي الدول التي تهتم أكثر برفع مستوى معرفة المـــواطن في مجـــال تكنولوجيـــا المعلومـــات والاتصالات، وتطوير المسؤولية الاجتماعية في المجتمع**"[8].

2.2– مفهوم أمن المعلومات(المصطلح، العناصر، الأهداف)

لقد أصبح أمر أمن البيانات والمعلومات يشكل هاجسًا وموضوعًا حيويًا مهمًا للغاية. ويختص أمن المعلومات بتأمين المعلومات المتداولة عبر شبكة الأنترنت من المخاطر التي تهددها.

فأمن المعلومات هو"العلم الذي يعمل على توفير الحماية للمعلومات من المخاطر التي تهددها، أو الحاجز الذي يمنع الاعتداء عليها، وذلك من خلال توفير الأدوات والوسائل اللازم توفيرها، لحماية المعلومات من المخاطر الداخلية أو الخارجية"[9]. وهو "المعايير والإجراءات المتخذة لمنع وصول المعلومات إلى أيدي أشخاص غير مخوّلين عبر الاتصالات، لضمان أصالة وصحة هذه الاتصالات"[10] وتجدر الإشارة إلى أن إجراء حماية المعلومات إجراء قديم، لكن لم يتم استخدامه بشكل فعلي إلا في بدايات التطور التكنولوجي. **ويرتكز أمن المعلومات على عدد من الأنظمة"[11] :**

–أنظمة حماية نظم التشغيل

–أنظمة حماية البرامج والتطبيقات.

-أنظمة حماية قواعد البيانات

-أنظمة حماية الولوج أو الدخول إلى الأنظمة.

للوصول إلى الغرض من الأبحاث والاستراتيجيات، ووسائل أمن المعلومات سواء من الناحية التقنية أو الأدائية، أو إلى تحقيق أهداف التدابير التشريعية في هذا المجال لابد من ضمان توفر العناصر التالية:

1-السرية أو الموثوقية CONFIDENTIALITY : أي التأكد من أن المعلومات لن تكشف ولن يطلع عليها من قبل أشخاص غير مخولين لذلك.

2-التكاملية وسلامة المحتوى INTEGRITY : أي التأكد من أن محتوى المعلومات صحيح، ولم يتم تعديله أو العبث به، وبشكل خاص لن يتم تدمير المحتوى أو تغيره أو العبث به في أية مرحلة من مراحل المعالجة أو التبادل، سواء في مرحلة التعامل الداخلي مع المعلومات أو عن طريق تدخل غير مشروع .

3-استمرارية توفر المعلومات أو الخدمة AVAILABILITY : أي التأكد من استمرار عمل النظام المعلوماتي، واستمرار القدرة على التفاعل مع المعلومات، وتقديم الخدمة لمواقع المعلوماتية، وان مستخدم المعلومات لن يتعرض إلى منع استخدامه لها أو دخوله إليها.

فالعلاقة إذن تتقاطع بين أمن المعلومات والأمن السيبراني من حيث الاهتمام بأمن المعلومات الموجودة بالسايبر، لكنهما يختلفان فيما تبقى من الاهتمامات، و في الوقت نفسه لا نستطيع استخدام أمن المعلومات والأمن السيبراني كمترادفتين، لأن أمن المعلومات هو أعم وأوسع من الأمن السيبراني.

لكنهما يتقاطعان في مجالاتهما، من حيث الاهتمام بأمن المعلومات الإلكترونية "السايبرية" فمجال الأمن السيبراني يعتني بأمن كل ما يوجد بالسايبر ومن ضمنه "أمن المعلومات" بينما يهتم مجال أمن المعلومات بأمن المعلومات إن كانت على السايبر.

الأمن السيبراني يهتم إذن "بأمن المعلومات على أجهزة وشبكات الحاسب الآلي والعمليات، والآليات التي يتم من خلالها حماية معدات الحاسب الآلي والمعلومات والخدمات، أو أي تغيير أو اختلاف قد يحدثّ من أي تدخل غير مقصود أو غير مصرح به. حيث يتم استخدام مجموعة من الوسائل التقنية والتنظيمية والإدارية، ومنع سوء الاستغلال لمنع الاستخدام غير الإيجابي للمعلومات الإلكترونية، ونظم الاتصالات والمعلومات التي تحتويها"[12].

3-2-مفهوم الأمن السيبراني(المصطلح، الأهمية، المجال،الفعالية)

أولا: مفهوم مصطلح سيبراني: كلمة سيبراني تُشعرك بظُلمةٍ وإبهام، رُبّما لأنها كلمةٌ جديدة، يمكن استبدالها بكلمة "إلكتروني" بحرية تامة.

مصطلح السبرانية هو صفة لأي شيء مرتبط بكلمة " Cyber سيبر" مأخوذة من كلمة مرتبطة بثقافة الحواسيب، أو تقنية المعلومات، أو الواقع الافتراضي. فالسيبرانية تعني فضاء الانترنت"[13].

و"إضافة كلمة **سايبر** إلى أي شيء آخر تضفي عليه معنى الإلكترونية مثل cyber-Security تعني الأمن الإلكتروني و cyber-Attac تعني الهجمات الإلكترونية، فكلمة **سايبر** تستخدم بمعنى "الفضاء

الإلكتروني"[14]. و**عندما نقول الأمن السيبراني فأننا نتحدث عن الأمن الإلكتروني**، .والأمنُ الإلكتروني يختص بأمن كل ما يتعلق بالإلكترونيات قد يكون أمن سيّارتك أو غسّالتك في بهو المنزل أو حتى أمنُ موجات محطة الراديو التي كُنت تستمتعُ عبرها لبرنامجك المفضّل."[15]

والإلكترونيات أنواعٌ مختلفة، بالتالي يقتضي هذا أن تكون طُرُق تأمين هذه الإلكترونيات مختلفة. فأمنُ الشبكات اللاسلكية مختلفٌ عن أمن نظم المعلومات الذي بدوره يختلفُ عن أمن النظم، و أمن النظم يختلفُ عن أمن إنترنت الأشياء. كما أن الأمنُ السيبراني يتعلّق بحماية السايبر سواءً تعلّق الأمر بالمعلومات أو لم يتعلّق. ويلتقي أمن المعلومات والأمن السيبراني في نقاط تقاطع بين مجاليهما –كما أشرنا سابقا– يستخدمها البعض كعذر وحُجّة لاستخدام إحدى العبارتين مكان الأُخرى.

