رهانات الأمن السيبراني الوطني في ظل التحول الرقمي
قراءة في التأصيل المعرفي واستراتيجية المواجهة التشريعية

د. دلالي جيلالي
أستاذ محاضر «أ»

د. بلبشير يعقوب
أستاذ محاضر «ب»

كلية الحقوق والعلوم السياسية، جامعة حسيبة بن بوعلي، الشلف، الجزائر

الملخص:

يرتبط الأمن القومي للدول في الوقت الراهن بمدى أمنها وقوة دفاعاتها السيبرانية وطنياً وإقليمياً ودولياً بالقدر الذي يرتكز فيه على مدى امتلاكها لتكنولوجيا المعلومات، وقدرتها على توظيفها لحماية حدود الفضاء السيبراني الاستراتيجي؛ الأمر الذي يتطلب بالتأكيد سياسة تشريعية وأمنية شاملة ترتكز على آليات الاستباق والرّدع، والدّعم المؤسسي واللوجيستي والتنسيق البيني أو متعدد الأطراف من أجل تأسيس منظومة شاملة للأمن السيبراني.

وفي ضوء ذلك، ستتناول هذه الدراسة بالتحليل والمناقشة مدى ضرورة إعادة النظر في الاستراتيجيات الأمنية لحماية الفضاء السيبراني والأدوات القانونية والسياسية اللازمة لذلك من جهة، ومن جهة أخرى إعادة النظر في الكثير من المفاهيم التقليدية مثل: الأمن، والسيادة، والقوة، والصراع، والحرب. وتهدف هذه الدراسة إلى تحفيز إرادة الرسميين نحو تأسيس منظومة شاملة للسيبرانية في الجزائر، من خلال حزمة من الآليات التشريعية والمؤسسية لضمان مواكبة ثورة المعلومات، والإحاطة بكل مستجدات عالم السيبرانية، وفي سبيل ذلك فقد اعتمدت الدراسة على المنهج الوصفي التحليلي والمقارن.

وقد خلصت الدراسة إلى أنّ الأمن السيبراني أصبح يشكّل جزءاً أساسياً من أي سياسة أمنية وطنية، وأنّ سوء الاستغلال المتنامي للشبكات الإلكترونية لأهداف إجرامية يؤثر سلباً على سلامة البنى التحتية للمعلومات الوطنية الحساسة لاسيما على المعلومات الشخصية والبنى التحتية الأمنية الاستراتيجية، كما انتهت إلى وجود قصور قانوني وتشريعي في معالجة تطورات الجرائم السيبرانية في بعديها الأمني والاستراتيجي. وأوصت الدراسة المشرّع الجزائري بضرورة وضع منظومة وطنية شاملة لأمن الفضاء السيبراني وحمايته، وتعزيز البيئة القانونية بالأدوات اللازمة بالوقاية من الجريمة السيبرانية استباقياً، ثم بعد ذلك اعتماد آليات الردع، كما أوصت أيضاً بضرورة وضع

استراتيجية لنشر الوعي وبنائه لدى مختلف شرائح المجتمع، سواء من كان منهم من المستخدمين العاديين أو المهنيين أو متخذي القرار والمسؤولين عن سياسات الأمن والسلامة، مما يقتضي تأمين انسجام الأنظمة القانونية المكافحة للجرائم السيبرانية.

كلمات دالة: الاستراتيجية الوطنية، الأمن السيبراني، السيادة السيبرانية، الجريمة السيبرانية، المواجهة التشريعية.

المقدمة:

أولاً: موضوع الدراسة

لا شك أنّ الأمن القومي للدول والمجتمعات هو محور وغاية كل سياسة أمنية أو دفاعية، غير أنّ الرهانات والتحديات التي يطرحها هذا الهدف تبدو في غاية الأهمية والحساسية، إذا ما أخذنا في الحسبان التطور التكنولوجي والثورة الرقمية الهائلة التي جعلت من العالم قرية صغيرة، وحتّمت على الدول انتهاج سياسات أمنية ودفاعية تأخذ في الاعتبار الفضاء الافتراضي المفتوح بكل ما يحتويه من زخم، وكل ما يتعرض له من أخطار وتحديات في عالم توحدت فيه البنى التحتية المعلوماتية على المستويات الوطنية والإقليمية والدولية.

في عصر يتشكل ويُعاد تشكيله بسرعة، وتتغيّر فيه قواعد اللعب السياسية، بل وتتحوّل فيه مفاهيم الحرية والأمن والقوة والجريمة والسيادة والحروب التقليدية، ذلك أنّ العولمة والاتصالات واختراق الحدود السياسية للدولة تفرض إيجاد بنية تحتية معلوماتية كونية، تجعل مسؤولية حماية الأمن مسؤولية دولية، مما يعزّز عولمة وعالمية القوانين لحماية هذه البنية.

فبالقدر الذي تطوّرت فيه الخدمات الإلكترونية، تطوّرت المخاطر والجرائم السيبرانية، وظهرت طرق جديدة لارتكاب الجرائم على الفضاء السيبراني. ومن الضروري أنّه على المجتمع بأفراده ومؤسساته التعايش مع وجود الجرائم السيبرانية، واتخاذ التدابير اللازمة لمواجهتها، مما يفرض تعزيز الجهود الوطنية والإقليمية والدولية لمواكبة التحولات في مفهوم الأمن القومي، وسياسات الدفاع ومفاهيم الجريمة والإرهاب الإلكتروني والتجارة الإلكترونية والبحث العلمي، للتعاطي بفاعلية مع المفاهيم الحديثة للأمن السيبراني وانعكاساتها الخطيرة التي لا تقف عند حدود تهديد الأفراد والمؤسسات، بل تتعداها إلى تهديد أمن الدول والمجتمعات، مما يستدعي مقاربة شاملة ومتكاملة لجميع التحديات التي يطرحها الفضاء السيبراني، وقراءة جديدة في مفهوم السيادة الوطنية والأمن القومي الإلكتروني، وآليات قانونية واتفاقية تواكب هذا التحوّل وتحدّ من مخاطر الفضاء السيبراني المتعددة.

ثانياً: أهمية الدراسة

تظهر أهمية هذه الدراسة بل وتتزامن مع الاهتمام الرسمي الذي توليه الجزائر في إطار تأمين فضائها السيبراني من الهجمات السيبرانية التي تتعرض لها من بعض الدول من

جهة، ومن جهة أخرى ضرورة مواكبة السباق المحموم نحو استغلال مساحات الفضاء السيبراني من أجل مواجهة مخاطر هذا الفضاء المفتوح على برامج الاختراق والقرصنة وكافة أشكال التهديدات السيبرانية داخلياً وخارجياً، مما أنتج تحوّلاً كبيراً في مفهوم الأمن القومي لم تعد فيه مكانة للمفاهيم التقليدية للحرب والقوة والصراع والسيادة والأمن، تواكب ما وصلت إليه ثورة المعلومات؛ الأمر الذي يتطلب من الجزائر والدول الأقل أمناً، إلكترونياً وسيبرانياً، انتهاج استراتيجيات أمنية جديدة وتوحيد الجهود الإقليمية خاصةً والدولية لمواجهة مخاطر الفضاء السيبراني الذي لم يعد حكراً على الدول والجيوش الوطنية التقليدية، بل صار مساحة لنشاط بعض الأفراد والكيانات والمنظمات الإرهابية، مما يؤكد الحاجة الملحة اليوم إلى تغيير التكتيكات والاستراتيجيات في مجال الأمن الوطني الإلكتروني من خلال مقاربة شاملة ومتكاملة لجميع التحديات التي يطرحها الفضاء السيبراني، وقراءة جديدة في مفهوم السيادة الوطنية والأمن القومي الإلكتروني.

ثالثاً: إشكالية الدراسة

في ظل ما يشهده العالم والحدود الإقليمية للجزائر اليوم من اختلالات في موازين القوى وفي محاور الثقل الدولية وإعادة رسم خارطة القوة الدولية، يطرح السؤال التالي: هل من الضروري إعادة النظر في الاستراتيجية الأمنية والدفاعية في مجال الأمن السيبراني الوطني بما يحفظ السيادة الوطنية والأمن القومي والمصالح الاقتصادية من الأخطار المحدقة والتهديدات الإقليمية للدول والجماعات، في ظل الانتشار الواسع للجرائم السيبرانية والقرصنة؟ وما طبيعة الآليات والاستراتيجيات والأدوات القانونية والسياسية الكفيلة بضمان أمن الحدود السيبرانية الوطنية وسبل التنسيق الإقليمي والدولي؟ وما مدى فاعليتها؟

رابعاً: منهج الدراسة

اعتمدنا في هذه الدراسة على المنهج الوصفي، من خلال مناقشة الظاهرة السيبرانية وتأصيلها معرفياً وفقهياً، وبيان ارتباطاتها ببعض المفاهيم التقليدية كالأمن، والحرب، والسيادة، والقوة والصراع)، كما اعتمدنا أيضاً على المنهج التحليلي لدى مناقشة وتقييم وتحليل السياسات الأمنية والاستراتيجيات التشريعية لمواجهة الخطر السيبراني المتصاعد في ظل تحديات الواقع وتجليات المستقبل. واستخدمنا كذلك المنهج المقارن لدى مقاربة الاستراتيجية الوطنية ومقارنتها بالاستراتيجيات الإقليمية والدولية في مجال أمن الفضاء السيبراني.

خامساً: الدراسات السابقة

الأمن السيبراني مفهوم فني وقانوني وسياسي جديد، والدراسات في هذا المجال البحثي حتماً ينبغي أن تكون جديدة يمكن أن نذكر منها على سبيل المثال لا الحصر الدراسات الآتية:

- «الاستراتيجية الجزائرية في مواجهة الجرائم السيبرانية – التحديات والآفاق المستقبلية»، دراسة للدكتور جمال بوازدية، وهي منشورة في مجلة العلوم القانونية والسياسية، جامعة الوادي، الجزائر، المجلد 10، العدد 1، 2019؛ قدّم فيها الباحث رؤية تقييمية للمقاربة الجزائرية في توفير الحماية للأنظمة المعلوماتية ومواجهة الجرائم المستحدثة.
- «الدفاع الوطني والسياسات الوطنية في الجزائر: الدور والتحديات»، دراسة للدكتور بارة سمير، منشورة في المجلة الجزائرية للأمن الإنساني، جامعة باتنة1، الجزائر، المجلد 02، العدد 2، 2017، قدم فيها الباحث قراءة في الواقع والتحديات التي يطرحها تأمين الفضاء السيبراني الجزائري وآليات المواجهة المستقبلية.

في حين ستكون دراستنا مساحة لتقديم رؤية متكاملة للأبعاد السياسية والقانونية للأمن السيبراني الجزائري، وسبل مواجهة التهديدات في الفضاء السيبراني المفتوح بالارتكاز على فك رموز التداخل بين المدلولات الفقهية والمفاهيم التقليدية والحديثة لأمن المعلومات والأمن السيبراني، وتقييم الاستراتيجيات الوطنية والإقليمية والدولية.

سادساً: خطة البحث

تقوم خطة هذه الدراسة على التقسيم الثلاثي، خصصنا فيها المبحثين الأولين لاستعراض التأصيل النظري والمعرفي لبعض المفاهيم المرتبطة بالسيبرانية، وهي مفاهيم جديدة غير تقليدية يلزم الإحاطة بها خصوصاً في ظل الخلط بين مفهوم الأمن الإلكتروني وما يرتبط به من مفاهيم فنية وتكنولوجية والأمن السيبراني الذي يمكن النظر إليه من زاوية سياسية أمنية تشريعية. في حين كان المبحث الثالث عبارة عن قراءة في الجهود الوطنية والدولية لتأمين الفضاء السيبراني من خلال بعض الآليات التشريعية والمؤسسية والاتفاقية، حيث جاءت الخطة على النحو الآتي.

المبحث الأول: أمن الفضاء السيبراني.. رؤية مفاهمية وتأصيل معرفي

المبحث الثاني: تحولات مفاهيم القوة والأمن والسيادة والحرب في ظل الفضاء الرقمي المفتوح

المبحث الثالث: الاستراتيجية الوطنية والإقليمية والدولية لمواجهة المخاطر والتهديدات السيبرانية

المبحث الأول

أمن الفضاء السيبراني.. رؤية مفاهمية وتأصيل معرفي

لاشك أنّ ثورة المعلوماتية وتطور التكنولوجيا الرقمية وانتشارها عمودياً وأفقياً كأداة في أيدي الدول والمنظمات والأفراد انعكست على موازين القوى في العلاقات الدولية، وأحدثت نمطاً جديداً في مقاربات الأمن القومي تعتمد الفاعل الرقمي الذي يصف الطرق والأساليب والنماذج التي يتبعها اللاعبون الرقميون، لانتهاج الخيارات المعلوماتية في خوض سباق التفوق الدولي، ويحتم أيضاً إعادة النظر في المفاهيم التقليدية للأمن والجريمة والحرب والصراع والقوة، وهو ما سنبيّنه في هذا المبحث من خلال تفكيك رموز التداخل بين هذه المفاهيم والمفاهيم ذات الصلة، وهذا ما سنتناوله في المطلبين الآتيين:

المطلب الأول

مفهوم الفضاء السيبراني وأمن المعلومات

يتطلب التأصيل لمفهوم السيبرانية الانتقال من المفهوم الفني البحث لأمن المعلومات إلى الامتدادات التي فرضها التدرج المعرفي لهذا المفهوم كما سوف نعرضه في الفروع التالية:

الفرع الأول

تعريف الفضاء السيبراني

يمكن تعريف الفضاء السيبراني على أنّه: «عبارة عن حيز سوسيو– مكاني أنتجه الدمج بين التكنولوجيات الوسائطية والإنترنت ضمن مصفوفة تشابكية تتيح إنتاج وتبادل مختلف أشكال البيانات والمضامين النصية والسمعية البصرية والتفاعل بين المستخدمين بكيفيات محكومة بأطر الواقع الاجتماعي وأنظمته الثقافية ورموزه التداولية ومحدداته»[1]، وهو تعريف يركز على البعد الفني في تحديد طبيعة مسمى الفضاء السيبراني بالتركيز على انتفاء مفهومي الزمان والمكان، نظير البعد السوسيو– ثقافي لمستخدمي هذا الفضاء من أفراد مجتمع المعرفة المعلوماتية، ضمن حدود افتراضية لا يمكن تأمينها إلاّ من خلال تدخل تكنولوجيا المعلومات وامتلاك كافة أدوات المعرفة الرقمية.

(1) Marcelo Mendonça Teixeira, Cyberculture: From Plato to The Virtual Universe , Munich, GRIN Verlag, 2012, https://www.grin.com/document/200832.

ويمكن القول أيضاً إنّ الفضاء السيبراني مصطلح حديث ظهر نتيجة الثورة الرقمية، ويشمل جميع الحواسيب والمعلومات التي بداخلها والأنظمة والبرامج والشبكات المفتوحة لاستعمال الجمهور العام، وتلك الشبكات التي صممت لاستعمال فئة محددة من المستعملين ومنفصلة عن شبكة الإنترنت العامة[2]، أي أنّه المجال المادي وغير المادي الذي يتكون وينتج عن عناصر هي: أجهزة الكمبيوتر، الشبكات، البرمجيات، حوسبة المعلومات، المحتوى، معطيات النقل والتحكم، ومستخدمو كل هذه العناصر[3]، يعتمد في حركته على ثنائيات من الآحاد والأصفار المتناهية الصغر في تغيير حركة العالم، وهي التي تدير شبكات من ملايين النظم والبرامج والتطبيقات، وهو ما يبيّن أهمية وخطورة القدرة على امتلاك آليات توظيف هذه البيئة الإلكترونية واستغلالها وتكييفها وفق المصالح والأهداف، وبما ينعكس على الملايين من الأشخاص من المتفاعلين والمتلقين[4].

