الأمن السيبراني (Cyper Security) في الجزائر: السياسات والمؤسسات

د. بارة سمير – جامعة قاصدي مرباح ـ ورقلة

الملخص:

في ظل التوجه الدولي نحو الحكومة الإلكترونية أصبحت قضية الأمن المعلوماتي السيبراني من التحديات الكبرى على الصعيدين الإقليمي والعالمي، لا سيما مع تزايد التهديدات الأمنية الإلكترونية، والجزائر كغيرها من الدول سعت منذ انتهاجها للإدارة الإلكترونية حماية منظومتها المعلوماتية من خلال العديد من الأجهزة والخلايا الأمنية.

لقد أصبح الأمن المعلوماتي السيبراني ركن أساسي ضمن المنظومة الأمنية المعاصرة، والتي يجب على الدفاع الوطني من خلال أجهزته كالدرك الوطني الجزائري باعتباره مسؤول أمني داخلي تحقيقه في ظل تنامي الجريمة الرقمية، وكذا نظرا للاستغلال المتنامي للشبكات الالكترونية لأهداف إجرامية، والتي تؤثر سلباً على سلامة البنى التحتية للمعلومات الوطنية الحساسة لا سيما على المعلومات الشخصية.

وعليه ما هو دور الدفاع الوطني في تحقيق الأمن السيبراني في الجزائر، أمام التحديات الوطنية والعالمية التي يفرضها الفضاء السيبراني حاليا ومستقبلا؟

من أجل معالجة هذه الإشكالية، ستحاول هذه الورقة البحثية تحليل العناصر الآتية:

1. أساسيات عن الأمن السيبراني والجريمة السيبرانية.
2. مؤسسة الدفاع الوطني وسياسات تحقيق الأمن السيبراني في الجزائر.
3. عوائق تحقيق الأمن السيبراني في ظل التحديات الآنية والمستقبلية.

Abstract:

Within the international trend toward e-Government information security has become a CYBERSPACE of the major challenges at the regional and global levels, especially with the increasing security threats to electronic commerce, Algeria, like other states have sought since it adopted the electronic administration and protection of the informatics system through many of the security organs and cells.

Information security has become a fundamental pillar within the cyber security system, which must be on national defense through his كالدرك Algerian National as an internal security official achieved in light of the growing digital divide, as well as crime and the growing exploitation of electronic networks, criminal goals, which adversely affect the integrity of the national information infrastructure, particularly on sensitive personal information.

Thus, what is the role of national defense in cyberspace security in Algeria, in front of the national and global challenges posed by CYBERSPACE of the present and the future?

مقدمة:

شهد القرن الحادي والعشرين ثورة متفردة في عالم تكنولوجيا الإعلام والاتصال، إلى الحد الذي أعد فيه بعض الخبراء والمختصين المجال المعلوماتي الإلكتروني (السيبراني) الميدان الخامس للنزاعات، بعد الأرض، البحر، الجو، والفضاء، ولربما يعود ذلك إلى درجة الانتشار والتطور السريعين لهذه التقنية، إذ لا يكاد مجال من مجالات الحياة إلا وارتكز على هذه الأخيرة، في ظل التحول نحو الخدمات الإلكترونية، التي قلصت الجهد، الوقت، والتكلفة، وساهمت بسرعتها ومرونتها في تلبية الاحتياجات، وأمام تغيير منطق الحروب حاليا إلى الاتجاه اللاتماثلي.

غير أنه وعلى الرغم من الإيجابيات التي حملتها الانترنت، إلا أنها حملت معها العديد من التهديدات والمخاطر التي تُرجمت في جرائم إلكترونية، لم تفرق بين الأشخاص والمؤسسات والدول، ناهيك عن التهديدات التي قد تطال أمن واستقرار الدول، إذ لا ينكر أحد الدور المتعاظم لشبكة الانترنت في الثورات العربية.

وتشير الإحصائيات المسجلة في الجزائر أن الجريمة الإلكترونية أخذت منحا تصاعديا في الآونة الأخيرة، وهو ما ينبأ بخطورة الوضع، لاسيما في ظل توجه الجزائر نحو تبني مقاربة الحكومة الإلكترونية، ومن هذا المنطلق فإن السلطات الجزائرية ملزمة باتخاذ الاحتياطات الأمنية اللازمة لتفادي أي نوع من الجرائم الإلكترونية.

ومن المعلوم أن الدفاع الوطني منذ الاستقلال تولى مسؤولية الدفاع عن الوطن في جميع الميادين، وتوفير الأمن بمعناه الواسع، الأمر الذي فرض عليه التعامل مع المتغيرات الحديثة والتكيف معها، بغية تحقيق هدفه الأسمى.

وفي هذا السياق جاءت هذه الورقة البحثية بإتباع منهج وصفي تحليلي، لتجيب عن الإشكالية التالية: ما هو دور الدفاع الوطني في تحقيق الأمن

السيبراني في الجزائر، أمام التحديات الوطنية والعالمية التي يفرضها الفضاء السيبراني حاليا ومستقبلا؟

أولا: أساسيات عن الأمن السيبراني والجريمة السيبرانية.

1.ماهية الأمن السيبراني:

يمكن تعريف الأمن السيبراني، انطلاقا من أهدافه، بأنه النشاط الذي يؤمن حماية الموارد البشرية، والمالية، المرتبطة بتقنيات الاتصالات والمعلومات، ويضمن إمكانات الحد من الخسائر والأضرار، التي تترتب في حال تحقق المخاطر والتهديدات، كما يتيح إعادة الوضع إلى ما كان عليه، بأسرع وقت ممكن، بحيث لا تتوقف عجلة الانتاج، وبحيث لا تتحول الأضرار إلى خسائر دائمة.

فهو النشاط أو العملية، والقدرة، أو نظم المعلومات واتصالات الدولة، حيث تكون المعلومات الواردة فيه محمية من أي دافع من التلف، والاستخدام غير المصرح به أو التعديل، أو الاستغلال.[1]

ومن الناحية العملية الإجرائية يمكن تلخيص الأمن السيبراني على أنه لا يتعدى المفاهيم التالية:

- "يتكون الأمن السيبراني إلى حد كبير من وسائل دفاعية تستخدم لكشف وإحباط المتسللين.
- "الأمن السيبراني ينطوي على حماية شبكات الكمبيوتر والمعلومات التي تحتويها من الاختراق ومن الضرر الخبيث أو التعطيل".
- "الأمن السيبراني ينطوي على الحد من هجوم المخاطر الخبيثة على البرمجيات وأجهزة الكمبيوتر والشبكات. وهذا يشمل الأدوات المستخدمة للكشف عن اقتحام ووقف الفيروسات، ومنع وصولها، وفرض التوثيق، وتمكين الاتصالات المشفرة".