خلاصة القول أن مفهوم الأمن السيبراني أوسع من أمن المعلومات، حيث يعمل تأمين البيانات والمعلومات التي تتداول عبر الشبكات الداخلية أو الخارجية التي يتم تخزينها في خوادم داخل أو خارج المنظمات لمنع الاختراقات.

ثانيا:أهمية الأمن السيبراني:

في عالمنا المترابط بواسطة الشبكة، يستفيد الجميع من برامج الدفاع السيبراني. فمثلاً على المستوى الفردي يمكن أن يؤدي هجوم الأمن السيبراني إلى سرقة الهوية أو محاولات الابتزاز، أو فقدان البيانات المهمة مثل الصور العائلية.

كما تعتمد المجتمعات على البنية التحتية الحيوية، مثل محطات الطاقة والمستشفيات، وشركات الخدمات المالية، لذا فإن تأمين هذه المنظمات وغيرها أمر ضروري، للحفاظ على عمل مجتمعنا بطريقة آمنة وطبيعية: كما أن المجتمع يستفيد من البحث العلمي في مجال الأمن السيبراني. فمثلاً عندما يضم فريق تالوس 250 باحثاً يحققون في التهديدات الجديدة والناشئة، واستراتيجيات الهجوم السيبراني. فهم يكشفون عن نقاط الضعف الجديدة ، ويثقفون الجمهور بشأن أهمية الأمن السيبراني، ويعملون على تقوية أدوات المصادر المفتوحة، ما يجعل العمل على الإنترنت أكثر أمانً للجميع .

ثالثا: مجالات الفضاء السيبراني:

الفضاء السيبراني ليس الإنترنت فقط، وإنما شبكات أخرى كثيرة متصلة. والفضاء السيبراني هو مجال عملياتي و"يعتبر الميدان الخامس للحروب الحديثة في ميدان الحرب البرية والجوية والبحرية والفضائية، يستخدم للدفاع أو الهجوم على المعلومات وشبكات الحاسب الآلي، وحرمان العدو من تنفيذ نفس المقدرات"15. الفضاء السيبراني هو"مجال عالمي داخل البيئة المعلوماتية يتكون من شبكة مستقلة من البني التحتية لأنظمة المعلومات، ويتضمن ذلك الإنترنت وشبكات الاتصالات وأنظمة الحاسب والمعالجات المدمجة ولا يقتصر على شبكة الإنترنت فقط، وإنما على شبكات عالمية مثل : pstn /Gsm /Swift /Acars /gps "".[16]

مجال الأمن السيبراني مجال من مجالات علم الحاسب وعلم التشفير، وقد اشتُقَّ من علم الرياضيات التطبيقية لأهميتهما، ثم ما لبثت هذه المجالات العلمية أن حلقت في فضاء العلم الرحب، لتتمدد وتتوسع وتخرج خارج الأطر العلمية لمجالها الأب"[17].

وهو المجال الجديد الخامس للحروب الحديثة عبر البر والبحر والجو والفضاء الحقيقي وهو يمثل جميع شبكات الحاسب الآلي الموجودة حول العالم، ويشمل الأجهزة الالكترونية المرتبطة من خلال شبكة الألياف البصرية والشبكات اللاسلكية"[18].

فالأمن السيبراني إذن هو ممارسة حماية الأنظمة والشبكات والبرامج من الهجمات الرقمية التي تهدف عادةً للوصول إلى المعلومات الحساسة لتغييرها أو إتلافها، أو ابتزاز المال من المستخدمين، أو مقاطعة العمليات التجارية. وهو سلاح استراتيجي بيد الحكومات والأفراد، لاسيما أن الحربً السيبرانية أصبحت جزءا لا يتجزأ من الأساليب الحديثة للحروب والهجمات بين الدول.

من المهام الأساسية للأمن السيبراني نذكر:

1-ضمان توافر استمرارية عمل نظم المعلومات

2-تعزيز حماية وسرية وخصوصية البيانات الشخصية

3-اتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين على حدٍ سواء من المخاطر المحتملة في مجالات استخدام الإنترنت المختلفة

4-حماية الأنظمة التشغيلية من أي محاولات للولوج بشكل غير مسموح به لأهداف غير سليمة

5-التأسيس لصناعة وطنية في مجال الأمن السيبراني لتحقيق الريادة في هذا المجال

6-تعزيز حماية أنظمة تقنية المعلومات، لتكون المرجع الوطني في شؤون تخصصها، بهدف حماية مصالح الوطن الحيوية وأمنه، والبني التحتية الحساسة فيه.

7-تعزيز حماية أنظمة التقنيات التشغيلية ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات وما تحويه من بيانات.

8-مراعاة الأهمية الحيوية المتزايدة لتخصصه وتعزيز حماية الشبكات.

رابعا: فعالية الأمن السيبراني: ينتهج الأمن السيبراني الناجح نهجاً معيناً، يتكون عادة من طبقات متعددة للحماية، تنتشر في أجهزة الكمبيوتر أو الشبكات، أو البرامج أو البيانات التي ينوي المرء الحفاظ على سلامتها، لإنشاء دفاع فعال من الهجمات السيبرانية.