كما عرَفته الوكالة الفرنسية لأمن أنظمة الإعلام (ANSSI) وهي وكالة حكومية مُكلفة بالدفاع السيبراني الفرنسي على أنّه: «فضاء التواصل المشكّل من خلال الربط البيني العالمي لمعدات المعالجة الآلية للمعطيات الرقمية»[5]. كما عرّفه البعض الآخر أيضاً بأنّه: «عالم افتراضي يتشابك مع عالمنا المادي، يتأثر به ويؤثر فيه بشكل معقد، حيث تقوم العلاقة بين العالمين على نظرة تكاملية تحمل بين طياتها مزايا ومخاطر لا تتوقف». وهناك من وصفه بالذراع الرابعة للجيوش الحديثة إلى جوار القوات الجوية والبحرية والبرية، خاصة أنّ عالم الإنترنت شهد بداية الحديث عن معارك حقيقية تدور في هذا العالم الافتراضي[6] شكّلت نمطاً جديداً من التهديدات والمخاطر والنزاعات غير التقليدية كان لها بالغ الأثر في تغيّر مفاهيم الصراع والقوة والسيادة.

وما يمكن استنتاجه من جملة هذه التعريفات هو أنّها تدرّجت بمفهوم الفضاء السيبراني وفق تراكم معرفي انتقل من منطلقات تقنية بحتة إلى ربطه بمفاهيم عابرة للتخصص

(2) محمود محارب، إسرائيل والحرب الإلكترونية – قراءة في كتاب حرب في الفضاء الإلكتروني – اتجاهات وتأثيرات على إسرائيل، المركز العربي للأبحاث ودراسة السياسات، بيروت، 2011، ص 1.

(3) The International Télécommunication Union, ITU Toolkit for CybercrimeLégislation, Geneva, 2010, p.12.

(4) سيف نصرت الهرمزي، رصف المقاربات لمنظورات الفاعل الرقمي والانكشاف الاستراتيجي في ظل الفضاء السيبراني، مجلة آداب الفراهيدي، العدد 37، جامعة تكريت، العراق، مارس 2019، ص 427.

(5) إسماعيل قادير، إدارة الحروب النفسية في الفضاء الإلكتروني: الاستراتيجية الأمريكية الجديدة في الشرق الأوسط، أبحاث الندوة الدولية – عولمة الإعلام – السياسي وتحديات الأمن القومي للدول النامية، تاريخ الاطلاع: 2020/05/31، البحث موجود على الرابط الآتي:
https://manifest.univ-ouargla.dz/documents/Archive/2016-2017/FDSP/11-04-

(6) عباس بدران، الحرب الإلكترونية – الاشتباك في عالم المعلومات، مركز دراسات الحكومة الإلكترونية بيروت، لبنان، 2010، ص 4.

المعرفي ذات أبعاد سوسيولوجية وسياسية وأمنية، لكنه لم يبتعد كثيراً عن مفهوم الفضاء المعلوماتي خصوصاً عند رسم معالم حدود هذا الفضاء ومكوناته.

الفرع الثاني

أمن المعلومات

إنّ أمن المعلومات هو مفهوم مركب من مصطلحي الأمن والمعلوماتية، وسنحاول تفكيكه على النحو الآتي:

أولاً: الأمن

يذهب البعض[7] إلى أنّ: «الأمن يعني التطور والتنمية سواء منها الاقتصادية أو الاجتماعية أو السياسية في ظل حماية مضمونة»، واستطرد قائلاً: «إنّ الأمن الحقيقي للدولة ينبع من معرفتها العميقة بالعوامل التي تهدّد مختلف قدراتها ومواجهتها، لإعطاء الفرصة لتنمية تلك القدرات تنمية حقيقية في كافة المجالات سواء في الحاضر أو المستقبل[8]، وله أربعة مستويات: الأمن الفردي، الأمن الوطني، الأمن الإقليمي الأمن الدولي»[9].

ويرى البعض الآخر[10] بأنّ الأمن هو: «غياب التهديد بالحرمان الشديد من الرفاهية الاقتصادية»، ويعود هذا التعريف إلى مفهوم القوة والتهديد بالحرمان الشديد من الرفاهية في مفهومها المادي المحسوس، وهو الجانب الاقتصادي، مشيراً إلى أهمية القوة الاقتصادية

(7) صاحب هذا الرأي هو روبرت ماكنامارا Robert McNamara (1916-2009)، وهو مستشار للرئيس الأمريكي الأسبق جون كينيدي، يصنّف كأطول وزير دفاع من حيث الفترة (1961-1968)، اشتهر بأنّه أول من أدخل ما يسمى بتحليل النّظم في السياسة العامة، بما أصبح اليوم يسمى بتحليل السياسات، كما كان مهندس سياسة الاستراتيجية الدفاعية في الحرب الباردة تدعى (الاستجابة المرنة)، كما قام أيضاً بتوحيد مهام المخابرات واللوجيستيات داخل البنتاغون في وكالتين مركزيتين هما: وكالة استخبارات الدفاع ووكالة تأمين الدفاع، تجدر الإشارة إلى أنه شغل أيضاً منصب مدير البنك الدولي إلى غاية 1981. وكان وصياً على معهد كاليفورنيا للتكنولوجيا ومؤسسة بروكينغز.

(8) James Carroll, House of War: The Pentagon and the Disastrous Rise of American Power, Houghton Mifflin Harcourt, 2016, p.104.

(9) عبد المعطي زكي، الأمن القومي قراءة في المفهوم والأبعاد، المعهد المصري للدراسات السياسية والاستراتيجية، تاريخ الاطلاع 2020/06/13 ص1، البحث موجود على الرابط الآتي: https://eipss-eg.org/wp-content/uploads/2016/02/الأمن-القومي-قراءة-في-المفهوم-والأبعاد.

(10) صاحب هذا الرأي هو جوزاف ناي (Joseph Nye) ولد في 19 يناير 1937، أستاذ وخبير في العلوم السياسية ومؤسس مركز الدراسات الليبرالية الجديدة في العلاقات الدولية. شغل منصب مساعد وزير الدفاع الأمريكي للشؤون الأمنية الدولية في حكومة كلينتون، ورئيس مجلس الاستخبارات الوطني، وهو صاحب مصطلح (القوة الناعمة والقوة الذكية)، له عدّة مؤلفات شكلت مصدراً رئيسياً لتطوير السياسة الخارجية الأمريكية في عهد أوباما منها: مستقبل القوة ووثبة نحو القيادة: الطبيعة المتغيّرة للقوة الأمريكية.

كركيزة رئيسية للأمن الوطني. أما ج. هولسن، و ج. ويلبوك فيؤكدان بأن الأمن الوطني: «قد يأخذ شكل أهداف تسعى الدولة لتحقيقها، من خلال السياسات والبرامج، والعمل على توسيع نفوذها في الخارج، أو محاولة التأثير على سلوك الدول الأخرى أو تغييره»[11].

وما يهمنا هنا هو الأمن القومي أو الوطني للصلة الوثيقة بينه وبين الأمن السيبراني تأثراً وتأثيراً.

وقد كان تعريف الأمن القومي يتم تقليدياً على أنّه الحماية من الهجوم الخارجي، وبالتالي فقد تم النظر إليه بشكل أساسي على أنّه يعني دفاعات عسكرية في مواجهة تهديدات عسكرية. وقد ثبت أنّ هذه الرؤية ضيّقة جداً؛ فالأمن القومي يقصد به تأمين سلامة الدول ضد أخطار خارجية وداخلية قد تؤدي بها إلى الوقوع تحت سيطرة أجنبية نتيجة ضغوط خارجية أو انهيار داخلي[12]. ويعرّف ولتمان وناشت وكويستر الأمن الوطني أو القومي بأنّه: «مجموعة من التهديدات الفيزيقية (physical) والتي ربما تواجه الدولة، وتدفع بالبنى والعقائد والسياسات العسكرية للتأهب لمواجهة هذه التهديدات... وهذه عوامل داخلية وخارجية، مثل التغيّرات الاقتصادية والاجتماعية التي ربما تؤثر بطريقة مباشرة أو غير مباشرة، وتنقص أو تزيد[13] من قدرة الدولة على مواجهتها».

وعليه فإنّ الأمن القومي للدول يعني قدرة الأمة على الدفاع عن أمنها وحدودها وصيانة استقلالها وسيادتها، وتنمية القدرات والإمكانات في مختلف المجالات السياسية والاقتصادية والثقافية والاجتماعية، بالاستناد على القدرة العسكرية والدبلوماسية، آخذة في الاعتبار الاحتياجات الأمنية الوطنية لكل دولة، والإمكانات المتاحة والمتغيرات الداخلية والإقليمية والدولية، حيث إنّ الأمن القومي صار محتاجاً إلى تعزيز مجال الحماية في الفضاء السيبراني، وإلى تأمين ما يسمى بالحدود السيبرانية بعد التحوّل الكبير في مفهوم القوة والأمن والسيادة في ظل المتغيرات الدولية الراهنة.

ثانياً: المعلومات

تعرّف المعلومات بأنّها: «نتائج عمليات النماذج، التكوين، التنظيم، أو تحويل البيانات بطريقة تؤدي إلى زيادة مستوى المعرفة للمستقبل[14]. وحسب الاتفاقية العربية لحماية الفضاء السيبراني، فإنّ المعلومات هي: «مجموع البيانات، التي تسمح بمعرفة

(11) جمال منصر، تحولات في مفهوم الأمن: من أمن الوسائل إلى أمن الأهداف، مجلة دفاتر السياسة والقانون، جامعة قاصدي مرباح ورقلة، الجزائر، المجلد 1، العدد 1، جانفي/ يناير 2009، ص 4-5.

(12) غانم محمد صالح، أمن الخليج العربي، بين الاحتكار الأمريكي ورغبة المشاركة الأوروبية، مجلة العلوم السياسية، العدد 32، كلية العلوم السياسية، جامعة بغداد، جانفي/ يناير 2008، ص 52.

(13) ذياب البداينة، الأمن وحرب المعلومات، الإصدار الثاني، ط1، دار الشروق، عمان، الأردن، 2006، ص 21.

(14) سونيا محمد البكري، نظم المعلومات الإدارية – المفاهيم الأساسية، الدار الجامعية، الإسكندرية، 2000، ص 98.

معيّنة، أي كل ما ينتج عن عملية جمع البيانات وتحليلها أو معالجتها، ووضع الملاحظات والتسجيلات عليها، وكل العمليات التي تؤدي إلى التمكين من الإجابة عن بعض الأسئلة، حول هذه البيانات»[15].

أمّا المعلوماتية فيمكن تعريفها بأنّها: «حالة من تسامي قيمة المعلومات إلى المستوى الذي يجعلها واحدة من عناصر القوة المعاصرة، وهي حالة تحققت بفعل التقدم التكنولوجي الهائل في مجال إنتاج المعلومات وإيصالها وتوزيعها، ثم انتقال النشاطات البشرية من حالة التصرف السلوكي إلى حالة التصرف الإجرائي»[16]. وقد صار الأمن القومي للدول اليوم مرتبطاً ببعد جديد هو مدى حصانة منظومتها الأمنية الإلكترونية فيما يسمى بأمن المعلومات[17] أو الأمن السيبراني، وهي منظومة ترتكز على جودة وتطور النظام المعلوماتي وأمن الشبكات، حيث يشمل هذا النظام كل مكوّنات هذا الحاسب الآلي المادية (Hardware) والمعنوية (Software) وشبكات الاتصال الخاصة به (Networks)، أو مجموع عناصر مادية وغير مادية يمكن باجتماعها العمل الفوري مع المعلومة[18].

ثالثاً: أمن المعلومات

عرّفه البعض بأنّه: «مجموعة من الإجراءات والتدابير الوقائية التي تستخدم، سواء في المجال التقني أو الوقائي، للحفاظ على المعلومات والأجهزة والبرمجيات، إضافة إلى الإجراءات المتعلقة بالحفاظ على العاملين في هذا المجال»[19]، ويمكن التعبير عنه أكاديمياً بأنّه: «العلم الذي يهتم بدراسة طرائق حماية البيانات المخزونة ضمن الحاسوب وأنظمة الاتصالات والذي يتناول سبل التصدي للمحاولات الرامية إلى معرفة البيانات المخزونة ضمن الحاسوب بصورة غير مشروعة، وإلى تلك التي ترمي إلى نقل أو تغيير أو

(15) الاتفاقية العربية لحماية الفضاء السيبراني المنبثقة عن مؤتمر مجلس وزراء العرب، المنعقد في بيروت من 23 إلى 25 يوليو 2018، ص 8.

(16) محمد وائل القيسي، مستقبل الأمن الاستراتيجي العالمي في ظل التحديات التكنو– معلوماتية والفضاء السيبراني، مجلة دراسات إقليمية، العدد 44، جامعة الموصل، العراق، أفريل/ أبريل 2020، ص 152.

(17) لابد أن نشير إلى ضرورة التمييز بين المعلومات وبين التكنولوجيا وأدواتها، فالمعلومة هي ما ينتج عن معالجة البيانات والمعطيات بشكل معين تستخدم فيه التكنولوجيا، سواء للتجميع، أو للوصول، أو للتخزين والمعالجة.

(18) رشا مصطفى أبو الغيط، الحماية القانونية للكيانات المنطقية، دار الفكر الجامعي، الإسكندرية، 2003، ص 5.

(19) نجم عبد الله الحميدي، نظم المعلومات الإدارية – مدخل معاصر، ط1، دار وائل للنشر، عمان، الأردن، 2005، ص 265.

تخريب برمجيات حماية البيانات»[20]، بأي وسيلة كانت، سواء أكانت اختراقاً أم تصميماً لفيروسات، أم محاكات برامج، أم تدمير للنظم الرقمية.

ويُعد مساساً بأمن المعلومات كل فعل يهدّد أمن شبكات الحاسوب، أو النظام الرقمي الوطني، أو قواعد البيانات الخاصة، أو العامة، وهو ما يصطلح عليه بالجريمة الإلكترونية أو المعلوماتية التي يعرّفها البعض بأنّها: «أي جريمة يمكن ارتكابها بواسطة نظام حاسوبي، أو شبكة حاسوبية، أو داخل نظام حاسوبي، وتشمل تلك الجريمة من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية[21].

وهذا الاعتداء على أمن المعلومات مرتبط أساساً بمفهوم الأمن السيبراني للدول، وقد يأخذ عدة أشكال:

- الإرهاب الإلكتروني.
- الاعتداء على قواعد البيانات الخاصة أو العامة لأجهزة الحاسوب، وسائر الأجهزة الإلكترونية والشبكات الرقمية.
- الاعتداء على المؤسسات الاقتصادية والمصرفية بالمساس بسرية البيانات والمعاملات والتداولات المالية الرقمية وغير الرقمية.
- غسيل الأموال، والجريمة الإلكترونية عبر الوطنية، بالإضافة إلى الاستغلال غير المشروع للنساء والأطفال والمساس بحرمة الحياة الخاصة للأشخاص وكرامتهم واعتبارهم من خلال جرائم القذف والتشهير الإلكتروني.
- قد يأخذ أيضاً شكل حروب غير معلنة في الفضاء السيبراني بين الدول (الجوسسة، والاختراق، والتهديدات السيبرانية للنظم الدفاعية والأمنية للدول).