- "الأمن السيبراني هو مجموعة من الأدوات والسياسات والمفاهيم الأمنية، والضمانات الأمنية، والمبادئ التوجيهية، من المخاطر المحدقة بالمعلومات ومعالجتها، والإجراءات، والتدريب، وأفضل الممارسات، وضمان التقنيات التي يمكن أن استخدامها لحماية البيئة الإلكترونية وتنظيم أصول المستخدم".

- "القدرة على الحماية أو الدفاع عن استخدام الفضاء الإلكتروني من الهجمات السيبرانية.

- "الهيئة التكنولوجيات والعمليات والممارسات وتدابير الاستجابة والتخفيف، والتي تهدف إلى حماية الشبكات وأجهزة الكمبيوتر والبرامج والبيانات من هجوم أو التلف أو الوصول غير المصرح به وذلك لضمان السرية والنزاهة وتوافر".

- "فن ضمان وجود واستمرارية مجتمع المعلومات للأمة، وضمان وحماية فضاء الإنترنت، والمعلومات الخاصة به، والأصول والبنية التحتية الحيوية.

- "حالة محمي ضد المجرم أو الاستخدام غير المصرح به للبيانات الإلكترونية، أو التدابير المتخذة لتحقيق ذلك. "

ولا شك بأن الوصول إلى تعريف يتصف بالشمولية للأمن السيبراني يستدعي منا الوقوف عند مجموعة من العناصر تعد الفاعلة والمتحكمة في تحقيقه وهي: التكنولوجيا- الأحداث – الاستراتيجيات والعمليات والأساليب – الإنسان – المرجع الأمني.

وبالتمعن في هذه العناصر نتوصل إلى أن الأمن السيبراني يجب أن يتميز بـ:

- طابع متعدد التخصصات الاجتماعية والتقنية.
- كونه شبكة خالية من الحجم، والتي قدرات الفاعلين يمكن أن تكون مماثلة على نطاق واسع.
- درجة عالية من التغيير، والترابط، وسرعة التفاعل.[2]

نخلص إلى أن الأمن السيبراني هو عبارة عن برامج وآليات تقنية، وقدرات بشرية تُفعل لمواجهة أي تعدي على المعلومات الإلكترونية بشتى أنواع الجريمة الإلكترونية.

2. ماهية الجريمة السيبرانية وأنماط التهديدات السيبرانية:

أ.تعريف الجريمة السيبرانية:

يشار إلى إساءة استخدام تكنولوجيا المعلومات والاتصالات من قبل المجرمين بالتبادل على أنها جرائم الإنترنت، أو إساءة استخدام الكمبيوتر، والجريمة المرتبطة بالحاسب الآلي، جريمة التكنولوجيا العالية، والجريمة الإلكترونية، والجريمة الإلكترونية كما عرفتها رابطة كبار ضباط الشرطة " تنطوي على "استخدام الكمبيوتر أو الإنترنت شبكات تكنولوجيا لارتكاب أو تسهيل ارتكاب الجريمة". أما المعهد الاسترالي لعلم الإجرام فيرى بأنها "تسمية عامة لجرائم ارتكبت باستخدام تخزين البيانات الإلكترونية أو جهاز الاتصالات".[3]

إن تحديد معنى جرائم الإنترنت ليست مهمة سهلة، فهي بنية واسعة للعديد من أنواع الناشئة من سوء المعاملة والجريمة الممكنة على تقنيات الاتصالات، والمعلومات. وتحتضن السلوكيات الضارة التي تحدث عبر الفضاء الإلكتروني والتي تتجاوز اختصاص الجيوسياسي، وتكتيكات تحقيق إنفاذ القانون والأساليب التقليدية.[4]

تشكل الجرائم الالكترونية تحدي كبير، للبيئة التي ترتكب فيها. إذ يمكن لمجرمي الإنترنت العمل من أي مكان في العالم، واستهداف أعداد كبيرة من الناس أو الشركات عبر الحدود الدولية، وتزداد التحديات التي تفرضها استنادا إلى نطاق وحجم الجرائم، والتعقيد التقني لتحديد هوية الجناة وكذلك ضرورة العمل على الصعيد الدولي لتقديمهم إلى العدالة. فالانترنت تفتح فرصا جديدة لمجرميها، على أساس الاعتقاد بأن إنفاذ القانون لا يعمل في عالم الانترنت [5].

ب. أنماط التهديدات السيبرانية:

يمكن أن نجمل أخطر التهديدات الالكترونية التي تواجهها الدول فيما يلي: [6]

1- تعطيل الخدمة.

2- إتلاف المعلومات أو تعديلها.

3- التجسس على الشبكات.

4- تدمير الأصول والمعلومات.

ج. أبعاد الأمن السيبراني:

- **البعد العسكري:**

لقد كانت بدايات الانترنت في بيئة عسكرية، بشكل أساسي، لتنتقل فيما بعد إلى الأوساط العلمية والأكاديمية، تمثلت في أبحاث تخدم القدرات العسكرية وتطورها، والانجازات العلمية، التي تسهم في تفوق بلد على آخر، حيث كان التنافس على أشده، بين الاتحاد السوفياتي، والولايات المتحدة الأميركية، في مجال الوصول إلى الفضاء الخارجي، وتطوير الأسلحة النووية. وتتراكم الأمثلة الموضحة لذلك، نذكر منها مثلا ما حصل في جورجيا، واستونيا، وكوريا الجنوبية، وإيران، كمثال على بعض الهجمات والاختراقات، التي ترجمت ماديا، سواء باندلاع صراع مسلح لاحق، كذلك الذي وقع، بين روسيا وجورجيا، أو بانقطاع الاتصال بالانترنت في استونيا، بين الدولة والمواطنين، والتشويش على الإدارات الحكومية.

كذلك اختراقات أنظمة المنشآت النووية، في إيران، وتحقق إمكانات التلاعب بها، مع ما يعنيه هذا من تعرض الأمن القومي، للدولة المعنية.