العناصر الأساسية المكملة:

1-المستخدمون: ينبغي على المستخدمين فهم مبادئ أمان البيانات الأساسية، والامتثال لها مثل اختيار كلمات مرور قوية، والحذر من المرفقات ذات المصدر المجهول في البريد الإلكتروني، والحرص على عمل النسخ الاحتياطي للبيانات .

2-التكنولوجيا: تعد التكنولوجيا ضرورة ملحة لمنح المنظمات والأفراد أدوات الحماية اللازمة من الهجمات السيبرانية، لذلك ينبغي حماية ثلاث كيانات رئيسية: **أجهزة الكمبيوتر، الأجهزة الذكية والراوترات.**

3- المحور الثاني: الإستراتيجية السيبرانية وحرية المواطن

1.3- حدود النظام الأمني(التوازن بين حرية المواطن والأمن) :

يظهر الأمن بوضوح في مجال عمل الأجهزة الأمنية التي تغزو المجال الخاص للمواطنين، باعتبار أن أنشطتها تتناقض مع جوهر الفكرة الحقوقية الإنسانية، وعملها يشكل خطرا نتيجة تصرفها بوسائل غير قانونية، **ما يقيد حرية المواطن، لكن بذات الوقت، ينبغي ألا نتجاهل هياكل السلطة التي تعد مكونًا مهمًا للدولة، يمكن أن يستند نشاطها إلى سيناريوهات مختلفة.**

فالديمقراطية والأمن يتفاعلان في إطار مجالين من حيث المفهوم، هما التعاون ألقسري والتعاون المتناغم، لذا لابد من حل التناقضات بين الأمن والقيم في الظروف المثالية، وعلى حساب الآليات الذاتية والتنظيم، وقد يتم ذلك بمساعدة مؤسسات المجتمع المدني والسيطرة المدنية، وإخضاع أجهزة تنفيذ القانون لسيطرة ديمقراطية عامة وحساسة، من أجل منع إساءة استخدام سلطاتها لضمان حقوق المواطن. ومن خلال دراسة تفاعل الدولة والمجتمع مع سياسة المعلومات، فأن إدخال تقنياتها الحديثة في جميع مجالات الحياة العامة، زاد بشكل كبير من اعتماد الدولة والمجتمع على كل فرد **بموثوقية البنية التحتية للمعلومات** وعلى **موثوقية المعلومات المستخدمة في أمنها**، من تعديل غير مصرح به أو من الوصول غير المشروع، **لدرجة أن بيئة المعلومات قد أصبحت واحدة من تلك المحفزات الرئيسية التي تجعل الهياكل الحكومية في حالة من التوتر بصفة مستمرة، تتوقع وتترصد المفاجآت الخارجية.** ولذلك تعمل الدول دائما على تطوير مناهج جديدة في مجال أمن المعلومات، كما أن استخدام الأدوات والحيازة السريعة، والكاملة للمعلومات يسمح للجهات الأمنية بتخطيط أعمالها، وتتبع فعالية الأنشطة التي تنفذها، **وتمنع عبرها المخاطر، وتبني علاقات فعالة مع الخصوم والشركاء، والمجتمع ليساعدها باختيار الوسائل المناسبة.**

ويترتب على كل ذلك، أن الدول والمجتمعات المهتمة **بالحفاظ على التوازن بين الحرية والأمن، هي التي تهتم أكثر برفع مستوى معرفة المواطنين في مجال تكنولوجيا المعلومات والاتصالات، وتطوير المسؤولية الاجتماعية في المجتمع، خاصة و أن الأدوات الشعبية للرقابة المدنية هي الشبكات الاجتماعية وغيرها قد أصبحت واحدة من أهم أشكال الاتصال عبر الإنترنت، باعتبارها أصبحت تشكل ثقافة جديدة في المجتمع.**

وبلا شك فأنها قد أصبحت مهيمنة على المجال السياسي وعلى النشاط الاجتماعي، كما **حولت الأفكار التقليدية للأمن إلى المساهمة في تطوير مؤسسات المجتمع المدني، والى المساهمة في تشكيل ثقافة المشاركة المدنية,** إضافة إلى أنها من الممكن أن توحد الناس في حل المشاكل المختلفة ذات الطابع المحلي على مستوى الحكم الذاتي المحلي، وحتى حل القضايا الكبرى.

أدى ظهور الشبكات الاجتماعية والعديد من منصات التواصل عبر الإنترنت إلى نشر أفكار وممارسات تتعمد الحصول على الخدمات أو الأفكار أو المعلومات الضرورية والأمنية عبره، لذلك فإن القضايا المتعلقة بالدولة والأمن الوطني، ليست فقط ذات صلة بالحروب السيبرانية، أو بضعف البنية التحتية الوطنية للمعلومات، وإنما هناك مشكلة خطيرة وحادة، تتمثل في أمن المواطن والمجتمع فيما يتعلق بمثل هذه التهديدات مثل المراقبة غير المبررة، والجمع غير القانوني للبيانات الشخصية.

لذا يتوجب حمايتها وتخزينها، وتشديد سياسة المعلومات، وبناء أسس الحماية التكنولوجية ومراقبة محتواها، وحل قضايا الأمن الوطني، والقومي الداخلي والخارجي باستخدام تكنولوجيا المعلومات الحديثة والعمل في المقام الأول في المجال الاجتماعي الثقافي، عبر استجابة المجتمع لتحديات عصر المعلومات وتجاوزه ظروف تطرف واتساع مجتمع المعلومات الشبكي، ليكون الأداة الأكثر إنتاجية لتشكيل نوع جديد من الشخصية الفردية التي تشارك بشكل واع ومسئول في حل المشكلات الأمنية الوطنية.