ومما يلاحظ على هذه التعريفات أنّها ركزت نظرياً على الجمع بين مفهومي الأمن والمعلوماتية بشكل يبدو فيه التركيز واضحاً على الجوانب الفنية والتكنولوجية المادية كعامل أساسي في ضبط المصطلح وتوظيفه معرفياً، وحتى مصطلح الجريمة الإلكترونية لم يبتعد كثيراً عن هذه الدائرة، ولعل الأمر يبقى مبرراً إذا اعتبرنا أنّ النصوص التشريعية لم تنجح في تفكيك رموز التداخل بين ما هو إلكتروني وما هو سيبراني إلاّ في حدود

(20) علاء عبد الرزاق السالمي، تكنولوجيا المعلومات، ط3، دار المناهج للتوزيع والنشر، عمان، الأردن، 2000، ص 392.

(21) حسن بن أحمد الشهري، نحو قانون دولي موحد لمكافحة الجرائم المعلوماتية، مجلة دراسات وأبحاث، جامعة زيان عاشور، الجلفة، الجزائر، المجلد 1، العدد 1، سنة 2009، ص 516.

ضيّقة، أو عندما يتعلّق الأمر بربطه بسياسات الأمن والدفاع الخارجي، وحاجتها إلى توظيف تكنولوجيا المعلومات والأدوات السيبيرية في ذلك. هذا ما ترجمته ديباجة اتفاقية بودابست لمكافحة الجريمة الإلكترونية لسنة 2001[22] التي أكدت على توسيع نطاق التعاون بين أعضاء مجلس أوروبا وغيرها من الدول في مجال مكافحة الجريمة الإلكترونية بتأكيدها على ضرورة تعزيز فعالية التحقيقات والإجراءات الجنائية المتعلقة بالجرائم ذات الصلة بنظم وبيانات الكمبيوتر، والتمكين من جمع الأدلة في الجرائم الجنائية ذات الطابع الإلكتروني.

المطلب الثاني

الأمن السيبراني والجريمة السيبرانية

دلالات المفهوم وجدلية العلاقة

أصبحت السياسات الأمنية والدفاعية للدول اليوم مرتبطة بمدى قدرتها على توظيف الفاعل الرقمي في حماية مجالها الجوي والبحري والبري والسيبراني من كل الجرائم الداخلية والاعتداءات الخارجية، مما يلزم منه تحديد مفهوم الأمن السيبراني، وماهية الجريمة السيبرانية قبل المرور إلى تأثيراتها وانعكاساتها على الأمن الوطني، والتكتيكات والاستراتيجيات الكفيلة بمواجهتها.

الفرع الأول

تعريف الأمن السيبراني

الأمن السيبراني هو عبارة عن مجموعة من الوسائل التقنية والإدارية التي يتم استخدامها لمنع الاستخدام من قبل غير المصرّح له على شبكات الكمبيوتر، أو سوء الاستغلال واستعادة المعلومات الإلكترونية التي تحتويها بهدف ضمان واستمرارية عمل نظم المعلومات، وتأمين حماية وسرية وخصوصية البيانات الخاصة بفواعل الفضاء السيبراني[23]، وعليه فهو المجال المتعلق بالإجراءات ومقاييس ومعايير الحماية

(22) اتفاقية بودابست لمكافحة الجريمة الإلكترونية، سلسلة المعاهدات الأوروبية رقم 185، مجلس أوروبا، 2001/11/ 3-2.

(23) يوسف بوغرارة، الأمن السيبراني: الاستراتيجية الجزائرية للأمن والدفاع في الفضاء السيبيري، مجلة الدراسات الإفريقية وحوض النيل، المركز الديمقراطي العربي، برلين، ألمانيا، المجلد1، العدد 3، سبتمبر 2018، ص 106.

المفروض اتخاذها، أو الالتزام بها، لمواجهة التهديدات، ومنع التعديات، أو للحد من آثارها في أقصى وأسوأ الأحوال.

وعرّفه ريشارد كومرو بأنّه: «عبارة عن وسائل دفاعية من شأنها كشف وإحباط المحاولات التي يقوم بها القراصنة»[24]. أمّا إدوارد أومورسو فعرّفه بأنّه: «وسائل من شأنها الحد من خطر الهجوم على البرمجيات أو أجهزة الحاسوب أو الشبكات، وتشمل تلك الوسائل الأدوات المستخدمة في مواجهة القرصنة وكشف الفيروسات ووقفها... إلخ»[25].

وبحسب تعريف الاتحاد الدولي للاتصالات في تقريره حول اتجاهات الإصلاح في الاتصالات للعام 2010-2011، فإنّه: «مجموعة من المهمات مثل تجميع وسائل وسياسات وإجراءات أمنية، ومبادئ توجيهية ومقاربات لإدارة المخاطر، وتدريبات وممارسات فضلى وتقنيات يمكن استخدامها لحماية البيئة السيبرانية وموجودات المؤسسات والمستخدمين»[26]، وهو المفهوم نفسه تقريباً الذي أخذت به وكالة الأمن الرقمي الأوروبية في أول تشريع أصدرته في هذا الشأن سنة 2001، فهو: «قدرة النظام المعلوماتي على مقاومة محاولات الاختراق أو الحوادث غير المتوقعة، التي تستهدف البيانات المتداولة أو المخزنة وفق إطار توافقي»[27]، تنتظم فيه الأدوات القانونية والسياسات الأمنية ووسائل الدفاع الإلكتروني لتحقيق أهداف الأمان السيبراني المنشودة وطنياً وإقليمياً ودولياً.

وما يمكن تسجيله بخصوص هذا المفهوم المستحدث في الفكر القانوني الجنائي والسياسي الأمني هو أنّ مفهوم الأمن السيبراني يضيف إلى البعد المادي والتكنولوجي لأمن المعلومات بعدين آخرين هما: بُعد قانوني يتعلق بوسائل الحماية القانونية من كل ما من شأنه أن يشكل جريمة، وبُعد سياسي يندرج في إطار السياسة الأمنية الداخلية والخارجية، وما تتطلبه من تعزيز وسائل وأدوات الدفاع من جهة، وتعاون بين الدولة والقطاع الخاص والمحيط الإقليمي من جهة أخرى.

(24) Richard A. Kemmerer, Cyber security, University of California Santa Barbara, Department of Computer Science, 2003, p.3.

(25) Edward Amoroso, Cyber Security, Silicon Press, 2007, p.1.

(26) ITU, Cyber security, Geneva: International Telecommunication Union (ITU), 2008.

(27) جمال بوازدية، الاستراتيجية الجزائرية في مواجهة الجرائم السيبرانية – التحديات والآفاق المستقبلية، مجلة العلوم القانونية والسياسية، جامعة الوادي، الجزائر، المجلد 10، العدد 1، أفريل/أبريل 2019، ص 1266.

الفرع الثاني

تعريف الجريمة السيبرانية

نظراً لحداثة النظام السيبراني واتساع نطاق الاعتماد على المعلوماتية في المجالات التقنية والاقتصادية والعسكرية والشخصية؛ فإنّه صار من الضروري وضع تعريف دقيق لكل نشاط يأخذ توصيف الجريمة ينتهك ضمن نطاق الفضاء السيبراني بكل مكوناته، وهو ما يعرف بالجرائم السيبرانية التي ما زال تحديد مفهومها وأشكالها ونطاقها محل جدل فقهي، فالجريمة السيبرانية هي: كل ما يقع على الشبكات وأنظمة تقنية المعلومات والأنظمة التشغيلية ومكوناتها (الأجهزة والبرمجيات والخدمات) من اختراق أو تعطيل أو تعديل أو استخدام أو استغلال غير مشروع[28]، ومن جهة أخرى هي: الجريمة التي يكون النظام المعلوماتي فيها وسيلة لارتكاب جريمة تقليدية، إما ضد الأموال كالتحويل الإلكتروني غير المشروع للأموال، أو ضد الأشخاص كجريمة السب أو القذف عبر الإنترنت[29].

والجدير بالذكر أنّه لا ينبغي الاكتفاء بالبعد التقني أو الفني في تعريف الجريمة السيبرانية أو الإلكترونية بالرّغم من أنّها تخضع مثل سائر الجرائم إلى مبدأ شرعية الجرائم والعقوبات، كما أنّ أبعادها لا تنحصر في البعد القانوني وحده، بل إنّ لها أبعاداً اقتصادية وسياسية وعسكرية، وهي من الجرائم العابرة للحدود التي يسهل في الغالب طمس أدلة إثباتها في الوقت الذي يصعب التحري والتحقيق فيها، كما أنّها ترتكب من قبل الأفراد والجماعات وكثيراً ما تكون مجالاً للاتفاق الجنائي والتنسيق الإجرامي الذي يتطلب بدوره تنسيقاً أمنياً وجهوداً دولية لمواجهتها تتعدى استراتيجية تعزيز الترسانة القانونية الجزائية.

والواقع أنّه يصعب التمييز بين الجريمة الإلكترونية والجريمة السيبرانية من الناحية النظرية على الأقل؛ لذلك يستخدم المفهوم الأول في الغالب لدى التطرق للجرائم السيبرانية، خصوصاً أنّه لم يتم حسم الجدل الفقهي حول تحديد تعريف ونطاق واضح لهذا المفهوم، وهذا ما يمكن فهمه من بعض الاتفاقيات الدولية التي جاءت بعنوان مكافحة الجريمة المعلوماتية، أو التشريعات الوطنية التي أسهبت في تحديد مفاهيم الأمن والجريمة الإلكترونية، مركّزة على الأبعاد التقنية والمادية والجرائم ذات الصلة.

(28) عبد العزيز بن فهد بن محمد بن داود، الجرائم السيبرانية: دراسة تأصيلية مقارنة، مجلة الاجتهاد للدراسات القانونية والاقتصادية، جامعة تمنراست، الجزائر، المجلد 9، العدد 3، سنة 2020، ص 149.

(29) نبيل إدريس، الجريمة السيبرانية بين المفاهيم والنصوص التشريعية – الجزائر أنموذجاً، مجلة القانون والمجتمع، جامعة أحمد دراية، أدرار، الجزائر، المجلد 5، العدد 2، سنة 2007، ص 30.

ومع الصعوبة والخلاف الفقهي حول تحديد مفهوم الجريمة السيبرانية، فقد اجتهدت بعض الدول في تعريفها حسماً لأي مغالطات في تفسير وتحديد أركان وأشكال ونطاق هذه الجرائم، حيث خصّص المشرع الجزائري قسماً كاملاً للجرائم المتعلقة بالمساس بأنظمة المعالجة الآلية للمعطيات في القانون رقم 04-15 المعدّل والمتمّم في قانون العقوبات[30]، حيث نصت المادة (01/02) من القانون رقم 09-04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها[31] على أنّ: «الجرائم المتصلة بتكنولوجيا الإعلام والاتصال هي 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». وما يعاب على هذا التعريف أنّه تقني بحت يركّز على المعطى المادي والفاعل الرقمي كوسيلة لارتكاب الجريمة السيبرانية، ويهمل العامل البشري والمعطيات الأخرى ذات الصلة وذات الانعكاس الاقتصادي والبعد الجيو- سياسي والأمني.

وعرّفها المشرع السعودي بأنّها: «أي فعل يرتكب متضمناً استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام»[32]. في حين عرّفها المشرع القطري بأنّها: «أي فعل ينطوي على استخدام وسيلة تقنية المعلومات أو نظام معلوماتي أو الشبكة المعلوماتية، بطريقة غير مشروعة بما يخالف أحكام القانون»[33]. أما المعهد الأسترالي لعلم الإجرام فيرى بأنّها: «تسمية عامة لجرائم ارتكبت باستخدام تخزين البيانات الإلكترونية أو جهاز الاتصالات»[34].

وعليه تعد جريمة سيبرانية كل فعل يأخذ وصف الجريمة في القانون الجزائي العام

(30) القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للأمر رقم 66-156، المؤرخ في 8 يونيو 1966، المتضمن قانون العقوبات، الجريدة الرسمية، الجزائر، العدد71، بتاريخ 10 نوفمبر 2004.

(31) القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، المؤرخ في 5 أوت/أغسطس 2009، الجريدة الرسمية، الجزائر، العدد47، بتاريخ 16 أوت/أغسطس 2009.

(32) النظام السعودي لمكافحة جرائم المعلوماتية الصادر بموجب المرسوم الملكي رقم: م/17 بتاريخ 1428/03/08هـ.

(33) القانون رقم 14 لسنة 2014، الصادر بتاريخ 2014/09/15، وللمزيد راجع أيضاً: مجمع البحوث والدراسات، أكاديمية السلطان قابوس لعلوم الشرطة، الجريمة الإلكترونية في المجتمع الخليجي وكيفية مواجهتها، البحث الفائز بمسابقة الأمير نايف بن عبد العزيز للبحوث الأمنية لسنة 2015-2016، ص 23-23.

(34) 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, p. 57.

يرتكب في الفضاء السيبراني من قبل أشخاص، أو جماعات، أو منظمات، أو دول بواسطة أجهزة الحاسوب وبرامج الإعلام الآلي وشبكة الإنترنت، أو الاعتداء عليها أو بها، مما يهدد حق الأفراد في الخصوصية وقواعد البيانات الخاصة وأنظمة المعلومات والاتصالات، وقد يأخذ بعداً آخر أمنياً وعسكرياً حينما يتعلق الأمر بأنظمة الدفاع الإلكتروني وسياسات الجوسسة، والجوسسة المضادة وبرامج التسلح.

الفرع الثالث

أشكال الجرائم والتهديدات السيبرانية

تتنوع الجرائم والتهديدات السيبرانية بتنوع الأشخاص أو الكيانات المرتكبة لها، وكذا الأدوات والأهداف، وبحسب كونها داخلية أو عابرة للحدود القطرية، نذكر منها ما يلي:

1. كل ما يعرّض الأمن القومي والعسكري والاقتصادي والاجتماعي، ويهدد البنية التحتية للدول وأسواق المال والقطاعات المصرفية، والسلم الدولي، والمنشآت النووية، والمؤسسات الصحية، وقطاعات النقل[35] بكل أنواعها، وفي هذا الصدد يمكن الإشارة إلى أضخم العمليات التي شكلت صورة من صور الاختراق والتهديد الأمني السيبراني عام 2016، والتي ما زالت تتزايد وتتنوع بفعل عدم تركيز أدوات القوة السيبرانية في أيدي الدول وحدها، حيث يشير التقرير التحليلي الصادر من طرف المخابر المختصة سنة 2016، إلى أنّ حالة انعدام فعّالية الإجراءات الأمنية، تسببت في تسجيل أكثر من 100 ألف واقعة و2260 اختراقاً في 82 دولة، وتبين أنّ 88% من الاختراقات هدفها دوافع مالية أو تجسسية، كما أعاد قراصنة (وسطاء الظل) الكرَّة سنة 2017، وأحدثوا كارثة في البرامج المستخدمة في أكثر من 100 دولة[36].

ولعل الإعصار السيبراني الذي عرفته الولايات المتحدة الأمريكية في 13 ديسمبر 2020[37] عندما اكتشفت عدة وزارات حساسة (وزارة الخزانة، وزارة التجارة،

(35) منى الأشقر جبور، الأمن السيبراني: التحديات ومستلزمات المواجهة، المركز العربي للبحوث القانونية والقضائية، جامعة الدول العربية، الندوة الأولى للمختصين في أمن وسلامة الفضاء السيبراني، بيروت، 28/27 أغسطس 2012، ص 4.