في هذا السياق، وجه خبراء أميركيون، خطابا مفتوحا إلى الرئيس الأميركي، جورج بوش"، في 2007، محذرين إياه، من خطر الهجمات السيبرانية على البنية التحتية الأميركية، التي تضم إلى الدفاع، إمدادات الطاقة

الكهربائية، والمياه، والاتصالات السلكية واللاسلكية، والخدمات الصحية، والنقل، والانترنت.[7]

وتكمن الميزة النسبية للقوة السيبرانية في قدرتها على ربط الوحدات العسكرية ببعضها البعض عبر الشبكات العسكرية في الفضاء الالكتروني، بما يسمح بسهولة تبادل المعلومات وتدفقها، وسرعة اتخاذ القرارات العسكرية، ومن ثمة تحقيق الأهداف عن بعدو ومن دون شك فإن عدم استغلال هذه التقنية والتسلح بها، أو تأمينها بشكل جيد من أي اختراق خارجي، سيؤدي بالضرورة إلى شن هجمات إلكترونية مضادة على شبكات القوات العسكرية، ومن ثم تدمير قواعد البيانات، وما يلحقه من مخاطر.[8]

- **البعد الاقتصادي:**

لقد أصبح الفضاء الإلكتروني جاذباً لقطاعات المجتمع كافة، وباتت المعرفة محرك الانتاج والنمو الاقتصادي، كما أيقن الجميع أن مبدأ التركيز على المعلومات والتكنولوجيا يعد عاملا من العوامل الأساسية للنهوض بالاقتصاد، وهو ما دفع بالدول في الآونة الأخيرة تزيد من استثمارها في المعرفة، وأصبحت عصرنة الاقتصاد مرتبطة بالتحكم في الاقتصاد الرقمي من طرف مختلف الفاعلين الاقتصاديين والاجتماعيين[9]. كما أن استخدام الكمبيوتر وشبكة الانترنت في تطوير الصناعات وتحريك الاقتصاد،ومعالجة كل المعاملات الاقتصادية والمالية، زاد من أهمية ضرورة توفير الأمن السيبراني لضمان حماية هذه المعلومات.

فعلى سبيل المثال،يشير تقرير صادر عن شركة Emarketer إلى أن حجما لتجارة الإلكترونية بلغ 1.5 تريليون دولار في عام 2014 بزيادة نسبتها 20% مقارنة بعام 2013 الذي بلغت فيه 1.2 تريليون دولار، ونظراً لارتفاع معدل الجرائم السيبرية المنظمة والخطيرة، فإن ذلك يمثل تهديدا صريحا لنمو الاقتصاد

الرقمي، ما لم تقم الدول بتعظيم معايير الأمن السيبراني بما يضمن الحد من هذه الجرائم [10].

- **البعد الاجتماعي:**

من الضروري تعميم المفهوم الصحيح والسليم للأمن إلى كل المشتركين في الشبكة الدولية للمعلومات، إذ تعتبر من الخطوات الأساسية التي تقوي مستوى الأمن إذا ما صيغت بطريقة واضحة وعُرفت ونفذت بذكاء، ولذلك يعتبر تنظيم الحملات الإعلامية والتثقيف المدني لأجل مجتمع معلومات مسؤول من الضرورة بمكان، بحيث تغطي التحديات والمخاطر، وتدابير الأمن والوقائية والرادعة لأجل تثقيف جميع الأفراد السيبرانيين للتعاطي مع عملية الأمن.

وينبغي التشديد على واجب الأمن، والمسؤولية الفردية والتدابير الرادعة، وكذلك التداعيات المحتملة –في إطار القانون الجنائي- التي تترتب عل عدم احترام الالتزامات التي يوجبها الأمن، وبصورة أكثر عمومية، فإن من الضروري توفير التثقيف والتدريب على تكنولوجيات المعلومات والاتصال، وليس فقط على الأمن والتدابير الرادعة. إذ يجب للثقافة الأمنية أن تغرس داخل ثقافة تكنولوجيا المعلومات.

ينبغي جعل الشبكة الدولية للمعلومات مشاعا مفتوحا للجميع بحيث يمكن لجميع المتعاملين السيبرانيين أن يستفيدوا من البنى التحتية والخدمات المتاحة لهم دون تحمل مخاطر أمنية زائدة. ويحتاج الأمر إلى بلورة مدونة أخلاقيات الأمن، تكون مقبولة ومحترمة من جانب جميع العاملين في الفضاء السيبراني. [11]

- **البعد القانوني:**

يترتب على النشاط الفردي والمؤسساتي والحكومي، في الفضاء السيبراني، نتائج قانونية، وموجبات تستدعي اهتماما خاص، لحل النزاعات التي يمكن أن تنشأ عنها. وهو ما يستدعي مواكبة التحولات التي رافقت ظهور مجتمع المعلومات. فظهرت حقوق أخرى، كحق النفاذ إلى الشبكة العالمية للمعلومات، وتوسعت بعض المفاهيم، لتشمل أساليب الممارسة الجديدة باستخدام تقنيات المعلومات والاتصالات، كالحق في إنشاء المدونات الالكترونية، والحق في إنشاء التجمعات على الانترنت، والحق في حماية ملكية البرامج المعلوماتية. كما ظهرت موجبات جديدة، ذات انعكاسات اقتصادية مثل: موجب الاحتفاظ ببيانات الاتصالات، وموجب الإبلاغ عن مخالفات وجرائم خاصة بالمحتوى.[12]

كل هذه التغيرات والتحولات تستدعي وجود ترسانة قانونية تنسجم مع التطورات الحاصلة، إن على مستوى الحقوق، أو على مستوى البيئات والعمليات.

- **البعد السياسي:**

هناك أمثلة كثيرة تدفع نحو الاهتمام بالبعد السياسي للأمن السيبراني، كالتسريبات المختلفة للوثائق الحساسة، التي تؤدي إلى مشكلات عويصة جدا، على المستوى الخارجي والدولي، كما أنه لا ينكر أحد الدور المتعاظم لشبكات التواصل الاجتماعي على المستوى السياسي (حملات انتخابية، تظاهرات افتراضية، حركات احتجاجية إلكترونية، كما يتم استغلال هذه المواقع من طرف العديد من الحكومات لتمرير سياساتها.

وفي سياق آخر يجب أن لا نغفل عن استخدام هذه المواقع من طرف الحركات الإرهابية لتجنيد أفرادها وجمع التمويل لعملياتها، وآلية للاتصال بينها كأفراد وكجماعات، وهو ما استوجب على الدول العمل على حماية أمنها من التهديدات والمخاطر التي قد تتعرض لها من خلال شبكة الانترنت.[13]

ثانيا: مؤسسة الدفاع الوطني وسياسات تحقيق الأمن السيبراني في الجزائر:

لقد وضعت قيادة الدفاع الوطني الأمن السيبراني أحد أولوياتها، على غرار باقي دول العالم التي سارعت إلى مراجعة سياساتها الأمنية، وإدراجها لآليات وميكانيزمات جديدة تعني بهذه المسائل، بالموازاة مع تطوير البنايات الأساسية المتعلقة بتكنولوجيات العالم الرقمي. ويفرض مطلب الأمن مضاعفة أنظمة الرقابة التي قد تشكل تهديدا ممكنا للحريات الفردية، ولهذا وجب مرافقة كل المقاربات الأمنية في مجال الأمن الرقمي للأطر القانونية والتكنولوجية الملائمة، وتأخذ بعين الاعتبار دقة الهجمات الالكترونية وتعقيداتها والتي يزداد خطرها مع التطور التكنولوجي واستخداماتها اليومية [14].