تشهد الدول "تباينا أو اختلافا في نهج إدارة الإنترنت أمنيا، واستخدامها لمفهوم الأمن السيبراني، يكمن اختلاف النهج في حقيقة أن التركيز يكون بين **المكون التكنولوجي والشبكات السيبرانية وسلوك المستخدمين**، وبين **فهم أوسع للمعلومات وحمايتها**، لذا يتم استخدام النهج التكنولوجي الذي تكون فيه **الأولوية لحماية المعلومات في أنظمة الكمبيوتر** و **أمن المعلومات وشبكات الاتصالات**"[19].

لذلك ترتكز الدول بشكل أساسي على إيجاد طرق للحماية من **هجمات القراصنة، ومن قراصنة الدول العدوانية والمنظمات الإرهابية.**

3.2- الإستراتيجية السيبرانية:

أولا: طبيعة الإستراتيجية السيبرانية: تنص الإستراتيجية السيبرانية وتؤكد على تحديد الهوية في الفضاء ألمعلوماتي، وعلى حاجته إلى أدوات النظام الأمني كالبنية الأساسية الحيوية، والحياة الفكرية والسماح لموضوعاتها بتبادل المعلومات، مع إمكانية تحديد هوية المستخدم بشكل موثوق به، وتحديد الهوية من خلال ضمان موثوقية تحديد هوية المستخدم، باستخدام أدوات تحديد الهوية الشخصية,

حيث شهدت الثلاث عقود الماضية، انتشارا متصاعدا لأعداد مستخدمي شبكة الانترنت والهواتف الذكية، واستخداماتها في مجالات الأعمال والتجارة والخدمات الحكومية، والتعليم والمعرفة والترفيه والسياحة، والرعاية الصحية وغيرها من الأنشطة الاقتصادية والاجتماعية والثقافية، ومع الفرص التي يمثلها النمو المستمر في أعداد مستخدمي شبكات الاتصالات والانترنت، والانتشار المتزايد في المعاملات والخدمات الالكترونية، **لذلك برزت أهمية مواجهة الإخطار، والتحديات التي تستهدف البني التحتية للاتصالات والمعلومات لأنها تهدد المعاملات والخدمات بوجه عام، وتقلص الثقة بين الخدمات والأعمال الالكترونية بوجه خاص.** ما يتطلب ضرورة وضع **إستراتيجية سيبرانية** تتضمن خطة عمل وعددا من البرامج و الأدوار، والأهداف المشتركة بين الدولة والمواطن والمؤسسات.

ولتحقيق الأمن السيبراني ينبغي أن تعتمد الإستراتيجية السيبرانية على عدد من الاجراءات:

1- توزيع الأدوار بين الجهات الحكومية والقطاع الخاص، ومؤسسات الإعمال والمجتمع المدني، وما ستقوم به الدولة من إجراءات، للتقدم نحو تحقيق الأهداف الأمنية المشتركة.

2-تقدم الإستراتيجية ملامح خطة عمل وفقا للأهداف.

3-تأكيد الشراكة المجتمعية بين الأجهزة الحكومية، و القطاع الخاص ومؤسساته، والمجتمع المدني لتنفيذ الأهداف.

4-دعم التحول نحو اقتصاد رقمي متكامل، يحقق طموحات المواطنين في تنمية اجتماعية واقتصادية شاملة، ويحمي مصالحهم، ويحافظ على مصالح الدولة العليا، ويسهم في نهضتها وازدهارها ورخاءها.

ثانيا: الإخطار السيبرانية عناصرها وسبل تفاديها:

1- الإخطار السيبرانية:

أ-خطر اختراق وتخريب البني التحتية للاتصالات وتكنولوجيا المعلومات:

لقد ظهرت أنماطا جديدة خطيرة للغاية من الهجمات السيبرانية، تستهدف إعاقة الخدمات الحيوية، وكذلك نشر برمجيات خبيثة وفيروسات لتخريب أو تعطيل البني التحتية للاتصالات وتكنولوجيا المعلومات، ونظم التحكم الصناعية الحيوية، وخاصة المرافق الهامة (منشآت الطاقة النووية والبترول والغاز الطبيعي والكهرباء والطيران والنقل بأنواعه وقواعد البيانات والمعلومات القومية والخدمات الحكومية والرعاية الصحية والإسعاف العاجل وغيرها) وذلك عبر عدة قنوات تشمل الشبكات اللاسلكية والذاكرة النقالة، بالإضافة إلى القنوات الأخرى الشائعة (البريد الالكتروني مواقع الانترنت والشبكات الاجتماعية وشبكات الاتصالات السلكية) ما يؤثر تأثيرا ملموسا على البني التحتية لتلك المنشآت والخدمات والأعمال المرتبطة بها، وقد ثبت عمليا أنها ليست بمنأى عن التعرض للهجمات السيبرانية الشرسة حتى لو كانت غير متصلة بالإنترنت.