(36) جمال بوازدية، مرجع سابق، ص 1274.

(37) Ellen Nakashima and Craig Timberg, Russian Government Spies Are Behind A Broad Hacking Campaign That Has Breached U.S. Agencies And A Top Cyber Firm, National Security, Dec.13th 2020, Available at: https://web.archive.org/web/20201213220635/https://www.washingtonpost.com/national-security/russian-government-spies-are-

إدارة الاتصالات والمعلومات الوطنية) بصمات هجمات سيبرانية عندما نجح قراصنة سيبرانيون في اكتشاف الشفرة البرمجية لثلاث شركات عملاقة هي: مايكروسوفت، وسولار ويندز، وفي أم وار (Microsoft-SolarWinds-VMware)[38]، ولم يتم في هذا الصدد تحديد مدى جسامة الأضرار وحساسية البيانات التي تم اختراقها أو تدميرها.

2. المساس بسرية الاتصالات على الوسائط الإلكترونية، وسرقة البيانات الشخصية وتسريبها واستخدامها دون إذن، ودون وجه حق، وسرقة الأموال، واختراق أنظمة المعلومات، والاعتداء على الملكية الفكرية، والصناعية والعلامات التجارية.

3. الجرائم العادية التي تستخدم الإنترنت في تنفيذها، كالسرقة والغش والخداع، والتغرير بالقاصرين، وتسهيل الدعارة، والترويج لنشاطات مخالفة للقانون.

4. التلاعب بالمعلومات الموجودة في نظام معيّن، وتشويهها أو إتلافها، سواء عبر الاقتحام اليدوي، أو عبر إرسال برامج وفيروسات مخصصة بذلك.

5. إتلاف المعطيات والبيانات المخزّنة الرقمية أو تشويهها، والتجسس على الشبكات، بالإضافة إلى تدمير الأصول والمعلومات[39] بواسطة الأنظمة الخبيثة والفيروسية بأهداف إجرامية أو إرهابية.

6. كافة التهديدات السيبرانية بما في ذلك قرصنة النضال الرقمي والحرمان من الخدمة وجريمة التجسس والتخريب والتدمير والهجمات الاستراتيجية من خلال الفيروسات التي تدمر المكوّن المادي مثل فيروس ستاكسنت[40]، بالإضافة إلى الهجمات التي تتعرض لها أنظمة التسلح النووي.

7. الإرهاب الإلكتروني، ويأخذ شكل التهديدات القائمة على مهاجمة أنظمة

behind-a-broad-hacking-campaign-that-has-breached-us-agencies-and-a-top-cyber-firm/2020/12/13/d5a53b88-3d7d-11eb-9453-fc36ba051781_story.html, Accessed on Dec.22nd 2020.

(38) Christopher Bing, Suspected Russian Hackers Spied on U.S. Treasury Emails – Sources, Reuters Dec. 13th 2020, https://www.reuters.com/article/us-usa-cyber-treasury-exclsuive-idUSKBN28N0PG, Accessed on Dec. 21st 2020.

(39) محمد مختار، هل يمكن أن تتجنب الدول مخاطر الهجمات الإلكترونية، مجلة اتجاهات الأحداث، مركز المستقبل للأبحاث والدراسات المتقدمة، العدد 6، جانفي/ يناير2015، ص 5-6.

(40) نسرين فوزي اللواتي، التفاعل بين الإنسان والحاسوب: التحدي الأكبر في العصر الرقمي، مجلة لغة العصر، بوابة الأهرام، القاهرة، تاريخ الاطلاع: 2020/08/14، متاح على الرابط التالي:
http://aitmag.ahram.org.eg/News/77860/

الحواسيب، بغرض الترويع أو الابتزاز أو إجبار الحكومات أو الأفراد على تحقيق أهداف سياسية أو دينية أو عقائدية[41]، وينبغي أن يكون الهجوم مدمراً وتخريبياً لتوليد الخوف، بحيث يكون مشابهاً للأفعال المادية للإرهاب.

(41) Dorothy E. Denning, Cyber terrorism, Global Dialogue, Autumn, 2000, p.1, Available at: http://palmer.wellesley.edu/~ivolic/pdf/Classes/Handouts/NumberTheoryHandouts/Cyberterror-Denning.pdf.

المبحث الثاني

تحولات مفاهيم القوة والأمن والسيادة والحرب

في ظل الفضاء الرقمي المفتوح

صار السلام السيبراني والأمن في الفضاء المعلوماتي اليوم أحد رهانات الدول في الحفاظ على أمنها القومي وضمان سيادتها الوطنية وسيطرتها على مجالها السيبراني بالشكل الذي يحقّق أكبر قدر من الحصانة للدفاعات الإلكترونية من جهة، ومن جهة أخرى يضمن لها القدرة الكافية على تطوير إمكاناتها الرقمية وتعزيز منظومتها السيبرانية حتى تكون رقماً أساسياً في المعادلة السيبر– أمنية وطنياً وإقليمياً ودولياً في ظل احتدام الصراعات والحروب السيبرانية، وهذا ما سيأتي بيانه في المطلبين التاليين:

المطلب الأول

الأمن السيبيري للدولة وعلاقته بالأمن القومي

في القرن الواحد والعشرين

إذا كان الأمن الإلكتروني يعنى بالحماية وغياب التهديد لقيم المجتمع الأساسية، وغياب الخوف من خطر تعرض هذه القيم للهجوم، فإنّ الفضاء السيبراني قد فرض إعادة التفكير في مفهوم الأمن، والذي يتعلّق بدرجة تمكن الدولة من أن تصبح في مأمن من خطر التعرض للهجوم، وإجراءات الحماية ضد تعرض المنشآت الحيوية والبنى التحتية للتهديد، خلال الاستخدام السيئ لتكنولوجيا الاتصال والمعلومات، كما فرض أيضاً إعادة النظر في المفاهيم التقليدية للحرب والقوة والسيادة.

الفرع الأول

الحروب السيبرانية.. حروب الجيل الخامس

تتزايد العلاقة بين الأمن السيبراني والأمن القومي كلما زاد نقل المحتوى المعلوماتي والعسكري والأمني والفكري والسياسي والاجتماعي والاقتصادي والخدمي والعلمي والبحثي إلى الفضاء السيبراني. ويمكن تعريف الحرب السيبرانية بأنّها: «التوظيف المتكامل للفواعل الرقمية والأنشطة السيبيرانية وأنشطة الحاسوب، والحرب النفسية، والخداع العسكري، وأمن العمليات، بالتنسيق مع قدرات داعمة وما يتصل بها من

إمكانية التأثير أو الإخلال بقدرات العدو»؛ ذلك أنّ الفكرة الرئيسية لفهم حرب المعلومات هي أنّ أساسها المركزي هو استخدام المعلومات والبيانات كسلاح[42].

لقد شهد العالم منذ تسعينيات القرن الماضي تحولاً واضحاً في مفاهيم القوة والسيادة والصراع والحروب، تجاوز في المفاهيم التقليدية المتمحورة حول العسكرية وأنظمة التسلح والردع إلى مفاهيم أقل تكلفة مادية، وأكثر فتكاً وفاعلية وتأثيراً في موازين القوى الإقليمية والدولية، وهو ما يعرف بحروب الجيل الخامس التي قامت على أنقاض المفاهيم التقليدية للحروب العسكرية، والثورات، والحرب الباردة، والحروب الأهلية، وحروب العصابات، والانقلابات العسكرية والثورات السلمية، حتى أصبح خبراء الاستراتيجية الأمنية والعسكرية يصنفون الدفاعات السيبرانية بأنّها ذراع رابعة لمنظومة الدفاع الوطني إلى جانب القوات البرية والبحرية والجوية.

إنّ الحرب السيبرانية مفهوم معاصر جرى تداوله حديثاً منذ عام 1993 في مؤلف بعنوان: (حرب الإنترنت قادمة) من قبل الباحث الاستراتيجي جون أركيلا الذي عد فيها حرب الإنترنت، شكلاً من أشكال الحروب التي يتم بواسطتها تعطيل أو حتى تدمير المعلومات ونظم الاتصالات، وفي خضم التطور الكبير في تكنولوجيا المعلومات والاستخدام الواسع لخدمات الإنترنت في كل مفاصل الدول ومؤسساتها، رجّح احتمال اللجوء إلى هذا النمط من أنماط الحروب المستقبلية[43]، فهي بمثابة حرب لا تناظرية بحساب التكلفة المتدنية نسبياً للأدوات اللازمة لشنّها، تتصف بالسرعة والمرونة والمراوغة، وفي بيئة مماثلة يتمتع فيها المهاجم بأفضلية على المدافع[44]، وهي تجسّد قمة التطور الذي بلغته ثورة المعلومات وبوابتها الحاسبة الإلكترونية التي تشكّل بدورها الأداة المحورية لهذا النوع من الحروب والميدان الرئيسي لها، وهي دائماً عرضة للتطور المستمر والتنوع والابتكار في تقنياتها ووسائلها لارتباطها الرأسي بقمتي الهرم التقني للحضارة الإنسانية، والمصالح الحيوية للدول[45].

(42) Kenneth V. Peifer, Ananalysis of unclassified current And Pending Air Force Information Warfare And Information Operations Doctrine And Policy, A Master Thesis, Graduate School of Logistics And Acquisition Management, Air Force Institute of Technology, Kaduna, Nigeria, December 1997, pp. 32-33.

(43) سامر مؤيد عبد اللطيف، الحرب في الفضاء الرقمي رؤية مستقبلية، مجلة رسالة الحقوق، مركز الدراسات القانونية والدستورية، جامعة كربلاء، العراق، السنة السابعة، العدد 2،سنة 2015، ص 77.

(44) أشرف السعيد أحمد، القرصنة الإلكترونية، دار النهضة العربية، القاهرة، 2013، ص 45-47.

(45) علي عبد الرحمن العبودي، هاجس الحروب السيبرانية وتداعياتها على الأمن والسلم الدوليين، ص 99، تاريخ الاطلاع: 2020-08/30، متوفر على الرابط الآتي:
https://www.iasj.net/iasj/download/ea15ee56e82595de

وتجدر الإشارة إلى احتمال الخلط معرفياً بين الحروب السيبرانية ومفهوم الحرب الإلكترونية، ذلك أنّه لا يمكن توصيف النزاع السيبراني بوصف الحرب إلاّ إذا كان مقترناً بنزاع مسلح تقليدي، أمّا الحرب الإلكترونية فليست الدول وحدها أطرافاً فيها؛ لأنّ الهجمات السيبيرية قد تكون من قبل أفراد، أو منظمات، أو شبكات، أو شركات كبرى، وليست مرهونة بوجود نزاع مسلح ثنائي أو متعدد الأطراف. وغالباً ما تكون أهدافها مقترنة بأهداف اقتصادية، تشارك فيها دول كبرى على مستوى دوائر صنع القرار والشركات الضخمة، وتتداخل فيها الأهداف العسكرية بالأهداف الاقتصادية، أو ما يعرف بالتجسس الصناعي[46]، حيث تتطلب مهارات نادرة لإنتاجها، ولا تحتاج لإطلاقها سوى منصات بسيطة غير مرئية تتمثل في موقع الإطلاق على شبكة الإنترنت ومحرك للبحث، وشبكة تواصل اجتماعي، وخادم افتراضي أو مادي، أو (سحابة بيانات)، ويمكن تصميم هذه المنصات من قبل أي أشخاص مثل: القراصنة، والمتطرفين الدينيين أو السياسيين والمجرمين الإلكترونيين من عصابات الجريمة المنظمة، ولا تترك الأسلحة الإلكترونية وما تفرزه من أزمات سوى القليل من الوقت للاستباق والوقاية والكشف، أو رد الفعل بسبب السرعة الإلكترونية للهجوم[47].

وهكذا تغيّرت الحروب التقليدية، وأصبحت الجيوش العسكرية في كافة أنحاء العالم تهتم بحرب المعلومات ودورها في حروب المستقبل، فبعد أحداث 11 سبتمبر 2001 في الولايات المتحدة الأمريكية، بدأ التركيز على الفضاء السيبراني كتهديد أمني جديد، خاصة مع استخدام تنظيم القاعدة له كساحة قتال ضد الولايات المتحدة الأمريكية، وفي عامي 2007 و2008 على التوالي كان الأمن القومي لكل من إستونيا وجورجيا مهدداً من طرف روسيا، حيث استعملت هجمات الحرمان من الخدمة لتقويض العمل في الإدارات والمؤسسات الحكومية لكلتا الدولتين، وأصبح الفضاء السيبراني للدولتين مجالاً للعمليات. وفي السياق نفسه، جاء الهجوم السيبراني بفيروس (ستاكسنت) على أجهزة الطرد المركزي الإيرانية من أجل تعطيل برنامج إيران النووي، ليمثّل نقلة نوعية مهمة في تطوير واستخدام الأسلحة السيبرانية[48].

(46) سعيد درويش، الحروب السيبرانية وأثرها على حقوق الإنسان: دراسة على ضوء أحكام دليل تالين، المجلة الجزائرية للعلوم القانونية والاقتصادية والسياسية، جامعة الجزائر1، المجلد 54، العدد 5، جوان/يونيو 2018، ص 186.

(47) عبد الغفار عفيفي الدويك، الأزمات والحروب السيبرانية... تهديدات تتجاوز الفضاء الإلكتروني، تقرير ومتابعة تحليلية، مركز الأهرام للدراسات السياسية والاستراتيجية، القاهرة، 2019، ص 434. منشور على الرابط الآتي: http://acpss.ahram.org.eg/News/16843.aspx

(48) David J. Smith, How Russia Harnesses Cyber Warfare, Defense Dossier, American Foreign Policy Council, Issue 4, August 2012, Available at: http://www.insidethecoldwar.com/files/august2012.pdf.

وتجدر الإشارة إلى أنّ التحديات في الفضاء السيبراني تتطلب مواكبة التحولات الحديثة في تكنولوجيا ومفاهيم أمن المعلومات، وأدوات الصراع الإلكتروني غير المرئية، مما يستلزم إعادة النظر في فهم حقيقة مفهوم الأمن الشامل، فالسلوك البشري يعد أمراً أساسياً لأمن الفضاء الإلكتروني الفعّال من جهة[49]، ومن جهة أخرى يعد أمراً ضرورياً لفهم طبيعة السباق وأدوات الحرب وأهدافها، واتجاه موازين القوة السياسية والعسكرية والتكنولوجية إقليمياً ودولياً.

الفرع الثاني

القوة السيبرانية

لقد صار لزاماً على كل الفاعلين في الفضاء السيبراني الأخذ في الحسبان أيضاً التحوّل في مفهوم القوة، واستيعاب مفهوم القوة السيبرانية كمفهوم جديد يتجاوز الأبعاد الاقتصادية والسياسية والعسكرية التقليدية، حيث يرى جوزيف ناي أنّ القوة السيبرانية هي: «القدرة على الحصول على النتائج المرجوة من خلال استخدام مصادر المعلومات المرتبطة بالفضاء السيبراني، أي أنّها القدرة على استخدام الفضاء السيبراني لإيجاد مزايا للدولة، والتأثير على الأحداث المتعلقة بالبيئات التشغيلية الأخرى وذلك عبر أدوات سيبرانية»[50]. وحتى تكتمل عناصر القوة السيبرانية، لابد للدولة من القيام بتطوير أسلحة في مجال الحرب السيبرانية لاستعمالها سواء في العمليات الهجومية أو من أجل الردع.