وتجسيدا لذلك باشرت الدولة الجزائرية وفي مقدمتها مؤسسة الدفاع الوطني إلى إعداد برامج خاصة لمجابهة الجريمة الالكترونية والحد من انتشارها، وإنشاء أجهزة جديدة تنسجم في أدوارها وتجهيزاتها مع المتغيرات الحاصلة في هذا المجال، إذ أصبحت الحماية السيبرانية جزء مهما في أي منظومة للدفاع، وقد استطاع الجيش الشعبي الوطني المضي قدما ومسايرة التطورات التكنولوجية والإعلامية الحاصلة في العالم، ومن ثمة تأمين وحماية نطاقه المعلوماتي، وتأمين الفضاء المعلوماتي لكل الناشطين فيه، وذلك من خلال التركيز على ثلاثة مرتكزات رئيسية وهي:

1. **النص القانوني:** استدرك المشرع الجزائري في السنوات الأخيرة ولو نسبيا الفراغ القانوني في مجال الجريمة الالكترونية، وذلك لما أصدر القانون 04- 15 المتضمن تعديل قانون العقوبات، حيث خصص قسمه السابع مكرر للمساس بأنظمة المعالجة الآلية للمعطيات، وتضمن ثمانية مواد، إذ تعلقت المادة 394 مكرر بمعاقبة كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك، أما المادة 394 مكرر1 فنصت على معاقبة كل من أدخل بطريق الغش معطيات في نظام

المعالجة الآلية أو أزال أو عدّل بطريق الغش المعطيات التي يتضمنها، ونصت المادة 394 مكرر2 على معاقبة كل من يقون عمدا عن طريق الغش بما يأتي:

- تصميم أو بحث أو تجميع أوتوفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مراسلة عن طريق منظومة معلوماتية يمكن أن تتركب بها الجرائم المنصوص عليها في القسم الأول. – حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان، المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم. أما المادة 394 مكرر3 فنصت على مضاعفة العقوبة المنصوص عليها في هذا القسم، إذا استهدفت الجريمة الدفاع الوطني، أو الهيئات والمؤسسات الخاضعة للقانون العام، دون الإخلال بتطبيق عقوبات أشد. وفي المادة 394 مكرر4 شدد المشرع على معاقبة الشخص المعنوي الذي يرتكب إحدى الجرائم المنصوص عليها بغرامة تعادل خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي. وجاء في المادة 394 مكرر5 أن كل من شارك في مجموعة أو إتفاق تآلف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها، وكان هذا التحضير مجسدا بفعل أو عدة أفعال مادية، يعاقب بالعقوبات المقررة للجريمة ذاتها. وأوردت المادة 394 مكرر6 على أنه مع الاحتفاظ بحقوق الغير حسن النية، يحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة مع إغلاق المواقع التي تكون محلا لجريمة من الجرائم المعاقب عليها، علاوة على إغلاق المحل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها. أما المادة 394 مكرر7 فنصت على أنه يعاقب الشروع في ارتكاب الجنح المنصوص عليها بالعقوبات المقررة للجنحة. [15]

ليصدر سنة 2009 القانون رقم:09- 04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

واستهل بالهدف الأسمى منه وهو الوقاية من الجريمة المعلوماتية، ليرصد في المادة الثانية منه المفهوم من هذا القانون من خلال توضيح ما يلي:

- **الجرائم المتصلة بتكنولوجيات الإعلام والاتصال:** وأشار إلى أنها جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية.
- **منظومة معلوماتية:** أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين.
- **معطيات معلوماتية:** أي عملية عرض للوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية، بما في ذلك البرامج المناسبة التي من شأنها جعل منظومة معلوماتية تؤدي وظيفتها.
- **مقدمو الخدمات:** أي كيان عام أو خاص يقدم لمستعملي خدماته، القدرة على الاتصال بواسطة منظومة معلوماتية و/أو نظام للاتصالات.

وأي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو لمستعمليها.

- **المعطيات المتعلقة بحركة السير**: أي معطيات متعلقة بالاتصال عن طريق منظومة معلوماتية تنتجها هذه الأخيرة باعتبارها جزء في حلقة اتصالات، توضح مصدر الاتصال، والجهة المرسل إليها، والطريق الذي يسلكه، وتاريخ وحجم ومدة الاتصال ونوع الخدمة.

- **الاتصالات الإلكترونية:** أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية.

وقد جاءت المادة الثالثة من هذا القانون لتوضح مجال تطبيقه، مما لا يدع مجالا للبس، إذ أشارت أنه مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات والاتصالات، يمكن لمقتضيات حماية النظام العام أو لمستلزمات التحريات أو التحقيقات القضائية الجارية، وفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية وفي هذا القانون، وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواه في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة المعلوماتية.

وقد بين المشرع في المادة الرابعة من هذا القانون الحالات التي يسمح بها باللجوء إلى المراقبة الإلكترونية وحددها في الآتي:

أ. للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب، أو الجرائم الماسة بأمن الدولة.

ب. في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.

ج. لمقتضيات التحريات والتحقيقات القضائية، عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية.

د. في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.

وأكد المشرع على أنه لا يمكن إجراء عمليات المراقبة في الحالات المذكورة أعلاه إلا بإذن مكتوب من السلطة القضائية المختصة، واستثنى

الحالة الواردة في الفقرة أ وخصها بإذن من النائب العام لدى مجلس قضاء الجزائر.

وأجازت المادة الخامسة من نفس القانون للمخولين قانونا الدخول بغرض التفتيش، ولو عن بعد إلى: منظومة معلوماتية أو جزء منها والمعطيات المعلوماتية المخزنة فيها، وإلى منظومة تخزين معلوماتية.

كما نصت المادة السادسة صراحة على إمكانية حجز المعطيات التي تخدم التحقيق وضرورة السهر على سلامتها، وإمكانية إعادة تشكيل هذه المعطيات قصد جعلها قابلة للاستغلال لأغراض التحقيق، شريطة أن لا يؤدي ذلك إلى المساس بمحتواها.

وأجاز المشرع في المادة السابعة في حال إستحال إجراء الحجز وفقا لما هو منصوص عليه في المادة السادسة إمكانية السلطة التي تقوم بالتفتيش إستعمال التقنيات المناسبة لمنع الوصول إلى المعطيات التي تحتويها المنظومة المعلوماتية، أو نسخها. وأوضحت المادة الثامنة إمكانية سلطة التفتيش إتخاذ الاجراءات اللازمة لمنع الاطلاع على المعطيات التي يشكل محتواها جريمة، لاسيما عن طريق تكليف أي شخص مؤهل باستعمال الوسائل التقنية المناسبة لذلك.