ب-خطر سرقة الهوية الرقمية والبيانات الخاصة:

تعد سرقة الهوية الرقمية من أخطر الجرائم التي تهدد مستخدمي الانترنت ومستقبل الخدمات الكترونية. من خلال تعرض البيانات الشخصية للمستخدم إلى السرقة، بهدف انتحال شخصيته والاستيلاء على ممتلكاته أو أمواله، أو الزج باسمه في تعاملات مشبوهة أو غير قانونية. حيث يستعين سارق الهوية بمعلومات موجودة بشبكات التواصل الاجتماعي والمهني المفتوحة أو قواعد البيانات والمعلومات القومية والشبكات الخاصة بالخدمات الحكومية وخدمات الضمان الاجتماعي، وشبكات الرعاية الصحية، ومواقع التجارة الالكترونية والأسواق الافتراضية، وشبكات المدفوعات الالكترونية، والصرافات الآلية، وبورصة الأوراق المالية، فضلا عن تعرض الأدوات والأنظمة المستخدمة في إجراء المعاملات الالكترونية للسرقة أو التخريب، ما يشكل خطرا كبيرا على مصالح

المستخدمين ومستقبل الخدمات الكترونية. كما قد تتعرض البيانات الخاصة بالمؤسسات العامة والشركات للسرقة، ما يعرضها لخسائر مادية وأدبية فادحة، فضلا عن الإضرار بسمعتها وخسارتها لعملائها وأصولها الأدبية، تؤدي إلى ضرر بالاقتصاد الوطني.

ج-خطر الإرهاب والحرب السيبرانية:

أمام انتشار نوع خطير من الهجمات والجرائم السيبرانية "تعتمد على تقنيات متقدمة (الحوسبة والذكاء الاصطناعي وانترنت الأشياء) وأجهزة التصنت (السلكية واللاسلكية) و برمجيات لفك شفرة الاختراق لأنظمة الشبكات والحاسبات وقواعد البيانات، وبرمجيات لتشفير العمليات المشبوهة، وبرمجيات خبيثة لاختراق أنظمة أمن الشبكات والحاسبات، لتسخيرها في القيام بعمليات إجرامية، وتعاملات مشبوهة دون علم أصحابها"[19] حيث يمكن "أن تضم شبكة آلية واحدة عشرات أو مئات الآلاف أو ملايين من الحواسب أو الأجهزة المتصلة بالإنترنت (انترنت الأشياء) التي يمكن استخدامها لشن هجمات متنوعة، مثل الهجمات الموزعة لإعاقة الخدمات على شبكات ومواقع مستهدفة لأغراض إجرامية، كالتخريب والإرهاب والتهديد والترهيب والابتزاز.أمام هذه الهجمات الشرسة، والجرائم السيبرانية المعقدة"[20] فكان لابد من منظومة خبرات مركبة لا تتوافر إلا على مستوى الدول المتقدمة تقنيا، وذلك لأغراض إستراتيجية وحربية، يمكن لتلك الدول استخدامها إلى جانب الهجمات العسكرية التقليدية فيما يسمي بالحروب السيبرانية.

2-العناصر الرئيسية لخطورة التهديدات وسبل تفاديها:

ترجع خطورة التهديدات السيبرانية الي ثلاث عناصر رئيسية:

أ-إسنادها إلي تقنيات متقدمة ومتطورة

غالبا ما تكون تلك التقنيات حكرا على دول معدودة وشركات كبري، كما أن كثير من تلك التقنيات سرية وغير متاحة للتصدير، وقد تحتوي النسخ المتاحة منها للتصدير لاستنادهاعلى أبواب خلفية أو ثغرات تجعلها مصدرا لتهديدات أضافية.

ب- سرعة وسهولة الانتشار:

إن نشر الفيروسات الخبيثة، أو شن هجمات إعاقة الخدمات وغيرها من الأخطار السيبرانية يمكن أن يحدث بسرعة فائقة، وسهولة في ظل انتشار واتساع نطاق استخدام شبكات الاتصالات وتكنولوجيا المعلومات، نظرا لسهولة شن الهجمات وبث الفيروسات عبر الحدود من أي مكان بأرخص التكاليف، خاصة وأنه يصعب أو يستحيل تعقب مصدر تلك التهديدات والأخطار في الوقت المناسب لتداركها والتغلب عليها.

ج- اتساع نطاق تأثيرها:

يتسع نطاق التهديدات وتأثيرها، سواء من حيث التأثير المباشر أو غير المباشر على البني التحتية، وما قد يتبعه من أضرار أو خسائر فادحة، وكذلك من حيث إمكانية الأضرار بمصالح

الجهات العامة والخاصة، **والتأثير على أعداد كبيرة من المواطنين بصورة مفاجئة** و في وقت قصير وعن بعد. خاصة "أن الهجمات والجرائم السيبرانية بطبيعتها تتعدي الحدود الجغرافية للدول، وعادة ما تعتمد على شبكات الجريمة المنظمة بشقيها التقليدي والتقني. لذا يجب أن تشمل مواجهة تلك الهجمات والجرائم الآليات التقليدية للتعاون الدولي لمكافحة الجرائم، بالإضافة إلى أطر تشريعية وتنظيمية، وآليات خاصة للتعامل مع المستحدثات التقنية المرتبطة بها"[21].

فالمواجهة الفاعلة للهجمات والجرائم السيبرانية تستلزم التعاون والتنسيق على المستوي الوطني، بين شركاء إتاحة وتشغيل البني التحتية في القطاعات الحيوية، وشركاء تقديم الخدمات من الجهات الحكومية والمؤسسات والشركات، بالإضافة إلى التعاون والتنسيق على المستويين الدولي والإقليمي مع المنظمات الدولية والتجمعات الإقليمية والمنتديات العالمية المهنية والتخصصية.

ثالثا: الإطار التنظيمي والتنفيذي لتفادي التهديدات والمخاطر:

لتفادي التهديدات والمخاطر لابد من وضع إطار تنظيمي، من خلال **إنشاء منظومة وطنية لحماية أمن الفضاء، وتأمين البني التحتية للاتصالات وتكنولوجيا المعلومات، ونظم وقواعد البيانات والمعلومات القومية وبوابات الخدمات الحكومية، والمواقع الحكومية على الانترنت،** وذلك "بإعداد وتفعيل ما يعرف بفرق الاستعداد، والاستجابة لطوارئ الحاسبات والشبكات، تكون هذه الفرق مسئولة عن أعمال المتابعة الأمنية لشبكات الاتصالات، والمعلومات الوطنية للقطاعات الحيوية والحواسب المتصلة بها، وعن التعامل مع أية أخطار سيبرانية تهددها أو هجمات سيبرانية توجه إليها، وعن التوعية والإعداد لمواجهتها"[22].