والواقع أنّ استخدام مصطلح القوة السيبرانية أكثر دقة من القوة الإلكترونية التي تترجم (Electronic Power)، إذ إنّ المقصود هو (Powercyber) وهي أكثر شمولية في ما نقصده في التعاملات الدولية[51]، حيث بدأ الاهتمام بهذا الموضوع بوضع فرضيات نظرية تدرس إمكانية استخدام أو تصميم أسلحة رقمية بالاستفادة من الثورة العلمية الهائلة في مجال علم الحاسوب والإنترنت، تتفوق هذه الأسلحة على العتاد العسكري التقليدي المادي، وتكون بديلة عنه لإحداث أكبر ضرر في منشآت العدو العسكرية

(49) جون باسيت وأوستن لونج وآخرون، الحروب المستقبلية في القرن الواحد والعشرين، ط1، مركز الإمارات للدراسات والبحوث الاستراتيجية، أبو ظبي، 2014، ص 61.

(50) Joseph S. Nye JR, Cyber Power, Harvard Kennedy School, 2010, p. 03.

(51) إيهاب خليفة، القوة الإلكترونية: كيف يمكن أن تدير الدول شؤونها في عصر الإنترنت، 2017، ص 5، تاريخ الاطلاع: 2020/09/05، متاح على الرابط الآتي:
https://middle-east-online.com/%D8%A5%D9%8A%D9%87%D8%A7%D8%A8-

والمدنية، بأساليب أكثر يسراً وأقل خسائر[52]، ومن هنا تم وضع برامج متطورة تخترق بيانات الجهة المستهدفة ومعلوماتها ونشاطاتها العسكرية والتأثير على منشآتها الحيوية، وأطلق على هذا النشاط القوة السيبرانية، مما يتطلب استراتيجية شاملة في مجال الأمن السيبراني ترتكز على ثلاثة محاور هي:

1. هجمات شبكات الحاسوب، من خلال اختراق الشبكات وتغذيتها بمعلومات محرّفة لإرباك مستخدمي الشبكات أو نشر الفيروسات بهدف تعطيل الشبكة.
2. الدفاع عن شبكات الحاسب الآلي ضد أي اختراق خارجي عبر تأمينها من خلال إجراءات معينة، يقوم بها (حراس الشبكات)، من خلال برامج وتطبيقات، تقوم بأعمال المراقبة للزائرين غير المرغوبين (الهاكرز) واستيقافهم للتعرف على هوياتهم أمام بوابات افتراضية للشبكات، بجانب المسح الشامل للشبكات بحثاً عن الفيروسات السيبرانية.
3. استطلاع شبكات الحاسب الآلي، وتعني القدرة على الدخول غير المشروع والتجسس على شبكات الخصم بهدف الحصول على البيانات دون تدميرها، والتي قد تشتمل على أسرار عسكرية، ومعلومات استخباراتية، وفي بعض الحالات قد يسمح للزائر المجهول بالدخول على الشبكة، وتتبعه بهدف التعرف على أساليب الخصم والقيام بعمليات ردع سيبراني مضاد، مما يعزز المخاوف التي تبديها معظم الدول حالياً من تعرض أمنها القومي نتيجة الاعتداءات السيبرانية، لاسيما وأنّ تقنيات المعلومات والاتصالات قد رفعت منسوب الخطر، عبر إتاحتها مصادر جديدة متشعبة ومتعدّدة، وإمكانات هائلة لتحقيق هذا الخطر، مقابل انخفاض نسبة المخاطر وإمكانات الانكشاف في جانب الجهة المعتدية.

الفرع الثالث

السيادة السيبرانية

على الرّغم من محاولات الخبراء والدول والمنظمات الدولية إيجاد تعريف موحد للحرب السيبرانية، إلاّ أنّه حتى الآن لم يتم الاستقرار على تعريف عام شامل لها، فبالنسبة للولايات المتحدة والناتو، يتم التركيز على الجانبين الاقتصادي والمادي لأوجه الحرب السيبرانية، على عكس دول منظمة شنغهاي للتعاون التي تحاول الدفع بتعريف يتضمن

(52) موسى محمد آل طويرش، الصراع السيبراني: مفهومه وأثره في العلاقات الدولية، مؤتمر كلية العلوم السياسية، الجامعة المستنصرية، العراق 27 فبراير 2019، ص2، متاح على الرابط الآتي:
https://uomustansiriyah.edu.iq/media/attachments/11/11_2019_04_16!10_41_58_AM.pdf

أوجه السيادة الوطنية، والحفاظ على الحدود والهوية الثقافية للشعوب كأهداف للصراع في الفضاء السيبراني[53]، مما ينعكس بشكل مباشر على تغيّر مفهوم السيادة التقليدية الذي أصبح من الضروري إعادة النظر فيه نتيجة عدم وجود حدود إقليمية بالمفهوم الجغرافي والجيوسياسي في ظل فضاء يموج بالفاعلين الرقميين والنشاط السيبراني المحموم.

إنّ السيادة السيبرانية مفهوم يختلف عن المصطلح الأكثر شيوعاً وهو الأمن السيبراني، ففي حين أنّ شواغل هذا الأخير المتعلقة بحماية البنية التحتية والعمليات المتصلة بالإنترنت، فإنّ السيادة السيبرانية تركّز على المعلومات والمحتوى الذي توفره الإنترنت كامتداد طبيعي للسيادة الوطنية في الفضاء الإلكتروني[54]، مما يؤدي بالدول إلى خفض تدفق الإنترنت ومستوى سرعة المعلومات من أجل بسط نفوذها على مجالها السيبراني، وهو مفهوم غامض يعرف جدلاً كبيراً بين الأكاديميين وحتى السياسيين.

وبشكل عام، فإنّ مصطلح السيادة السيبرانية يستخدم غالباً للتعبير عن قوة الدولة واستقلالها في الفضاء السيبراني، وذلك لوصف أشكال مختلفة من الاستقلالية والتحكم والسيطرة على البنى التحتية الرقمية، والتقنيات والمحتويات الرقمية والاتصالات، وكافة الأشياء التي يمكن أن ترتبط بالفضاء السيبراني والتعامل معه[55]، وهذا نتيجة التحول الرقمي الكبير الذي فرض إضافة معطى جديد إلى مقومات السيادة الوطنية يرتكز على أمن البنى التحتية الرقمية وشبكات الاتصالات ومنظومة الدفاع السيبراني.

المطلب الثاني

المخاطر والتهديدات في الفضاء السيبراني

وأثرها على الأمن والسلم الدوليين

يعج الفضاء السيبراني بالعديد من المخاطر التي تعتبر في الأساس جرائم تقليدية، أسهم التحول الرقمي وتنوع الفاعلين وصعوبة الإثبات وتعدد آليات المواجهة في فداحتها، ويمكن أن نذكر منها المخاطر والتهديدات الآتية:

(53) محمد فخر الدين، حدود المجال الخامس: ما هي الحروب السيبرانية؟ مؤتمر حروب الفضاء السيبراني، 2020/9/7، البحث موجود على الرابط الآتي: https://bit.ly/3rvr1zk

(54) Jinghan Zeng and Tim Stevens and Yaru Chen, China's Solution to Global Cyber Governance: Unpacking the Domestic Discourse of "Internet Sovereignty", P&P Politics & Policy, Volume 45, Issue 3, June 2017, p. 432, Available at : https://onlinelibrary.wiley.com/doi/abs/10.1111/polp.12202.

(55) فاطمة بيرم، السيادة الوطنية في ظل الفضاء السيبراني والتحولات الرقمية: الصين أنموذجاً، المجلة الجزائرية للأمن الإنساني، جامعة باتنة 1، الحاج الأخضر، باتنة، الجزائر، المجلد 5، العدد 1، جانفي/ يناير 2020، ص 799.

الفرع الأول

التهديدات السيبرانية

لا تقتصر التهديدات والمخاطر في الفضاء السيبراني على الحروب السيبرانية والصراعات غير المرئية بين الدول سعياً منها نحو تأمين مجالها السيبراني وتعزيز منظومتها الدفاعية الرقمية، فهذا الفضاء السيبراني مجال لأشكال أخرى من التهديدات التي يرتكبها الأفراد والجماعات والمنظمات، على غرار الإرهاب السيبراني والقرصنة الإلكترونية، وهذا ما يجعل بعض الدول تقوم باستكشاف إمكانية اتباع نهج حربي تقليدي عندما يتعلّق الأمر بمناورات سيبرانية، مما يجعلها تصمّم أسلحة سيبرانية هجومية وقدرات دفاعية أيضاً، وهي تعتبر الأسلحة السيبرانية بمثابة (مضاعِفات القوة)، التي ينبغي استعمالها في المقام الأول بالاقتران مع الأعمال العسكرية الأكثر تقليدية من أجل تعزيز قدراتها الحربية بشكل كبير[56]، حيث يمكن اعتبار هذه المناورات حرباً معلوماتية وتهديداً للأمن القومي تضاهي الأعمال العسكرية، سواء أسفرت عن خسائر أم لا[57]، وبهذا الصدد فإنّ العديد من البلدان تعتبر إتلاف المعلومات على الإنترنت شكلاً من أشكال الاعتداء العسكري ضد معنويات الجمهور، ومن ثم تكون مستعدة للتصدي للتهديدات السيبرانية باستخدام القوة العسكرية[58].

الفرع الثاني

القرصنة الإلكترونية

تعد القرصنة الإلكترونية جريمة مكتملة الأركان في معظم التشريعات الجزائية، فهي ترتكب من طرف أشخاص – هواة أو محترفين – لتحقيق أهداف إجرامية، وإحداث تلف بالأجهزة والبرمجيات الرقمية الحديثة، والمساس بأمن الشبكات وسريتها، فهي عبارة عن عملية دخول غير مشروع، إلى أجهزة الغير وشبكاتهم الإلكترونية؛ أي أن تُوجّه

(56) Kevin Coleman, Russia's Cyber Forces, Available at: https://www.military.com/defensetech/2008/05/27/russias-cyber-forces.

(57) حمدون إ. توريه، الاستجابة الدولية للحرب السيبرانية: البحث عن السلام السيبراني، الاتحاد الدولي للاتصالات، يناير 2011، ص 79-80. تاريخ الزيارة: 2019/8/31، متاح على الرابط الآتي: www.itu.int › S-GEN-WFS.012011--1-MSW-A.docx

(58) Gregory Asmolov, "Russia: New Military Doctrine and Information Security":Global Voices متاح على الرابط الآتي: http://globalvoicesonline.org/2010/02/23//russian-military-doctrine تاريخ الزيارة: 23 فبراير 2010.

هجمات إلى معلومات الكمبيوتر أو خدماته، بقصد المساس بالسرية أو المساس بسلامة المحتوى والتكاملية، أو تعطيل القدرة والكفاءة للأنظمة للقيام بأعمالها[59]، ويقول محمد أمين الشوابكة بأنّها: «جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية أو داخل نظام حاسوبي، وتشمل تلك النتيجة من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية»[60]. والواقع أنّ أي محاولة لتحديد مفهوم القرصنة الإلكترونية يجب أن تأخذ في الحسبان المعطيات المتعلقة بموضوع الجريمة أو نمط السلوك محل التجريم، والوسيلة المستخدمة في ارتكابها، وكذا صفات القرصان، وهدفها.

ورغم أنّ التشريعات الجنائية سبقت في أحكامها الجزائية التقليدية عصر الإنترنت، إلاّ أنّ الكثير منها حاول تدارك الأمر، من خلال استحداث جرائم وعقوبات تواكب الثورة الرقمية، وتستهدف تجريم كل ما من شأنه المساس، أو الاعتداء على أنظمة المعلومات وقواعد البيانات، وهو ما ذهب إليه المشرع الجزائري في القانون رقم 04-15 المعدل والمتمم لقانون العقوبات، والذي تمّ بموجبه تجريم بعض الأفعال التي تتصل بالمعالجة الآلية للمعطيات، وذلك من خلال عقوبات أصلية وتكميلية، حيث جرّم فعلي الدخول والبقاء غير المشروعين للنظام المعلوماتي، وكذا المساس بالمنظومة المعلوماتية، حيث تكون العقوبة في الحالة الأولى الحبس من ثلاثة أشهر إلى سنة والغرامة من 50000 إلى 100000 دينار جزائري (المادة 394 مكرر من قانون العقوبات الجزائري)، في حين تشدّد العقوبة في حال أدى الفعل إلى حذف البيانات أو تخريب المعطيات لتصل إلى الحبس من ستة أشهر إلى سنتين، والغرامة من 50000 إلى 150000 دينار جزائري.

ونص المشرع الجزائري أيضاً في المادة (394 مكرر1) من قانون العقوبات، على عقوبة الاعتداء العمدي على المعطيات الموجودة داخل النظام، بالحبس من ستة أشهر إلى ثلاث سنوات والغرامة من 500000 إلى 2000000 دينار جزائري، في حالة ارتكاب الجرائم الماسة بالأنظمة المعلوماتية، وفي حالة حيازة، أو إفشاء، أو نشر، أو استعمال المعطيات المتحصل عليها من إحدى الجرائم الماسة بالأنظمة المعلوماتية، تكون العقوبة الحبس من شهرين إلى ثلاث سنوات والغرامة من 1000000 إلى 5000000 دينار جزائري.

كما نصت المادة (394 مكرر4) من القانون نفسه على العقوبات الواجبة التطبيق على الشخص المعنوي في حالة ارتكابه لأي جريمة اعتداء على نظام المعالجة الآلية للمعطيات

(59) فتيحة ليتيم ونادية ليتيم، الأمن المعلوماتي للحكومة الإلكترونية وإرهاب القرصنة، مجلة المفكر، جامعة محمد خيضر، بسكرة، الجزائر، المجلد 10، العدد 12، سنة 2015، ص 242.

(60) سالم مدني، مدى إمكانية تطبيق الحدود على الجرائم الإلكترونية، ورقة عمل مقدمة إلى ندوة المجتمع والأمن: الجرائم الإلكترونية الملامح والأبعاد، الرياض، 2007، ص 516.

بغرامة تعادل خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي، وذلك وفقاً لشروط المادة (51 مكرر) من القانون نفسه، إلى جانب تجريم الاشتراك والاتفاق والتحضير والشروع في أعمال تؤدي إلى وقوع هذا النوع من الجرائم بنص المواد (394 مكرر5 و394 مكرر6 و394 مكرر7) من قانون العقوبات الجزائري.

ومع أنّ المشرع الجزائري اعتمد في تجريم هذا النوع من الأفعال على أبعاد الركن المادي والطابع الجنحي لهذه الأعمال وجسامتها والظروف المشددة لعقوباتها؛ إلاّ أنّ ما يعاب عليه هو تركيزه على كون هذه الجرائم تعد مساساً بالنظام المعلوماتي المادي، وعدم ربطه لهذه الجرائم بالبعد الأمني حينما تكون تهديداً حقيقياً للأمن الوطني السيبراني، وهذا ما سيأتي بيانه لاحقاً في هذه الدراسة.

ولم يقتصر نطاق حماية المشرّع الجزائري لنظم المعلومات في الفضاء السيبراني على الجرائم المستحدثة إلكترونياً فحسب، بل امتد نطاق هذه الحماية ليشمل حقوق الملكية الأدبية والفنية والتجارية والصناعية في الفضاء السيبراني، فبخصوص براءات الاختراع نصت المادة (3) من الأمر رقم 03-07[61] المتعلّق ببراءات الاختراع على الشروط الواجب توافرها في الاختراع حتى يحظى بالحماية، وهي: الجدة والقابلية للتطبيق الصناعي، فإذا كانت براءة الاختراع تتعلّق بالحاسوب أو البرمجيات شرط أن تكون جزءاً من ذاكرة الحاسوب نفسه، وأن يتوفر فيها عنصر الابتكار وتنصب على منتوج صناعي جديد، مع الإشارة إلى أنّ المادة (7) من الأمر المذكور أعلاه استبعدت صراحة برامج الحاسوب من نطاق الحماية.