وقد شددت المادة التاسعة على عدم استعمال المتحصل عليها إلا في الحدود الضرورية للتحريات أو التحقيقات القضائية.

وألزمت المادة العاشرة مقدمي الخدمة بضرورة تقديم المساعدة اللازمة لجهات التحقيق، كما يتعين عليهم كتمان سرية العمليات التي ينجزونها بطلب من المحققين.

وقد تضمن الفصل الخامس من هذا القانون إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته، حيث أوضحت المادة 14 من القانون المهام الموكلة لها ولخصتها فيما يلي:

- تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته.

- مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيات الإعلام والاتصال بما في ذلك تجميع المعلومات وإنجاز الخبرات القضائية.

- تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وتحديد مكان تواجدهم.[16]

وتجسيدا لذلك صدر المرسوم الرئاسي رقم 15- 261 والذي حدد تشكيلة وتنظيم الهيئة وسير عملها.

2. **التطور التقني:** تعتبر طبيعة الجريمة الإلكترونية وانفرادها بمميزات خاصة كانعدام الحواجز الجغرافية، وصعوبة الكشف عن هوية المستخدم، من بين الدواعي التي تفترض التسلح بأحدث الوسائل التقنية للتمكن من مجابهة أخطارها، ولهذا يستلزم على الجهات المختصة بالتحقيقات في الجرائم المتصلة بالمعلوماتية، أن تمتلك الوسائل والتقنيات اللازمة لفك ألغاز الجرائم، ويمكن حصر ذلك في العناصر التالية:

- تنمية وتعزيز القدرات البشرية المكلفة بعمليات التحقيق في الجرائم الإلكترونية.
- توافر أحدث المعدات التكنولوجية في مجال الإعلام الآلي، الاتصالات اللاسلكية.
- التمتع بقاعدة بيانات واسعة محدثة باستمرار.
- القدرة على تصميم البرامج المعلوماتية وتطويرها.

لقد شكلت هذه العناصر محور إهتمام مؤسسة الدفاع الوطني من الاستقلال، واستطاعت من خلال سعيها المتواصل إلى تطوير إمكاناته وقدراته على جميع الأصعدة، ويمكن أن نلحظ ذلك بشكل جلي، في درجة الاحترافية التي يتمتع بها أفراد الدرك الوطني، واستخدامهم لوسائل وتقنيات حديثة تساعد على انجاز التحقيقات والتحريات في مجال التحقيق ففي حوادث السير مثلا يمتلك الدرك الجزائري وسائل وبرامج خاصة تساعد في إعادة تمثيل حوادث المرور بشكل دقيق ومفصل مما يسهل الخروج بتوقعات وتفسيرات تساعد المحققين في انجاز تقاريرهم.

واستطاعت وحدات الدرك الوطني من اقتناء أحدث التجهيزات والبرامج التقنية لحماية البنى التحتية المعلوماتية ضد كل المخاطر الرقمية، وتكوين أفرادها على أعلى المستويات. ويتضح ذلك في الأدوار التي تؤديها إنجازاتها، إذ يعتكف أفرادها على وضع التدابير اللازمة لمنع تسرب إمتحانات البكالوريا 2017، وضع تطبيق طريقي في الخدمة، إلى غير ذلك من الانجازات المعلوماتية

3. **الجهاز العملياتي:** ويتمثل هذا الأخير في المراكز والوحدات التي أنشئت لغرض مواجهة الجريمة الالكترونية، ومدى إستعدادتها لأدائها من ذلك والمتمثلة أساسا في:

- **مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية للدرك الوطني:** وقد أنشئ في سنة 2008 ويعتبر الجهاز الوحيد المختص بهذا الصدد في الجزائر، وهدف إلى تأمين منظومة المعلومات لخدمة الأمن العمومي، واعتبر بمثابة مركز توثيق ومقره يوجد ببئر مراد رايس، هذا المركز يعكف على تحليل معطيات وبيانات الجرائم المعلوماتية المرتكبة، وتحديد هوية أصحابها سواء كانوا أشخاص فرادى أو عصابات، وهذا كله من أجل تأمين الأنظمة المعلوماتية والحفاظ عليها، لاسيما تلك المستعملة في المؤسسات الرسمية والبنوك والبيوت. كما يهدف إلى مساعدة باقي الأجهزة الأمنية الأخرى في

أداء مهامها، واستطاعت قيادة الدرك الوطني من خلال التكوين المستمر والمتميز لأفرادها والملتقيات الدولية والوطنية وتبادل الخبرات مع دول أخرى أن توفر القوى المؤهلة وذات الكفاءة من مهندسي الإعلام الآلي، رجال قانون، وهذا من أجل الفهم الصحيح للجريمة المعلوماتية والتصدي لها. في ذات السياق، وقد استطاع المركز من معالجة أزيد من 100 جريمة إلكترونية سنة 2014، وما يفوق 500 قضية رقمية خلال سنة 2015، منها 300 جريمة تتعلق بمواقع التواصل الاجتماعي "فايسبوك"، و20 جريمة رقمية تعلقت باختراق مواقع رسمية لمؤسسات خاصة وعامة، استهدف مجرموها أنظمة المعالجة الآلية للمعطيات.

- **المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني:** مؤسسة عمومية ذات طابع إداري تحت الوصاية المباشرة لوزير الدفاع الوطني مكلفة بالمهام التالية:

- إجراء الخبرات والفحوص العلمية في إطار التحريات الأولية والتحقيقات القضائية وهذا بغرض إقامة الأدلة التي تسمح بالتعرف على مرتكبي الجنايات والجنح.
- ضمان المساعدة العلمية أثناء القيام بالتحريات المعقدة باستخدام مناهج الشرطة العلمية.
- المشاركة في الدراسات والتحاليل المتعلقة بالوقاية والتقليل من كل أشكال الإجرام.
- تصميم وانجاز بنوك المعطيات.
- المشاركة في تحديد سياسة جنائية مثلى لمكافحة الإجرام.
- المبادرة وإجراء بحوث متعلقة بالإجرام باللجوء إلى التكنولوجيات الدقيقة.
- العمل على ترقية البحوث التطبيقية وأساليب التحريات التي أثبتت فعاليتها في ميادين علمي الإجرام والأدلة الجنائية على الصعيدين الوطني والدولي.