كما ينبغي تشجيع ودعم وتنمية البحث العلمي والتطوير، ودعم التعاون بين الجهات البحثية والشركات الوطنية "خاصة في مجال تحليل البرمجيات الخبيثة المتقدمة، ومجال تحليل الأدلة الرقمية، وفي مجال حماية وتأمين نظم التحكم الصناعية، ومجال تطوير أجهزة وأنظمة تأمين النظم والشبكات، ومجال التشفير والتوقيع الالكتروني، ومجال حماية البني التحتية للاتصالات وتكنولوجيا المعلومات، ومجال تأمين الحواسب الحسابية، وحماية قواعد البيانات الكبرى، ومجال تقنيات الذكاء الاصطناعي، وانترنت الأشياء"[23].

كما ينبغي تنمية الكوادر البشرية والخبرات اللازمة لتفعيل منظومة الأمن السيبراني في مختلف القطاعات، بالتعاون والشراكة مع القطاع الخاص والجامعات ومؤسسات المجتمع المدني.

كما ينبغي التعاون مع الدول الصديقة والمنظمات الدولية والإقليمية ذات الصلة، ليشمل تبادل الخبرات، وتنسيق المواقف في مجال أمن الفضاء السيبراني، ومكافحة الجرائم السيبرانية حيث أن تلك الجرائم لا تعترف بالحدود الجغرافية أو السياسية.

كما ينبغي وضع وتنفيذ خطط وحملات للتوعية المجتمعية بالفرص والمزايا التي تقدمها الخدمات الالكترونية المؤمنة للأفراد والمؤسسات.

و **ينبغي أخيرا التركيز على أهمية الأمن السيبراني** الذي يهدف إلى حماية تلك الخدمات من المخاطر والتحديات التي قد تواجهها الدولة، **فضلا عن حماية خصوصية المواطن، وإطلاق برامج لحماية أمن الأطفال من مخاطر الانترنت.**

4.2- القطاعات المستهدفة والبرامج:

أولا: القطاعات المستهدفة

1-قطاع الاتصالات وتكنولوجيا المعلومات:

يشمل قطاع الاتصالات وتكنولوجيا المعلومات شبكات الاتصالات السلكية واللاسلكية، والكوابل البحرية والأرضية، وأبراج الاتصالات، وشركات تقديم خدمات الاتصالات والأقمار الصناعية للاتصالات، ومراكز التحكم والانترنت

2-قطاع الخدمات المالية:

يضم قطاع الخدمات المالية شبكات ومواقع البنوك، وشبكات ومواقع تقديم المعاملات المصرفية، وشبكات الدفع الالكتروني، وشبكات ومواقع البورصة، وشركات تداول الأوراق المالية وشبكات الخدمات المالية والبريدية.

3-قطاع الطاقة:

يضم قطاع الطاقة نظم وشبكات ومحطات التحكم في إنتاج وتوزيع الكهرباء والبترول والغاز ومحطات السدود ومحطات الطاقة النووية وغيرها من الطاقات.

4-قطاع الخدمات الحكومية:

يشمل قطاع الخدمات الحكومية بوابة ومواقع الحكومة الالكترونية، ومواقع الجهات والمؤسسات الحكومية، وقواعد البيانات والمعلومات القومية، وأهمها قاعدة بيانات الرقم القومي والشبكات والمواقع المتصلة بها.

5-قطاع النقل والمواصلات:

يشمل قطاع النقل مواصلات النقل البري والبحري والجوي، ويضم كافة نظم ومراكز وشبكات التحكم في القطارات والمترو والمرور، ونظم التحكم في الملاحة الجوية والبحرية.

6-قطاع الإعلام والثقافة:

يشمل قطاع الإعلام والثقافة شبكات ونظم ومواقع الخدمات الإعلامية والبث، بالإضافة إلى المواقع الرسمية للدولة والقطاعات ذات التأثير على النشاط الاقتصادي، مثل الاستثمار والسياحة والتجارة والصناعة والزراعة والري، والتعليم بمختلف مستوياته.

ثانيا: أهم البرامج الاستراتيجية":

1- برنامج لتطوير الإطار التشريعي الملائم لأمن الفضاء السيبراني، ومكافحة الجرائم السيبرانية، وحماية الخصوصية وحماية الهوية الرقمية:

تعد هذه البرامج بمشاركة من الإطراف المعنيين، وهم **ذوي الخبرة** في القطاع الحكومي والخاص والأكاديمي، **ومؤسسات المجتمع المدني**، مع الاسترشاد **بالخبرات والتجارب والبرامج الدولية** ذات الصلة، والعمل **بالاتفاقية الإفريقية** لأمن الفضاء السيبراني التي أقرها مؤخرا مجلس الاتحاد الإفريقي. حيث أن "وجود أي فراغ تشريعي بشأن الجرائم السيبرانية قد يضر ضررا بالغا بمنظومة المعاملات الإلكترونية والخدمات الالكترونية"[24].

فلا شك أن "مبدأ **شرعية الجرائم والعقوبات** " يشكل أحد أهم المبادئ الراسخة والذي يقضى بأنه " لا جريمة ولا عقوبة إلا بنص يستوجب عدم إمكانية التوسع في تطبيق النصوص العقابية، وتجريم أفعال لم تتناولها التشريعات القائمة، أو تتعرض لها بعقوبة مناسبة"[25] ومن ثم يجب على الدول ملاحقة هذا التطور بصياغة قواعد تشريعية جديدة وملائمة لمواجهة تلك الجرائم المعاصرة التي تهدد اعتبارات الثقة والأمان في المعاملات الإلكترونية التي تكتسب أهمية كبرى يوماً بعد يوم.