وفي حالة حقوق المؤلف فقد أكّدت المادة (5) من الأمر رقم 03-05[62] المتعلّق بحقوق المؤلف والحقوق المجاورة، أنّه من بين المصنفات المشمولة بالحماية قواعد البيانات، سواء أكانت مستنسخة على دعامة قابلة للاستغلال بواسطة آلة، أم أي شكل من الأشكال الأخرى، والملاحظ هنا أنّ المشرع قد وسّع من نطاق المؤلّفات المحميّة، حيث أدمج تطبيقات الإعلام الآلي ضمن المصنفات الأصلية والمعبّر عنها بمصنفات قواعد البيانات وبرامج الإعلام الآلي، التي اعتبرتها المادة (4) من الأمر نفسه ضمن المصنفات الأدبية المكتوبة الأولى بالحماية، والتي يصل نطاق حمايتها القانونية زمنياً إلى حدود 50 سنة من تاريخ وفاة المؤلف (المادة 58 من الأمر نفسه).

(61) الأمر رقم 03-07، مؤرخ في 19 جمادى الأولى 1424هـ الموافق 19 يوليو 2003، يتعلق ببراءات الاختراع، الجريدة الرسمية، الجزائر، العدد 44، بتاريخ 2003/07/23، ص 27.

(62) الأمر رقم 03-05 مؤرخ في 19 جمادى الأولى 1424هـ الموافق 19 يوليو 2003، يتعلق بحقوق المؤلف والحقوق المجاورة، الجريدة الرسمية، الجزائر، العدد 44، بتاريخ 2003/07/23، ص 3.

وقد اعتبر المشرع الجزائري في المادة (151) وما بعدها من الأمر نفسه، أنّ كل الأفعال التي تعدّ مساساً بحقوق التأليف والابتكار أيّاً كان نوع الفعل تأخذ توصيفاً جنحياً، سواء من قبيل التقليد أو التزوير والمحاكاة أو المساس بسلامة المصنف أو بيعه وتأجيره، أو تداول المصنف الأدبي والفني أو أي تطبيق أو برنامج آلي، وذلك من خلال عقوبات أصلية وتكميلية تتمثل في الحبس من ستة أشهر إلى ثلاث سنوات والغرامة من 500000 إلى 1000000 دينار جزائري، مع منح القاضي السلطة التقديرية لمصادرة المبالغ المساوية لمبلغ الإيرادات الناتجة عن الاستغلال غير المشروع للمصنف الرقمي أو الأداء المحمي قانوناً (المواد 156/153 إلى 159 من الأمر رقم 03-05).

والجدير بالذكر أنّه لا يمكن بأي حال القول بأنّ حماية قواعد الملكية الفكرية في الفضاء المعلوماتي المفتوح تدخل في إطار حماية الفضاء السيبراني، نظراً لصعوبة الفصل نظريّاً وواقعياً بين ما هو تقني معلوماتي بحت وما هو أمني، خصوصاً أنّ جل ما هو متوفر من نصوص تشريعية وتنظيمية لا يوجد فيه إشارة إلى مفهوم السيبرانية كمدلول تقني واضح، وأنّ معظم الاستخدامات المفاهيمية مستنتجة من تعريفات فنية مادية تندرج ضمن آليات تحديد مفهوم الجريمة الإلكترونية وأدوات مواجهتها.

وتأخذ القرصنة الإلكترونية عدة توصيفات منها: الاحتيال المعلوماتي، والاختراقات وجرائم التقنية العالية، وجرائم أصحاب الياقات البيضاء، والأنونيموس (الهاكرز المتخفون)، الذين يشنون منذ أكثر من عقدين حرباً لا هوادة فيها ضد المواقع الرسمية والسرية للدول والجماعات وفق منطلقات أيديولوجية معيّنة لتحقيق أهداف خاصة، أو في إطار التوظيف لفائدة جهات رسمية أو استخباراتية أو بدوافع شخصية، غير أنّ جميع السياسات التشريعية وآلياتها الردعية وحتى الجهود التنسيقية عجزت عن مواجهة هذا النوع من الجرائم في ظل ثورة رقمية مهولة، وفضاء افتراضي مفتوح على كل المخاطر والابتكارات، وفي عالم افتراضي يتجدد ويتطور ويتأقلم مع كل الآليات المستخدمة لمواجهته.

ومن أشهر هذه التحديات والصعوبات التي تواجه مكافحة القرصنة الإلكترونية ما يلي[63]:

- الصبغة العالمية للجريمة الإلكترونية المرتكبة عبر الإنترنت.
- صعوبة إثبات الجريمة الإلكترونية.

(63) أنيس العذار، مكافحة الجريمة الإلكترونية، المجلة الأكاديمية للبحث القانوني، جامعة عبد الرحمن ميرة، بجاية، الجزائر، المجلد 17، العدد 1، سنة 2018، ص 727-730.

– عدم قدرة نصوص التجريم التقليدية على مسايرة تطور الجريمة الإلكترونية.

والجدير بالذكر أنّ الجريمة السيبرانية قامت في الواقع على فكرة القرصنة الإلكترونية، فإذا كانت هذه الأخيرة عبارة عن توظيف للأدوات السيبيرانية من أجل أهداف سياسية أو أمنية (دفاعية أو هجومية)، فإنّ القرصنة الإلكترونية هي عملية تقنية بحتة قد لا يكون للمنطلقات والتكتيكات الأمنية أو الأبعاد الاستراتيجية للسيطرة على أكبر المساحات في المجال السيبراني الدولي الأولوية فيها، فقد تكون أهدافها تقنية فحسب، وقد تتعداها إلى الأغراض الاقتصادية والتجارية، حينما يتعلق الأمر ببراءات الاختراع الإلكترونية والحروب التجارية الدولية كما هو الشأن بين الصين والولايات المتحدة الأمريكية، أو بين شركتي آبل وسامسونج وبين شركتي هواوي وآبل.

ومع ذلك فإنّ الأمن السيبراني يتطلب استراتيجية متعددة المحاور والمستويات والأدوات ينبغي قطعاً ألاّ تنحصر في الصعيد الوطني؛ لأنّ التهديد السيبراني ينعكس بالضرورة على الأمن القومي للدول والجريمة السيبرانية (إرهاب، اختراق، قرصنة...إلخ) هي جريمة ذات امتدادات خارجية والعكس صحيح، والفاعل الرقمي في الفضاء السيبراني ليس حكراً على الدول المتطوّرة تكنولوجياً، بل وليس محصوراً في أيدي السلطة والأنظمة الاستخباراتية، أو ما يسمى بالجيوش الإلكترونية، مما يتطلب انتهاج استراتيجية وطنية وإقليمية ودولية لمواجهة المخاطر والتهديدات السيبرانية وانعكاساتها على الأمن القومي.

الفرع الثالث

الإرهاب السيبراني

على الرّغم من الاختلاف في تحديد مفهوم الإرهاب في الأساس، إلاّ أنّ هناك اجتهادات حول تحديد مفهوم الإرهاب السيبراني تحاكي تماماً مفاهيم الواقع، حيث عرّفته الأمم المتحدة بأنّه: «استخدام الإنترنت لنشر الأعمال الإرهابية». أمّا مكتب التحقيقات الفدرالي الأمريكي (F.B.I) فيعرّفه بأنّه: «كل اعتداء قصدي ذي دوافع سياسية على المعلومات، أو النظام المعلوماتي، أو البرامج، أو البيانات ينتج عنه أعمال عنف ضد المدنيين، سواء ارتكبت من قبل مجموعة وطنية أو عملاء غير مرئيين»[64]. في حين يعرّفه حلف شمال الأطلسي بأنّه: «أي هجوم سيبراني، يستخدم أو يستغل شبكات المعلوماتية أو شبكات

(64) إسحاق العشعاش، الإرهاب السيبراني وتحديات الدول: دراسة مقارنة مع الاتفاقيات الدولية، مجلة بحوث، جامعة بن يوسف بن خدة، الجزائر، المجلد 12، العدد 1، سنة 2018، ص 178.

الاتصال، لإحداث تدمير كاف لإثارة الرعب وإرهاب مجتمع، لأهداف إيديولوجية»[65]. كما تعرّفه كليات الحرب الأمريكية بأنّه: «هجمات الشبكات الكمبيوترية، انطلاقاً من تصنيفه تحت بند (العمليات الإلكترونية)[66].

ويعود أصل الربط بين مفهوم الإرهاب والسيبرانية إلى استخدام وسائل ووسائط التكنولوجيا المعلوماتية والاتصالية في تنفيذ أعمال إرهابية تتجاوز تداعياتها الأبعاد المحلية والوطنية لتؤثر بشكل كبير على الأمن القومي والإقليمي والدولي.

ويتضمن الإرهاب الإلكتروني أو الرقمي بهذا المعنى ما يلي[67]:

- أعمال اختراق المواقع وأنظمة المعلومات، وكافة أشكال القرصنة.
- نشر الرعب وأشكال التهديد الموجّهة نحو الأفراد أو الدول.
- استقطاب الأفراد للانخراط في التنظيمات الإرهابية والجهادية والجريمة عبر الوطنية.
- محاولة السيطرة الكاملة على المؤسسات والهياكل الاستراتيجية للدول عن طريق استعمال أسلحة تكنولوجيا المعلومات والاتصالات، أو مواجهة المعلومات من خلال الوسائط الإلكترونية[68]، وهو ما يؤدي في نهاية المطاف إلى شلل هذه الأنظمة.

والإرهاب في الفضاء السيبراني يعد معضلة حقيقية تواجه الدول وتهدّد الأمن والعلاقات الدولية، مما يتطلب حشد الجهود الدولية للحد من انتشاره، بانتهاج سياسات أمنية واستراتيجيات شاملة، وتنسيق إقليمي ومتعدد الأطراف، في ظل الفضاء الإلكتروني

(65) NATO Glossary of Terms and Definitions, AAP-06 Edition 2012Version 2. (NATO) defines terrorism as "the unlawful use Or, threatened use of force or violence against individuals or property tocoerce or intimidate governments or societies to achieve political, religious or ideological objectives".
https://ccdcoe.org/cyberdefinitions.html, Accessed on: 31/8/2019.

(66) Jennie M. Williamson, Information Operations: Computer Network Attack in the 21s Century. Carlisle Barracks, PA, U.S. Army War College, 2002, pp. 22-25. Also available online at: (http://handle.dtic.mil/100.2/ADA402018).

(67) حكيم غريب، الإرهاب السيبراني والأمن الدولي: التهديدات العالمية الجديدة وأساليب المواجهة، المجلة الجزائرية للدراسات السياسية، المدرسة الوطنية العليا للعلوم السياسية، الجزائر، المجلد 5، العدد 2، سنة 2018، ص 106.

(68) Mark R. Shulman, Discrimination in the Laws of Information Warfare, School of Law, Faculty Publications, Pace University, Columbia Journal of transnational Law, 1999, p. 937. (http://digitalcommons.pace.edu/lawfaculty/224).

المفتوح الذي يتغير كل يوم ويتطوّر في كل لحظة، ويهدّد مباشرة الأمن القومي للدول، من خلال الهجوم على أنظمة صنع القرار والأنظمة الدفاعية للدولة، والسعي للسيطرة على قواعد المعلومات، واستهداف الاتصالات وأنظمة المواصلات والخدمات العامة للمواطنين والدولة[69].

ولما كان الإرهاب الرقمي يندرج في إطار الحرب الرقمية، التي تعرف من خلال الإجراءات التي يتم اتخاذها بشكل سلبي على المعلومات ونظم المعلومات، وفي الوقت ذاته الدفاع عن هذه المعلومات والنظم التي تحتويها[70]؛ فإنّه يتطلب جهوداً فردية ودولية لمكافحته، حيث خلص التقرير رقم (98-2013/A/68) الصادر عن فريق الخبراء الحكومي المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية التابع للجمعية العامة للأمم المتحدة في سياق الأمن الدولي إلى أنّ: «القانون الدولي وبخاصة ميثاق الأمم المتحدة ينطبق على استخدام الدول لتكنولوجيات المعلومات والاتصال، وهو عنصر لابد من المحافظة عليه من أجل حفظ السلام والاستقرار، وتهيئة بيئة تكنولوجية منفتحة ومأمونة[71]، وهي مسؤولية دولية تنطلق من الوعي بخطورة الظاهرة والآثار الوخيمة التي تهدد استقرار الدول والأمن والسلم الدوليين».

(69) Martin C.Libicki, Conquest in Cyberspace: National Security and Information Warfare, New York, Cambridge University Press, 2007, p.13.

(70) Michael Wynne, Flying and Fighting in Cyberspace, Space Power Journal & Air, fall 2007, p. 1.
http://www.airpower.au.af.mil/apjinternational/apj-a/2007/fal07/wynne.pdf.

(71) إسحاق العشعاش، مرجع سابق، ص 192.

المبحث الثالث

الاستراتيجية الوطنية والإقليمية والدولية لمواجهة المخاطر والتهديدات السيبرانية

مع كل الصعوبات في تحديد مفهوم الأمن وطرق مواجهة الإجرام السيبراني العابر للحدود الذي تجاوز حدود فكرة القوة العسكرية إلى مفهوم القوة السيبرانية؛ فإنّه ينبغي تعزيز البيئة التشريعية الوطنية والاتفاقية الإقليمية بالآليات اللازمة للردع والمواجهة، وتعاوناً دولياً في نفس مستوى التعاون الدولي لمكافحة الإرهاب والجريمة المنظمة، وهو ما سوف نناقشه في المطلبين الآتيين:

المطلب الأول

الاستراتيجية الوطنية لحماية الفضاء السيبراني

لاشك أنّ أي استراتيجية وطنية لمواجهة الجرائم السيبرانية ينبغي أن تنطلق من الوعي بخطورة الإجرام السيبراني، والحاجة إلى معالجة الظاهرة نظراً لامتداداتها الإقليمية وأبعادها العالمية؛ الأمر الذي يمر حتماً عبر توفير البيئة التشريعية اللازمة والكوادر الإدارية والتقنية ذات الكفاءة العالية.

الفرع الأول

في المجال التشريعي

إنّ الشواهد الواقعية تشير إلى أنّ الجهود الوطنية في مجال مكافحة الجرائم السيبرانية ما زالت دون المستوى المطلوب، سواء من حيث إيجاد محاكم متخصصة أو دوائر تحقيق تكون مساندة للقضاء ومتخصصة للنظر في هذا النوع من الجرائم، أو من حيث الاهتمام بالجانب التدريبي لكوادر الأمن العام أو القضاة، لاسيما وأنّ الجرائم المعلوماتية تعد من الجرائم التي تحتاج إلى معرفة فنية دقيقة من أجل التعامل مع مرتكبيها، كما أنّ الجانب التشريعي في مكافحة جرائم المعلوماتية يعتريه القصور في العديد من المحاور، وخاصة فيما يتعلّق بالإجراءات الجزائية للتعامل مع هذا النوع من الجرائم[72].