- المشاركة في كل الملتقيات والمحاضرات والندوات على الصعيدين الوطني والدولي لتطوير مستوى مستخدمي المعهد.
- المساهمة في تنظيم دورات الإتقان والتكوين ما بعد التدرج في تخصص العلوم الجنائية.

ولتأدية مهامه على أكمل وجه فان المعهد الوطني للأدلة الجنائية وعلم الإجرام يحتوي على العديد من الأقسام والمصالح المختصة من أهمها:

- مصلحة البصمات: يتم على مستوى هذه المصلحة مقارنة البصمات للتعرف على الجثث وتجدر الإشارة إلى أن الدرك الجزائري مجهز بأنظمة التعرف الآلي على البصمات (AFIS : The Automated Fingerprint Identification System) مصلحة الوثائق: في هذه المصلحة يتم التأكد من صحة الوثائق والإمضاءات والتحقق من النقود وكذلك التأكد من صحة الوثائق السرية.

- مصلحة الإعلام الآلي: على مستوى هذه المصلحة يتم رصد و مراقبة وتتبع عمليات الاختراق والقرصنة المعلوماتية وكذا اكتشاف المعلومات المسروقة وتفكيك البرامج المعلوماتية.مصلحة البيئة: تشرف هذه المصلحة على عمليات البحث في أسباب تلوث المياه والتربة وكذا الكشف عن المواد السامة المتواجدة في المحيط أو أماكن العمل.

- **المصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة لمديرية الأمن الوطني:**

استجابة لمطلب الأمن المعلوماتي ومحاربة التهديدات الأمنية الناجمة عن الجرائم الإلكترونية قامت مصالح الأمن بإنشاء المصلحة المركزية للجريمة الإلكترونية التي عملت على تكييف التشكيل الأمني لمديرية الشرطة القضائية،والتي كانت عبارة عن فصيلة شكلت النواة الأولى لتشكيل امني خاص لمحاربة الجريمة الإلكترّونية على مستوى المديرية العامة للأمن الوطني والتي أنشئت سنة 2011، ليتم بعدها إنشاء المصلحة المركزية لمحاربة الجرائم

المتصلة بتكنولوجيات الإعلام والاتصال بقرار من المدير العام للأمن الوطني وأضيف للهيكل التنظيمي لمديرية الشرطة القضائية في جانفي 2015". [17]

جدول رقم:01 يوضح عدد القضايا المعالجة من طرف مركز الوقاية من جرائم المعلوماتية ومكافحتها

السنة	عدد القضايا المعالجة	طبيعة القضايا
2009	18	- التهديد - جرائم المساس بالنظام العام - الإرهاب - جرائم المساس بأنظمة المعالجة الآلية للمعطيات (الاختراق) - تحريض القصر على الفسق والدعارة - إهانة هيئة نظامية - إهانة رموز الدولة - النصب والاحتيال - التحرش الجنسي ضد القصر - الاعتداء على الحياة الخاصة
2010	22	
2011	24	
2012	30	
2013	46	
2014	102	
2015	240	

المصدر: عز الدين عز الدين، "الإطار القانوني للوقاية من الجرائم المعلوماتية ومكافحتها"، قيادة الدرك الوطني، **مداخلة بالملتقى الوطني حول: الجريمة المعلوماتية بين الوقاية والمكافحة.** جامعة محمد خيضر ببسكرة، 16 نوفمبر 2015، ص30.

جدول رقم 02 يوضح عدد القضايا المعالجة من طرف المديرية العامة للأمن الوطني:

السنة	عدد القضايا المعالجة	عدد الأشخاص المتورطين
2007	31	31
2008	06	10
2009	29	21
2014	245	/
2015	409	347

المصدر: حملاوي عبد الرحمان، دور المديرية العامة للأمن الوطني في مكافحة الجرائم الإلكترونية، المديرية الولائية للأمن الوطني ببسكرة، مداخلة بالملتقى الوطني حول: **الجريمة المعلوماتية بين الوقاية والمكافحة**، جامعة محمد خيضر ببسكرة، 2015/9/16، ص10.

- الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها:

تشكلت هذه الهيئة بمقتضى المرسوم الرئاسي رقم 15- 261 [18] وهي سلطة إدارية مستقلة لدى وزير العدل، تعمل تحت إشراف ومراقبة لجنة مديرة يترأسها وزير العدل وتضم أساسا أعضاء من الحكومة معنيين بالموضوع ومسؤولي مصالح الأمن وقاضيين من المحكمة العليا يعينهما المجلس الأعلى للقضاء.

وتضم الهيئة قضاة وضباط وأعوانا من الشرطة القضائية تابعين لمصالح الاستعلامات العسكرية والدرك الوطني والأمن الوطني وفقا لأحكام القانون الإجراءات الجزائية.

وكلفت الهيئة باقتراح عناصر الإستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وتنشيط وتنسيق عمليات الوقاية منها، ومساعدة السلطات القضائية ومصالح الشرطة القضائية في مجال مكافحة هذه الجرائم، من خلال جمع المعلومات والتزويد بها ومن خلال الخبرات

القضائية، وضمان المراقبة الوقائية للاتصالات الإلكترونية، قصد الكشف عن الجرائم المتعلقة بالأعمال الإرهابية والتخريبية والمساس بأمن الدولة [19].

ثالثا: عوائق تحقيق الأمن السيبراني في ظل التحديات الآنية والمستقبلية:

تواجه مصالح الدرك الوطني ومصالح الأمن الوطني العديد من العوائق والتحديات، التي تعيقها في تحقيق الأمن الإلكتروني، يمكن أن نذكر أهمها فيما يلي:

- زيادة عدد المشتركين في شبكة الإنترنت (أكثر من 10 ملايين مشترك بالجزائر): ومع زايدة عدد مستخدمي الشبكة تزداد المخاطر، لتتحول عملية اكتشاف هوية مرتكبي الجرائم الإلكترونية إلى تحدي بسبب صعوبة البحث والتحري ضمن هذا العدد الهائل والمتجه نحو الارتفاع باستمرار.
- انتشار تكنولوجيا الإنترنت فائقة السرعة والتدفقADSL/ VSAT/SDSL: تسهم التكنولوجيا المتطورة في سرعة انجاز الجريمة، وهذا يضع الجهات الأمنية المختصة أمام تحدي سرعة مباشرة التحقيقات ومتابعة الجناة، والتسلح بالأجهزة المتطورة والبرامج الحديثة السريعة الخدمة.
- التطور التكنولوجي وظهور الإنترنت اللاسلكي WIFI/3G/4G: عبر هذه التقنيات لم يعد المجرم يحتاج للجلوس وراء الحواسيب الموصولة سلكيا بشبكة الإنترنت، للقيام بجريمته، مما يستدعي من الجهات الأمنية رفع التحدي، والاستعداد بأحدث التقنيات لمواجهة والتصدي لهذه التطورات.
- الاستعمال الواسع لشبكات التواصل الاجتماعي: إذ وصل عدد مستعملي هذه المواقع في الجزائر إلى أكثر من 7 ملايين مستعمل، وهو ما ساهم بشكل كبير في ارتفاع أنواع متعددة من الجرائم الإلكترونية، مثل: القذف، التحرش الجنسي، استغلال القصر، وغيرها، وهذا ما يستوجب وضع استراتيجيات جد محكمة لضمان الأمن السيبراني عند استخدام مواقع التواصل الاجتماعي.