2- برنامج تطوير منظومة وطنية متكاملة لحماية أمن الفضاء السيبراني وتأمين البني التحتية للاتصالات وتكنولوجيا المعلومات:

تعتمد برنامج تطوير منظومة وطنية متكاملة لحماية أمن الفضاء السيبراني وتأمين البني التحتية للاتصالات وتكنولوجيا المعلومات على إعداد وتفعيل ما يعرف بفرق الاستجابة لطوارئ الحواسب، وفرق مواجهة حوادث أمن الحواسب في القطاعات الحيوية علي المستوي الوطني، وذلك انطلاقا من التجربة الرائدة في قطاع الاتصالات وتكنولوجيا المعلومات. تكون هذه الفرق مسئولة عن أعمال المتابعة الأمنية لشبكات الاتصالات والمعلومات الوطنية والحواسب المتصلة بها، وعن التعامل مع أية أخطار سيبرانية تهددها أو هجمات سيبرانية توجه إليها، وعن التوعية والأعداد لمواجهتها.

3 -برنامج لحماية الهوية الرقمية (برنامج المواطنة الرقمية)، وتفعيل البني التحتية اللازمة لدعم الثقة في التعاملات الالكترونية بوجه عام وفي الخدمات الحكومية الالكترونية بوجه خاص:

برنامج حماية الهوية الرقمية، تعتمد مثلا على بنية المفتاح المعلن التي يعتمد عليها التوقيع الالكتروني، وتنظمها وتشرف عليها هيئة تنمية صناعة تكنولوجيا المعلومات، وتشمل مركز السلطة الجذرية للتصديق الالكتروني بالهيئة، والسلطة الحكومية للتصديق الالكتروني بوزارة المالية، وشركات مرخص لها من الهيئة لتقديم خدمات التوقيع الالكتروني.

يعتمد البرنامج **على تشكيل لجنة عليا للمواطنة الرقمية تقوم بإعداد رؤية استراتيجية (على المستوي القومي) للمواطنة الرقمية**، ووضع خطة عمل لتحويل مفهوم المواطنة الرقمية إلي واقع ملموس، وإطلاق مشروعات قومية تستهدف تطبيقات موسعة، تسهم في تيسير وتأمين التعاملات الالكترونية، اعتمادا على البنية التحتية التي تم إنشاءها.

4-برنامج لدعم البحث العلمي والتطوير وتنمية صناعة الأمن السيبراني

برنامج لدعم البحث العلمي والتطوير وتنمية صناعة الأمن السيبراني، يهتم بدعم برامج ومشروعات التعاون بين الجهات البحثية والشركات الوطنية، خاصة في مجال تحليل البرمجيات الخبيثة المتقدمة ومجال تحليل الأدلة الرقمية، وفي مجال حماية وتأمين نظم التحكم الصناعية، ومجال تطوير أجهزة وأنظمة تأمين النظم والشبكات، ومجال التشفير والتوقيع الالكتروني، ومجال حماية البني التحتية للاتصالات وتكنولوجيا المعلومات، ومجال تأمين الحواسب الحسابية وحماية قواعد البيانات الكبرى ومجال تقنيات الذكاء الاصطناعي وانترنت الأشياء.

كما ينبغي كأولية قصوى إنشاء مراكز أو معامل وطنية لاعتماد الأنظمة والأجهزة والبرمجيات والتطبيقات المستخدمة في الجهات الحيوية وفي البني التحتية الهامة.

5- ببرنامج للتوعية المجتمعية بالفرص والمزايا التي تقدمها الخدمات الالكترونية للأفراد والمؤسسات والجهات الحكومية، وبأهمية الأمن السيبراني لحماية تلك الخدمات من المخاطر والتحديات التي قد تواجهها، على أن تشمل احتفاليات وحملات سنوية موسعة علي مستوي الوطن، والمؤتمرات والندوات، وورش العمل النوعية في مختلف القطاعات وأن تخاطب مختلف المستويات، بدءا من المستوي القيادي وحتي الأطفال وطلاب المدارس والجامعات والمواطن البسيط. و ينبغي إصدار ونشر تقارير دورية للتوعية بأهم الإخطار السيبرانية وآليات مواجهتها وبالجهود التي تبذل والأنشطة ذات الصلة بمجال الأمن السيبراني.

الخاتمة:

الخلاصة التي يمكن أن نخرج بها من الدارسة، هي أن واجب المواطنة لا يتلخص في التنظيم الذاتي للمواطن ليتحدد فقط في الاحتجاج والدفاع عن حقوقه **بل يتم التعبير عنها أيضا عن طريق رفع مستوى التعليم الذاتي في مجال تكنولوجيا المعلومات**, كما أن المشاركة النشطة للمواطن والهيئات الحكومية والمنظمات العامة – في نظام ضمان الأمن الوطني والقومي- تساهم في توفير أمن أكثر فعالية على جميع المستويات، ولهذا فأن الثقافة السياسية والإستراتيجية للمجتمع لها دور مهم في تشكيل النظام الأمني، **يترتب على هذا أن الدول والمجتمعات المهتمة بالحفاظ على التوازن بين الحرية والأمن، هي الدول التي تهتم أكثر برفع مستوى معرفة المواطن في مجال تكنولوجيا المعلومات والاتصالات، وتطوير المسؤولية الاجتماعية في المجتمع.**

وأمن المعلومات ضروري لحماية خصوصية المواطن والوطن معا، باعتبار أنه يشمل كل ما من شأنه حماية المعلومة التي قد تكون في نظام حاسوبي خاص. بمعنى آخر أمن المعلومات هو المظلة الكبرى التي تغطي كل الأفرع الأخرى المرتبطة بحماية البيانات والمعلومات وتأمينها **ضمن إستراتيجية سيبرانية.**

في هذا السياق نختم دراستنا هذه ببعض الاقتراحات المستخلصة:

-ينبغي وضع إطار تشريعي ملائم للأمن السيبراني، بمشاركة القطاع الخاص والمجتمع المدني، والاسترشاد بالخبرات الدولية، و كل المبادرات ذات الصلة.