(72) لورنس سعيد الحوامدة، الجرائم المعلوماتية أركانها وآلية مكافحتها: دراسة تحليلية مقارنة، مجلة الميزان للدراسات الإسلامية والقانونية، جامعة العلوم الإسلامية العالمية، ماليزيا، المجلد 4، العدد 1، سنة 2017، ص 27.

وهنا تجدر الإشارة إلى أنّه من بين ما يجب أن تعالجه منظومة القوانين السيبرانية ما يتعلق بـ: الأمن والدفاع الإلكتروني، وأسماء النطاقات التجارية، والجرائم الإلكترونية، سواء عبر الإنترنت أو في الإنترنت، وحقوق الملكية، وقوانين الخصوصية الشخصية، وحرية التعبير[73]، وهو ما دفع الجزائر في مستهل عام 2020 إلى وضع منظومة وطنية لأمن الأنظمة المعلوماتية[74] تهدف إلى إرساء إطار تنظيمي لإعداد الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية وتنسيق تنفيذها، حيث ترتكز هذه الاستراتيجية على هيئتين أساسيتين هما: المجلس الوطني لأمن الأنظمة المعلوماتية، ووكالة أمن الأنظمة المعلوماتية، اللتان تعملان بالتنسيق المباشر مع رئيس الجمهورية ووزير الدفاع الوطني.

كما أولت الجزائر أيضاً اهتماماً شديداً للإرهاب والقرصنة الإلكترونية، مما جعل الجزائر تخصص العديد من النصوص القانونية لمعالجة الظاهرة تشريعياً، وذلك من خلال قانون العقوبات (المواد من 87 مكرر إلى 87 مكرر6) التي نصت على جرائم الانخراط والتحريض والتشجيع والمشاركة والتعاطف والدعم والتمويل والنشر لصالح الجماعات الإرهابية، في حين ضاعفت المواد (من 394 مكرر إلى 394 مكرر7 المذكورة آنفاً) العقوبة حينما يتعلق الأمر باستهداف الدفاع الوطني أو المؤسسات العمومية (قانون العقوبات الجزائري رقم 04–15 المؤرخ في 10 نوفمبر 2004 المعدّل والمتمّم)، مع أنّ هذه الأفعال عوقبت وجرّمت بقطع النظر عن وسيلة ارتكابها، حيث إذا كان مجالها هو الفضاء السيبراني فإنّ الخسائر تكون أفدح، والمخاطر تكون أكبر.

غير أنّ التعديل الذي أتى به القانون رقم 16-02 المؤرخ في 19 يونيو سنة 2016 المعدّل لقانون العقوبات قد أضاف المادة (87 مكرر 11) التي تعاقب كل جزائري أو أجنبي يرتكب أفعالاً إرهابية، «أو يدبرها أو يعد لها أو يشارك فيها أو يدرب عليها أو يتلقى تدريباً عليها»، باستخدام تكنولوجيات الإعلام والاتصال (المادة 3 فقرة 2)، وأضاف التعديل المذكور المادة (87 مكرر 12) التي تنص على أن القانون يعاقب كل من يستخدم تكنولوجيات الإعلام والاتصال من أجل دعم تلك الأعمال أو تنظيمها أو نشر أفكارها بطريقة مباشرة أو غير مباشرة، أو تجنيد الأشخاص لصالح جمعية أو تنظيم أو جماعة أو منظمة يكون غرضها الإرهاب.

وبالتالي يتبيّن أنّ الأسلحة الإلكترونية المستعملة في الجريمة السيبرانية صارت بديلاً عن التهديدات اللا تماثلية (الإرهاب، والجريمة المنظمة والسلاح النووي)؛ لأنّه لا يحتاج

(73) يحيى مفرح الزهراني، الأبعاد الاستراتيجية والقانونية للحرب السيبرانية، مجلة البحوث والدراسات، جامعة الوادي، الجزائر، المجلد 14، العدد 1، سنة 2017، ص 234.

(74) المرسوم الرئاسي رقم 20-05 المؤرخ في 20 جانفي/يناير 2020، يتعلق بوضع منظومة وطنية لأمن المنظومة المعلوماتية، الجريدة الرسمية، الجزائر، العدد 4، بتاريخ 26 جانفي/ يناير 2020، ص 5.

إلى حدود جغرافية، ولا توجد وسائل مراقبة لتحديد هويته في الشبكة العنكبوتية على غرار الحروب التقليدية[75]، ممّا يؤدي إلى غياب الأمن القانوني أو حتى في تناقض الأحكام والقوانين، وتنازع الأنظمة القانونية من جهة أولى، وفي اتساع إمكانات نشوء مجالات للجريمة السيبرانية من جهة ثانية، إذ يرتفع منسوب هذه المخاطر مع انعدام التعاون بين الدول المختلفة، أو حتى مع وجود تعاون لا يضمن ملاحقة فاعلة تتلاءم وطبيعة الأعمال والجرائم والاعتداءات السيبرانية العابرة للحدود وللأنظمة القانونية، والتي لا يقف توسعها على المستوى الجغرافي، بحيث تطال أي إنسان في أي بقعة من الأرض، بل يتعداها إلى توسعها على المستوى الموضوعي بما يطال الدول وأمنها واستقرارها[76]، مما يقتضي أخذ جميع أبعاد الأمن السيبراني بعين الاعتبار، لدى وضع أي استراتيجية أو سياسة.

الفرع الثاني

في المجالين الإداري واللوجستي

تراهن الجزائر فيما خص هذين المجالين على غرار الكثير من البلدان على منظومة دفاعية وسياسة أمنية محكمة وشاملة يكون فيها الفاعل الرقمي مرتكزاً أساسياً ومحدداً للأمن القومي الوطني والإقليمي، حيث سارعت إلى مراجعة سياساتها الأمنية، وإدراجها لآليات جديدة تعنى بهذه المسائل، بالموازاة مع تطوير البُنى الأساسية المتعلقة بتكنولوجيات العالم الرقمي[77]، ويفرض مطلب الأمن مضاعفة أنظمة الرقابة التي قد تشكل تهديداً ممكناً للحريات الفردية، لهذا وجب مرافقة كل المقاربات الأمنية في مجال الأمن الرقمي للأطر القانونية والتكنولوجية الملائمة، والأخذ بعين الاعتبار دقة الهجمات الإلكترونية وتعقيداتها والتي يزداد خطرها مع التطور التكنولوجي واستخداماتها اليومية[78].

ولتحقيق هذه الأهداف تم اعتماد استراتيجية تعتمد تعزيز الدفاعات الإلكترونية الوطنية مرتكزة على نظام قانوني وبيئة تشريعية توفر الآليات الأساسية لحماية وتأمين المجال السيبراني الوطني معتمدة على التطور التقني في تكنولوجيا المعلومات والاتصالات،

(75) جمال بوازدية، مرجع سابق، ص 1270.

(76) منى الأشقر جبور، الأمن السيبراني: التحديات ومستلزمات المواجهة، مرجع سابق، ص 06.

(77) جمال رضوان، الأمن السيبراني: أولوية في استراتيجيات الدفاع، مجلة الجيش، الجزائر، العدد 630، جانفي/ يناير 2016، ص 40-41.

(78) سمير بارة، الأمن السيبراني في الجزائر: السياسات والمؤسسات، المجلة الجزائرية للأمن الإنساني، جامعة باتنة 1، الحاج الأخضر، باتنة، الجزائر، المجلد 2، العدد 2، سنة 2017، ص 264.

وفي هذا الصدد تم العمل على توفير الوسائل الآتية[79]:

- 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.

أما على المستوى اللوجستي والعملياتي، فقد تم استحداث عدة أجهزة لتأمين مجالها السيبراني الوطني نذكر منها:

- مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية للدرك الوطني.
- المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني.
- المصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة لمديرية الأمن الوطني.
- الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

المطلب الثاني

التعاون الدولي في مجال الأمن السيبراني

من خلال ما سبق، يتبيّن لنا أنّ المجال السيبراني المفتوح وما يمثله من أخطار أثرت وتؤثر في موازين القوى الدولية، يحتاج معه المجتمع الدولي إلى تعاون وتنسيق أمني من أجل الحد من هذه المخاطر والتهديدات، وتأمين حقوق الأفراد والمصالح الاستراتيجية للدول، وهذا التعاون الدولي ينبغي أن يتم على مستويين: إقليمي (عربي)، وعالمي.

الفرع الأول

على المستوى العربي

راهنت الدول العربية في مسعاها لضمان أمنها القومي على اعتماد الأمن السيبراني وتعزيز القدرات الدفاعية الإلكترونية كمرتكز أساسي لضمان أمنها الداخلي والإقليمي، وفي هذا الصدد تم على مستوى جامعة الدول العربية تبني اتفاقية تهدف إلى تعزيز

(79) المرجع السابق، ص 269.

التعاون وتدعيمه بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات[80] لدرء أخطار هذه الجرائم، حفاظاً على أمن الدول العربية ومصالحها وسلامة مجتمعاتها وأفرادها، وضماناً للحفاظ على القوى الوطنية والعربية من أي اعتداءات أو اختراقات إلكترونية، والإسهام في حفظ الثروات الإنسانية والمالية والتقنية والمعلوماتية للمؤسسات الحكومية والخاصة والأفراد من الهجمات والقرصنة الإلكترونية، بالإضافة إلى تأمين حماية البيانات والبُنى التحتية ضد أي هجوم إلكتروني أو اختراقات، مما يقتضي وضع آليات قانونية وتشريعية تضمن الاستخدام السيبراني الآمن.

وفي هذا الصدد شددت الاتفاقية العربية لبناء الثقة في مجال الأمن السيبراني[81] على ضرورة تعزيز التعاون العربي البيني والدولي، حيث نصت المادة (13) منها على ضرورة تعاون الدول الأعضاء، مع الهيئات الدولية والإقليمية، المتخصصة في قضايا حماية الفضاء السيبراني، لاسيما اللجان التابعة للأمم المتحدة، والاتحاد الدولي للاتصالات، والآيكان (هيئة الإنترنت للأسماء والأرقام)، وجامعة الدول العربية، وهيئات الاتحاد الأوروبي، ومجموعة دول الكومنولث، ومنظمة التعاون والتنمية الاقتصادية، وأي هيئة دولية أخرى ذات اختصاص وصلة بمسائل الأمن السيبراني، كما نصت المادة (14) على ضرورة تعاون الدول العربية الأعضاء، لحماية الفضاء السيبراني، والخدمات الإلكترونية، في منع ومكافحة الجرائم السيبرانية، طبقاً للقوانين والإجراءات الداخلية لكل دولة منها، من خلال الآتي:

- تبادل المعلومات المتعلّقة بأنشطة وجرائم الجماعات التي تنظّم الاعتداءات والهجمات على الأنظمة المعلوماتية والبُنى التحية للاتصالات والمعلومات والمواقع الإلكترونية، وتتبُّع مواقعها ووسائل اتصالاتها ودعاياتها المستخدمة.
- التحرّيات وتقديم المساعدة في مجال القبض على الهاربين من المتهمين أو المحكوم عليهم بجرائم سيبرانية وفقاً لقانون وأنظمة كل دولة.
- تبادل الخبرات والدراسات والبحوث وتوفير المساعدات الفنّية المُتاحة لإعداد برامج ودورات تدريبية مشتركة خاصة بكل دولة، أو بين الدول المتعاقدة للعاملين في مجال مكافحة الجرائم السيبرانية لرفع مستوى أدائهم.

(80) الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، جامعة الدول العربية، مجلس وزراء العدل العرب، القاهرة، 2010/12/21، والتي صادقت عليها الجزائر بموجب المرسوم الرئاسي رقم 14-252 بتاريخ 13 ذو القعدة 1435هـ الموافق 8 سبتمبر 2014، ويتضمن التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، المحررة بالقاهرة بتاريخ 21 ديسمبر 2010، الجريدة الرسمية، الجزائر، العدد 57، بتاريخ 2014/09/28، ص 4.

(81) الاتفاقية العربية لحماية الفضاء السيبراني بين الواقع والطموح، جامعة الدول العربية، مجلس وزراء العدل العرب، بيروت، 23-25 يوليو 2018.

وعلى الرّغم من ذلك، ما زالت هناك ثغرات تشريعية في الأنظمة القانونية العربية، لجهة المواضيع التي تتصل بتحقيق الأمن والثقة في الفضاء السيبراني، ويعود ذلك إلى غياب تشريعي كامل لبعض المواضيع واللجوء إلى تطبيق القوانين التقليدية في مواضيع أخرى، إضافة إلى تعارض بعض ما أقرّ من تشريعات، مع الإرشادات العالمية أو الممارسات الفضلى، الصادرة عن المنظمات الدولية.

الفرع الثاني

على الصعيد الدولي

يبدو أنّ الدول ما زالت إلى اليوم عاجزة عن وضع تعريف موحد للحرب السيبرانية؛ ممّا أجهض جهود المنظمات الدولية والمراكز البحثية لاقتراح الآليات الناجعة لمواجهة هذا التهديد، رغم وجود الأدلة الدامغة على الجرم المستنتج من بعض الأحداث التي عرضها الخبراء كعيّنات، مثل الهجمات السيبرانية التي استهدفت المصالح الحيوية (المنشآت النووية، والعسكرية) لبعض الدول على غرار ما حصل في كل من إستونيا وجورجيا والعراق وإيران[82]، ذلك أنّ ثغرات الأمن والدفاع أصبحت من الأزمات الدائمة التي لم تجد طريقها إلى الحل في الدول العظمى رغم الإمكانيات المادية – البشرية والتقنية – التي تتمتع بها، لأنّ الفجوة التي تم اكتشافها وتتكرر في كل مرة أنّ هناك اختلالاً وعدم احترام لقواعد حماية الأنظمة المعلوماتية من طرف المستخدمين؛ لذا نجد أنّ أنظمة الأمن والدفاع كثيراً ما تقف عاجزة أمام الاختراقات[83]. كما حذر خبراء في أمن المعلومات[84] من خطورة الاستمرار في تطوير الأسلحة السيبرانية، ويمكن في هذا الإطار الإشارة إلى العديد من الجهود الدولية والتنسيق المشترك لمكافحة الجرائم السيبرانية، نذكر منها على سبيل المثال لا الحصر:

(82) جمال بوازدية، مرجع سابق، ص 1272.

(83) عبد الله بن عبد العزيز بن فهد العجلان، الإرهاب الإلكتروني في عصر المعلومات، المؤتمر الدولي الأول حول حماية المعلومات والخصوصية في قانون الإنترنت، القاهرة، 2-4 جوان/يونيو 2008.