- عمليات التخفي أثناء استعمال خدمات شبكة الانترنت (Proxy): وهي من أكبر الإشكاليات التي تواجهها الجهات المختصة بالتحقيق، ويتطلب تعاون جهات متعددة، والتسلح بالوسائل المتطورة التي يمكن لها رصد الجزئيات وفك الشفرات، وتطوير البنى التحتية الخاصة بالمعلومات وتحديثها باستمرار، وتصميم برامج عالية التطور.[20]

- غياب التنسيق بين الدول والحكومات:إذ من المعلوم أن الجريمة الإلكترونية عابرة للحدود والقارات، وهو ما يعني أن مرتكبيها يمكنهم النفاذ إلى أنظمة الحاسوب في أحد الدول، ليتم التلاعب واختراق البيانات في بلد آخر، تسجل النتائج في بلد ثالث، ناهيك عن أنه من الممكن تخزين أدلة الجريمة الإلكترونية في حاسوب موجود في بلد آخر، غير الذي ارتكبت فيه الجريمة، وكل هذا يساعد المجرم الالكتروني في إخفاء هويته ونقل المواد من خلال قنوات موجودة في بلدان مختلفة، وبالتالي ونتيجة القدرة على التنقل إلكترونيا من شبكة إلى أخرى والنفاذ إلى قواعد البيانات في قارات مختلفة، تصبح عدة دول ومحاكم وقوانين وقواعد معنية بذلك، ما يشكل تحديا حقيقيا. ولذلك فإن المحاربة الفعالة للجريمة الإلكترونية تستدعي تعاونا دوليا متزايدا، سريعا، وفعالا، وعلى أعلى درجات التنسيق.[21]

- التطور التكنولوجي في مجال الانترنت والاتصالات: وهو ما يفرض على الأجهزة الأمنية المختصة بأن تساير هذا التطور، سواء من حيث إكتساب التكنولوجيا والتقنية أو من حيث التمكن من استخدامها واستثمارها بالشكل اللازم، وهذا قد يرهق ميزانياتها المحدودة، ولذلك يتوجب توفير جميع الامكانات المادية، المالية والبشرية اللازمة للتحقيق الأمن السيبراني.

- نشر التوعية بمفهوم الأمن السيبراني لمستخدمي شبكة الإنترنت: وهو ما يستوجب القيام بحملات توعوية بين مستخدمي شبكة الانترنت لاتخاذ التدابير اللازمة لضمان الحد الأدنى من الأمان، وتعليمهم آليات التشفير، والاحتياطات

الواجب توفيرها عند استخدام مواقع التواصل الاجتماعي، كما يجب توعيتهم بضرورة التحلي بثقافة التبليغ في الوقت اللازم لتتمكن الجهات المعنية من القيام بدورها في الوقت المناسب، والتوصل إلى مرتكبي الجرائم.

- تفعيل القوانين على أرض الواقع وتطبيقها بصرامة: إذ من بين أكبر الإشكالات التي تسهم في انتشار الجريمة الالكترونية، هو الإفلات من العقاب، والتأخر في تفعيل القوانين، وهو يمنح المجرم فرصا لتكرار جرائمه، ولذلك من الضروري تأكيد على تطبيق القوانين، كما يجب أن تتكيف النصوص القانونية مع التغيرات الحاصلة في هذا المجال، كما يتوجب إنشاء محاكم متخصصة بالجرائم الإلكترونية، نظرا للانتشار الواسع لهذه الجرائم.

الخاتمة:

إن الأطروحات الجديدة للأمن تستوجب علينا التوقف والتمعن في هذا المفهوم، بما ينسجم والتغيرات الحاصلة في العالم، لاسيما في ظل التطور الرهيب في مجال الإعلام الآلي وتكنولوجيا الاتصالات والمعلومات، إلى حد التوجه إلى إنشاء ما أصطلح على تسميته بالمدن الذكية، والتي تحولت فيها الخدمات من الشكل التقليدي إلى الإلكتروني، لتخلق بذلك ميدانا جديدا يختلف عن سابقيه، وعلى الرغم من إيجابياته إلا أنه يستلزم توفير الأمن لنجاح هذه الخدمات.

والجزائر كغيرها من الدول اتجهت نحو تبني مقاربة الحكومة الإلكترونية، وعلى الرغم من حداثة التوجه إلا أن عدد الجرائم المرتكبة، يوحي بحجم الأخطار التي تتربصها، وهو ما يجعل مؤسسة الدفاع الوطني أمام تحدي جديد، وهو تحقيق الأمن السيبراني.

وختاما، نورد بعض التوصيات، التي يتبناها المرصد العربي للسلامة والأمن في الفضاء السيبراني، وأهمها: [22]

- التزام القرارات الصادرة عن الأمم المتحدة وعن القمة العالمية لمجتمع المعلومات بشقيها، والداعية إلى نشر ثقافة الأمن السيبراني.
- اتخاذ تدابير تعتمد الأمن كعنصر ضروري في الانتاج، لاسيما ما يخص البرامج والأجهزة المستخدمة في تقنيات الاتصال.
- وضع إطار تعاون، يضمن تبادل المعلومات، ونقل الممارسات الفضلى، في المجال الأمني.
- تأمين انسجام الأنظمة القانونية، المكافحة للجرائم السيبرانية، بما يمنع نشوء جنات رقمية.
- وضع إستراتيجية لنشر الوعي، وبنائه، لدى مختلف شرائح المجتمع، سواء منهم المستخدمين العاديين، او المهنيين، أو متخذي القرار، والمسئولين عن سياسات الأمن والسلامة.
- اعتماد مبادئ خلقية للسلوك السيبراني، على مثال أخلاقيات وأصول التعامل القائمة في المجتمع التقليدي، وتكون بمثابة عقد اجتماعي، يؤسس لسلوك، يضمن سلامة الجماعة، وسلامة مواردها.
- وضع إستراتيجية، وسياسة أمنية واضحة وملزمة، لكل المعنيين بصناعة المعلومات، وبادراه وسائل الاتصالات، والبني التحتية، كما لأولئك المعنيين بصناعة أدوات وبرامج الاتصال، وخزن المعلومات ومعالجتها.
- أخذ جميع أبعاد الأمن السيبراني، بعين الاعتبار، لدى وضع أي إستراتيجية أو سياسة، بما في ذلك، حاجات المواطنين والمؤسسات، كما حقوقهم وواجباتهم، بحيث تأتي الخطة متكاملة، ومنسجمة مع ما يمكن توقع الالتزام به، من قبل المعنيين، بأمن مجتمع المعلومات.
- الإقرار بالمسؤولية عن تحقيق الأمن السيبراني، كجزء لا يتجزأ من الأمن القومي والوطني.