-وضع إطار تنظيمي مناسب بالاعتماد على الخبرة الدولية والوطنية، لإنشاء نظام وطني للأمن السيبراني، ومراكز استجابة للطوارئ، وتأسيس البنية التحتية اللازمة، لضمان الثقة في المعاملات الإلكترونية وحماية الهوية الرقمية، مثل البنية التحتية للمفاتيح العامة ومكاتب الائتمان بمشاركة القطاع الخاص.

-وضع وتنفيذ برامج لبناء القدرات البشرية اللازمة لتفعيل نظام الخدمات الإلكترونية في جميع القطاعات وذلك بالتعاون مع القطاع الخاص والجامعات والمنظمات غير الحكومية. مع التعاون مع الدول الأخرى والمنظمات الدولية ذات الصلة بمجالات الأمن السيبراني والخدمات الإلكترونية والعمل على رفع الوعي العام بفوائد الخدمات الإلكترونية للأفراد والشركات والمؤسسات وبأهمية الأمن السيبراني.

-**إنشاء مركز** للاستجابة لطوارئ الإنترنت والحاسب، يكون ال**مركز** مسئولا عن الاستجابة لحوادث أمن الكمبيوتر والمعلومات، وتوفير الدعم والدفاع والتحليل في مجال الهجمات السيبرانية، والتعاون مع الهيئات الحكومية والمالية، وأي قطاعات معنية بالبنية التحتية المعلوماتية الحرجة، كما يوفر المركز أيضاً الإنذار المبكر ضد انتشار البرمجيات الخبيثة، والهجمات السيبرانية الضخمة ضد البنية التحتية للاتصالات في الجزائر.

ونقترح أن يتكون المركز من أربع إدارات رئيسية:

الإدارة الأولى: بمراقبة المخاطر والتعامل مع الحوادث السيبرانية

الإدارة الثانية: وتحليل الأدلة السيبرانية

الإدارة الثالثة: تحليل البرمجيات الخبيثة

الإدارة الرابعة: فحص الثغرات واختبارات الاختراق

هكذا يمكن للمركز أن يؤدي مهمة ناجعة من حيث للاستجابة لطوارئ الإنترنت والحاسب، حول توفير نظام للإنذار المبكر ضد البرمجيات الخبيثة، والهجمات الإلكترونية التي تنتشر بنطاق واسع ضد البنية التحتية الحيوية للمعلومات في الجزائر.

الهوامش:

1-معجم المعاني الجامع.نقلا عن ناصر إبراهيم عبد الله. المواطنة، عمان، مكتبة الرائد العلمية. 2002. ص 13

2- المرجع نفسه ص 13

3- المرجع نفسه ص 14

4-حسني هاشم محمد. المواطنة. 01 يناير 2020. الدار المصرية اللبنانية. ص 7

5-عثمان بن صالح العامر. أثر الانفتاح الثقافي على مفهوم المواطنة لدى الشباب.2013. ص 11

6-يسين السيد.المواطنة في زمن العولمة. سلسلة المواطنة. المركز القبطي للدراسات الاجتماعية، القاهرة. 2002 ص 19

7- حسني هاشم محمد. مرجع سابق. ص 10

8- يسين السيد. مرجع سابق. ص 20

9- البديوي إبراهيم بن عبد المحسن . ماهية أمن المعلومات. مجلة الأمن، العدد 51. وزارة الداخلية، الإدارة العامة للعلاقات والتوجيه.2011 . ص 22

10- البديوي إبراهيم بن عبد المحسن المرجع نفسه. ص 22

11- البديوي إبراهيم بن عبد المحسن المرجع نفسه. ص 23

12- جوستاف لندستروم "مواجهة تحدي الأمن السيبراني" أبحاث مركز جنيف للسياسات الأمنية السلسلة البحثية. رقم 7. 2012 ص 55

13- الأمن السيبراني :المخاطر المشتركة، والمسؤوليات المشتركة،طبعةI/S: مجلة القانون والسياسة لمجتمع المعلومات رقم 2 . 2012.ص 11

14- جوستاف لندستروم. مرجع سابق.ص 19

15- فردس شرير. تقرير حول الحرب السيبرانية (يتضمن مسرد مصطلحات وقائمة مراجع مختارة (مستندات رسمية، حلف الناتو، منظمة التعاون الاقتصادي والتنمية على حسب البلد،حرب معلوماتية، أمن سيبراني، كتب) 2012 . ص 6

16- جيه لويس وكيه تيملين. "الأمن السيبراني والحرب السيبرانية: التقييم الأولي للعقيدة الوطنية والتنظيم" مركز الدراسات الإستراتيجية والدولية. واشنطن2011.ص 22

17- جيه لويس وكيه تيملين. المرجع نفسه. ص 7

18- جيه لويس وكيه تيملين. المرجع نفسه. ص 7

19- الأمن السيبراني :المخاطر المشتركة. مرجع سابق.ص 12

20- المرجع نفسه. ص13

21- جوستاف لندستروم. مرجع سابق.ص 23

22- فردس شرير. . مرجع سابق.ص 29

23- المرجع نفسه. ص30

24- المرجع نفسه. ص30

25- المرجع نفسه. ص31