- إنشاء مراكز للسلامة المعلوماتية، ولطوارئ الاتصالات، تتعاون فيما بينها، وفق آلية واضحة وشفافة وفاعلة.
- تدريب وتأهيل وحدات عسكرية وأمنية خاصة، يمكنها مراقبة البنى التحتية للاتصالات، بحيث تقوم بتحديد المخاطر المحتملة، وإزالتها.
- تأهيل وحدات أمنية وعسكرية خاصة، تتولى التعاون على المستوى الخارجي، مع الهيئات العاملة على مكافحة المخاطر، والحد منها ومن آثارها.
- تأهيل الأجهزة القضائية المختصة، والشرطة القضائية، بحيث تتمكن من القيام بواجبها، في مجال ملاحقة ومحاكمة المجرمين السيبرانيين.
- تحويل الأمن السيبراني، إلى جزء من خطط التنمية والتطوير كافة.
- توجيه دعوة من خلال جامعة الدول العربية، إلى دول العالم، لمناقشة إقرار معاهدة دولية، تنطلق ديباجتها من مقررات القمة العالمية لمجتمع المعلومات، مضافا إليها، الإقرار بضرورة عدم تحويل الفضاء السيبراني إلى مجال يهدد السلم الدولي، مع الالتزام بعدد من المبادئ، وفي مقدمها: مبدأ سيادة الدول، والمساواة فيما بينها، وحق كل دولة في الإفادة من قدرات تقنيات المعلومات والاتصالات، بما يضمن قدرتها على المنافسة في هذا المجال، وتحقيق رفاه شعوبها.
- إنشاء هيئات تحكيم وطنية، متخصصة في القضايا السيبرانية، وخدمات استشارات، مسبقة ولاحقة لأي نشاط إلكتروني، يمكن لمن يرغب، اللجوء إليها.

الهوامش

[1]Douwe Korff, CYBER SECURITY DEFINITIONS – a selection. P1, in: https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CPDP%202015%20-%20KORFF%20Handout.pdf

[2]Dan Craigen, Nadia Diakun-Thibault, and Randy Purse, Defining Cybersecurity. Technology Innovation Management Review, October 2014,pp 14-15.

[3]Cameron S. D. Brown,"Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice", **International Journal of Cyber Criminology.** Vol 9, Issue 1, January – June 2015, p57.

[4]Matheus M. Hoscheidt, Elisa Felber Eichner, LEGAL AND POLITICAL MEASURES TO ADDRESS CYBERCRIME, United Nations: UFRGSMUN UFRGS Model, v.2, 2014, p 446.

[5]Home ofice, Cyber Crime Strategy, March 2010, p9, in https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/228826/7842.pdf

[6] محمد مختار، "هل يمكن أن تتجنب الدول مخاطر الهجمات الإلكترونية؟"،**مجلة اتجاهات الأحداث**. العدد: 6، يناير 2015، ص ص 5-6.

[7] منى الأشقر، "الأمن السيبري: التحديات ومستلزمات المواجهة"، اللقاء السنوي الأول للمختصين في أمن وسلامة الفضاء السيبراني، بيروت 27-28 أغسطس 2012، القاهرة: جامعة الدول العربية: المركز العربي للبحوث القانونية والقضائية، ص 15.

[8] محمد مختار، **نفس المرجع السابق**، ص6.

[9] للتوسع حول الاقتصاد الرقمي ينظر: آمال بوجليدة، الاقتصاد الرقمي: التحول من الاقتصاد الصناعي إلى اقتصاد المعلومات، **مجلة الجيش**. العدد: 630، جانفي 2016، ص ص 45-47.

[10] محمد مختار، **نفس المرجع السابق**، ص 6.

[11] الاتحاد الأوروبي للاتصالات، **دليل الأمن السيبراني للبلدان النامية**. جنيف: الاتحاد الدولي للاتصالات، 2006، ص ص: 16-17.

[12] منى الأشقر، **نفس المرجع السابق**، ص 17.

[13] محمد مختار، **نفس المرجع السابق**، ص 7.

[14] ج. رضوان، "الأمن السيبراني: أولوية في استراتيجيات الدفاع"، **مجلة الجيش**. العدد: 630، جانفي 2016، ص ص: 40-41.

[15] الجمهورية الجزائرية الديمقراطية الشعبية، قانون رقم: 04-15 المؤرخ في 10نوفمبر 2004 يعد ويتمم الأمر رقم66-156 المتضمن قانون العقوبات، **الجريدة الرسمية**. العدد:74، 2004/11/10، ص ص 11-12.

[16]الجمهورية الجزائرية الديمقراطية الشعبية، قانون رقم: 09-04 المؤرخ في 5 أوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، **الجريدة الرسمية**. العدد:47، 2009/09/16، ص ص 5-8.

[17]أنظر: http://www.essalamonline.com/ara/permalink/52564.html#ixzz4UVGdiFR1

[18]للتوسع حول الهيئة ينظر: الجمهورية الجزائرية الديمقراطية الشعبية، مرسوم رئاسي رقم:15-261 المؤرخ في8 أكتوبر 2015يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، **الجريدة الرسمية**. العدد:53، 2015/10/8، ص ص 16-20.

[19] إلهام غازي، "الوقاية ومكافحة الجريمة المعلوماتية في التشريع الجزائري"، **مجلة الجيش**. العدد:630، جانفي 2016، ص44.

[20] عزالدين عز الدين، الإطار القانوني للوقاية من الجرائم المعلوماتية ومكافحتها، **المرجع السابق**، ص ص 6-7.

[21] للتوسع ينظر: كريستينا سكولمان، "الإجراءات الوقائية والتعاون الدولي لمحاربة الجريمة الإلكترونية"، في: برنامج الأمم المتحدة، **برنامج تعزيز حكم القانون في بعض الدول العربية- مشروع تحديث النيابات العامة، أعمال الندوة الإقليمية حول: الجرائم المتصلة بالكمبيوتر**. المملكة المغربية، 19-20 يونيو 2007 ص:119.

[22] منى الأشقر، **نفس المرجع السابق**، ص ص 25-26.