(84) منهم الخبير الروسي يوجين كاسبرسكي Eugene Kaspersky المدير العام لشركة (كاسبرسكي لاب Kaspersky Lab) المتخصصة في مجال أمن الحواسيب، الذي حذّر من أنّ استمرار تطوير الأسلحة السيبرانية وانتشارها Cyber Weapons من شأنه أن يغيّر وجه العالم الذي نعرفه، وأنّ البنية التحتية للعالم ليست مستعدة بعد لحماية نفسها من مثل هذه الأسلحة. مشار إليه لدى: ربيع محمد يحيى، إسرائيل وخطوات الهيمنة على ساحة الفضاء السيبراني في الشرق الأوسط: دراسة حول استعدادات ومحاور عمل الدولة العبرية في عصر الإنترنت 2002 ـ 2013، ص 77، تاريخ الاطلاع: 2020/9/11 متاح على الرابط الآتي:
http://strategicvisions.ecssr.com/ECSSR/ECSSR_DOCDATA_PRO_EN/Resources/P

1. اتفاقية بودابست لمكافحة الجريمة المعلوماتية:

تعد اتفاقية بودابست إحدى أهم الاتفاقيات في مجال التعاون الدولي لمكافحة الإجرام السيبراني، حيث اعتمدت هذه الاتفاقية مصطلح جرائم الإنترنت على نطاق واسع[85]، وهي ترمي بشكل أساسي إلى مواءمة عناصر القانون الموضوعي الجنائي المحلي والأحكام المتصلة بالجرائم في مجال الجريمة الإلكترونية، والتنصيص على صلاحيات القانون الإجرائي الجنائي الداخلي اللازمة للتحقيق في هذه الجرائم، ومتابعتها قضائياً، علاوة على الجرائم الأخرى التي ترتكب عن طريق الكمبيوتر، أو التي تكون الأدلة المتصلة بها في شكل إلكتروني، وإلى إنشاء نظام سريع وفعّال للتعاون الدولي، وهي بمثابة صك دولي ملزم بشأن هذه المسألة، أو مبدأ توجيهي لأي بلد لوضع تشريع وطني شامل لمكافحة جرائم الإنترنت، وإطار للتعاون الدولي بين الدول الأطراف في هذه الاتفاقية[86].

وقد تضمنت هذه الاتفاقية مجموعة من المبادئ العامة المتعلقة بالتعاون الدولي في مجال الشؤون الجنائية، وحدّدت الإجراءات المتعلقة بطلبات المساعدة المتبادلة بين الدول في غياب الاتفاقيات الدولية[87]، وقد وقّعت على هذه الاتفاقية 30 دولة، ولأهمية هذه الاتفاقية انضمَّ إليها العديد من الدول من خارج المجلس الأوروبي، وأبرز هذه الدول الولايات المتحدة الأمريكية، التي صادقت عليها في 22 سبتمبر 2006، ودخلت حيّز النفاذ في الأول من يناير 2007[88]، وتهدف الاتفاقية إلى التالي[89]:

- توحيد عناصر القانون الجزائي المحلي مع الأحكام المتعلقة بالجرائم الإلكترونية.
- توفير الإجراءات القانونية اللازمة للتحري وملاحقة الجرائم المرتكبة إلكترونياً بواسطة الكمبيوتر.
- تعيين نظام سريع وفعّال للتعاون الدولي.
- الحفاظ بشكل سريع على البيانات المخزّنة على أجهزة الكمبيوتر وحفظها والإفصاح الجزئي عن حركة هذه البيانات المخزنة على الكمبيوتر.

(85) Jan-Jaap Oerlemans, Investigating cybercrime, Doctoral Thesis, Leiden University, Netherlands, 2017, p. 20, Available at : https://scholarlypublications.universiteitleiden.nl/handle/1887/44879.

(86) Cypercrime-Budapest Convention and related standards-council of Europe 17.1.2017, available at: http://www.coe.int/en/web/cybercrime/the-budapest-conventio.

(87) عبد العال الديربي ومحمد صادق إسماعيل، الجرائم الإلكترونية، ط1، المركز القومي للإصدارات القانونية، القاهرة، 2012، ص 8.

(88) ليلى الجنابي، فعالية القوانين الوطنية والدولية في مكافحة الجرائم السيبرانية، مجلة الحوار المتمدن، العدد 34، سنة 2017، ص 23-24، تاريخ الاطلاع: 2019/9/11، متاح على الرابط الآتي:
http://www.ahewar.org/debat/show.art.asp?aid=571423&r=0

(89) جورج لبكي، المعاهدات الدولية للإنترنت، مجلة الدفاع الوطني، بيروت، العدد 83، كانون الثاني / يناير 2013. تاريخ الاطلاع: 2020/09/11، متاح على الرابط الآتي :
https://www.lebarmy.gov.lb/ar/content/%D8%A7%D9%84%D9

- جمع معلومات عن حركة البيانات وعن إمكان وجود تدخّل في محتواها.

2. مجموعة الدول الثماني G8[90]:

اعتمد وزراء العدل والداخلية التابعين لبلدان الـ G8 وهي: (الولايات المتحدة الأمريكية واليابان وألمانيا، وروسيا الاتحادية وإيطاليا والمملكة المتحدة وفرنسا، وكندا) في اجتماعاتهم المختلفة سياسات لمكافحة العديد من جرائم الإنترنت تستند إلى المبادئ التالية:

أ. عدم إتاحة ملاذات آمنة للمعتدين على تكنولوجيا المعلومات.

ب. التنسيق بين جميع الدول المعنية في ملاحقة مرتكبي جرائم الإنترنت ومحاكمتهم بغض النظر عن مكان حدوث الضرر.

ج. تدريب الموظّفين المكلفين بتنفيذ القوانين وتجهيزهم بالمعدات الضرورية للتعامل مع الجرائم ذات التقنية العالية.

وبالإضافة إلى ذلك دعت هذه الدول إلى مواصلة العمل حتى يتم التوصّل إلى حلول دولية ناجحة، وقد تبنت في هذا الإطار عدة مبادئ وتوصيات من أبرزها:

- مبادئ وخطة العمل بشأن الجريمة ذات التكنولوجيا العالية وجرائم الكمبيوتر 1997.
- مبادئ بشأن الحصول على المعلومات المخزّنة على الكمبيوتر خارج حدود الدول 1999.
- توصيات لتعقّب الاتصالات على الشبكة خارج الحدود الوطنية في التحقيقات الإرهابية والإجرامية 2002.
- مبادئ توافر البيانات الأساسية لحماية السلامة العامة 2002، وإعلان بيان دول مجموعة الثمانية فيما يتعلق بحماية نظم المعلومات 2002، ناهيك عن مجموعة من البروتوكولات والإعلانات الدولية، نذكر منها على سبيل المثال لا الحصر: إعلان فيينا لسنة 2000[91]، وإعلان بانكوك 2005[92]، وبروتوكول ستراسبورغ لسنة 2003[93].

(90) ليلى الجنابي، مرجع سابق، ص 22.

(91) UN. Vienna Declaration on Crime and Justice. Article 18. 1.2.2017, Available at: https://www.unodc.org/documents/commissions/CCPCJ/Crime

(92) UN. Bangkok Declaration, Article 15-16. 1.2.2017, Available at : http://www.un.org/events/11thcongress/declaration

(93) Council of Europe- Details of Treaty No.189- 2017.1.18, Available at: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189.

الخاتمة:

في ختام هذه الدراسة، تبيّن للباحثين أنّه وفي خضم التحولات الدولية الراهنة سياسياً واقتصادياً وأمنياً وعسكرياً وعلمياً، أصبح من الضروري إعادة النظر في خارطة المفاهيم الجيوسياسية والجيو- استراتيجية على نحو يأخذ في الحسبان التحولات والاختلالات الحاصلة في موازين القوى الدولية التي تطبعها حرب محمومة بين الدول الفاعلة صاحبة الريادة في مجال تكنولوجيا الاتصال والمعلومات من أجل تأمين مصالحها الوطنية والاقتصادية وضمان أمنها القومي؛ الأمر الذي أدى إلى إعادة النظر في كثير من المفاهيم التقليدية (الأمن والقوة والحرب والصراع والسيادة)، حيث طرحت الدراسات الاستراتيجية والأمنية الحديثة أمام الباحثين نمطاً جديداً من الحروب غير التقليدية لا مكان فيه للمفاهيم التقليدية، وشكلاً جديداً من النظم الدفاعية يحتل فيها الفاعل الرقمي أساس المعادلة الأمنية فيما يسمى بالدفاع السيبراني وتأثيراته على مفاهيم السيادة السيبرانية، في ظل فضاء رقمي مفتوح مفعم بالمخاطر والتهديدات الأمنية، كما أنتج هذا الوضع أشكالاً من الصراعات الدولية والإقليمية أسهمت فيه الثورة الرقمية بشكل واضح في ترجيح موازين القوى بين الدول التي صارت تعتمد استراتيجيات أمنية ودفاعية تعتمد حرباً معلوماتية ضروساً، البقاء فيها لمن يحسن استخدام تكنولوجيا المعلومات، ويوظّفها لخدمة أهدافه الدفاعية أو الهجومية.

وقد كان للتطور المهول الحاصل في المجال الرقمي والصراع المحتدم في الفضاء السيبراني أثر واضح في تغيّر كثير من المفاهيم التقليدية؛ إذ لم تعد القوة العسكرية وحدها هي الضامن لتحقيق الأمن القومي بفعل امتلاك دول غير نافذة دولياً، ومنظمات، وكيانات وأفراد هامش مناورة كبير في هذا الفضاء؛ ممّا أدى إلى انتشار أشكال وصور من التهديدات والجرائم السيبرانية التي تتطلب تعزيز آليات الوقاية والمواجهة بالتحرك في المساحة بين الجهود التشريعية، والتنسيق الأمني الدولي الاستراتيجي للتقليل من فداحة هذه المخاطر والتهديدات، والحد من احتدام الحروب الكونية السيبرانية، والتي رغم قلة إمكاناتها إلاّ أنّ أدواتها وأسلحتها أكثر فتكاً وأشد تدميراً.

وقد تمّ تسجيل مجموعة من النتائج، كما تم تقديم مجموعة من التوصيات، وذلك كالآتي:

أولاً: النتائج

1) صعوبة تفكيك التداخل المفاهيمي بين أمن المعلومات والأمن السيبراني في ظل اعتماد مقاربة تقنية محضة في تحديد معالم حدود الفضاء المعلوماتي وفواعله وأدواته وارتباط السيبرانية بالبعد الأمني والاستراتيجي.

2) لقد بات الأمن السيبراني يشكّل جزءاً أساسياً من أي سياسة أمنية وطنية، حيث بات معلوماً أنّ صناع القرار في العالم، أصبحوا يصنفون مسائل الدفاع السيبراني/الأمن السيبراني كأولوية في سياساتهم الدفاعية الوطنية.

3) إنّ سوء الاستغلال المتنامي للشبكات الإلكترونية لأهداف إجرامية يؤثر سلباً على سلامة البنى التحتية للمعلومات الوطنية الحساسة، لاسيما على المعلومات الشخصية والبنى التحتية الأمنية الاستراتيجية.

4) انحصار الآليات التشريعية في نصوص قانونية وتنظيمية تعنى في مجملها بالجريمة المعلوماتية، والجزاءات المقررة بشأنها، دون أي إشارة إلى السيبرانية في بعديها الأمني والاستراتيجي.

5) وجود قانون شامل للسيبرانية في الجزائر يتطلب منظومة متكاملة من الآليات التشريعية والمؤسسية لضمان مواكبة ثورة المعلومات، والإحاطة بكل مستجدات عالم السيبرانية، وهي خطوة وإن كانت غير كافية إلا أنّها تعبر عن توجه حقيقي نحو توفير الإمكانات اللوجيستية والفنية لتأمين حدودها السيبرانية.

ثانياً: التوصيات

في ضوء النتائج السابقة، توصي الدراسة بما يلي:

1) نوصي السلطتين التنفيذية والتشريعية في الجزائر بالتعاون من أجل وضع منظومة وطنية شاملة لأمن وحماية الفضاء السيبراني الذي أصبح اليوم واحداً من أهم مرتكزات بناء وتوفير الشروط السليمة للتنمية الشاملة المبنية على تداول آمن وتوفير مُجد للمعلومات باستخدام الفضاء السيبراني وتكنولوجيا المعلومات كجسر ووسيلة ومتن لهذا الكم الهائل من المعلومات.

2) نوصي السلطة التنفيذية بانتهاج سياسة استراتيجية للأمن والدفاع السيبراني تنطلق من الوعي بالعلاقة المتلازمة بينه وبين الأمن القومي؛ ذلك أنّ الأمن السيبراني يمس أمن الثروة الرقمية والثقافية للناس وللمنظمات وللبلدان، مع أنّ التحديات التي ينطوي عليها ذلك مُعَقدة.

3) نوصي السلطة التنفيذية بضرورة توفر الإرادة اللازمة لتصميم وتنفيذ استراتيجية لتطوير بنى تحتية وخدمات رقمية تشمل استراتيجية للأمن السيبراني تكون متماسكة وفعّالة، وقابلة للتحقق منها ومن إدارتها، ويجب أن تكون استراتيجية الأمن السيبراني جزءاً من نهج متعدد التخصصات، مع وجود حلول جاهزة على المستوى التثقيفي، والقانوني، والإداري، والتقني.

4) نوصي السلطة التنفيذية بالعمل على تحفيز ونشر وعي وطني بثقافة الأمن السيبراني من أجل تحصين المجتمع، وإنجاح خطط التنمية الشاملة؛ الأمر الذي من شأنه أن ينعكس إيجاباً على الاستجابة القوية للأبعاد البشرية والقانونية والاقتصادية لاحتياجات أمن البنية الأساسية الرقمية من أجل بناء الثقة، وتحقيق النمو الاقتصادي.

5) نوصي السلطات التنفيذية والإدارية بضرورة تعزيز الكوادر الفنية والأمنية المؤهلة والمدربة، وتزويدها بالوسائل القانونية والتقنية والتكنولوجية، مع تفعيل الإرادة التنفيذية لحماية المجال السيبراني الوطني باعتباره مجالاً حيوياً أولى بالحماية ومرتكزاً أساسياً للسيادة الوطنية؛ لأنّ الكثير من الدول العربية، تفتقر إلى موارد بشرية ومالية، وإلى إرادة واضحة وحازمة، تساعد على متابعة ما يجري في الفضاء السيبراني من نشاطات غير شرعية تنطلق من أراضيها. وفي هذا المجال، لابد من التشديد على ضرورة التعاون بين القطاعين العام والخاص والمجتمع المدني للتوصل إلى نشر ثقافة احترام القانون في الفضاء السيبراني، وحماية الحقوق والحريات الأساسية.

6) نوصي كذلك المشرّع بتعزيز البيئة القانونية بالأدوات اللازمة للوقاية من الجريمة السيبرانية استباقياً، ثم بعد ذلك اعتماد آليات الردع، فالشواهد الواقعية تشير إلى أنّ البيئة التنظيمية والتشريعية العربية، ما زالت في طور التشكل على الرغم من أنّ بعض الدول العربية عضو في الاتحاد الدولي للاتصالات، وفي الأمم المتحدة، وفي الشراكة الدولية متعددة الأطراف لمكافحة التهديدات السيبرانية، لكنها تحتل مراتب متأخرة دولياً في مجال أمن الفضاء السيبراني، ممّا يؤكد هشاشة دفاعاتها الإلكترونية واختلالاتها في مفهوم السيادة، مما يقتضي وضع إطار تعاون يضمن تبادل المعلومات ونقل الممارسات الفضلى في المجال الأمني.

7) نوصي السلطة التنفيذية بضرورة وضع استراتيجية لنشر الوعي وبنائه لدى مختلف شرائح المجتمع، سواء من كان منهم من المستخدمين العاديين أو المهنيين أو متخذي القرار والمسؤولين عن سياسات الأمن والسلامة، مما يقتضي تأمين انسجام الأنظمة القانونية المكافحة للجرائم السيبرانية.

المراجع:

أولاً: باللغة العربية

1. الكتب العامة:

- جون باسيت وأوستن لونج وآخرون، الحروب المستقبلية في القرن الواحد والعشرين، ط1، مركز الإمارات للدراسات والبحوث الاستراتيجية، أبو ظبي، 2014.
- نجم عبد الله الحميدي، نظم المعلومات الإدارية – مدخل معاصر، ط1، دار وائل للنشر، عمان، الأردن، 2005.
- سونيا محمد البكري، نظم المعلومات الإدارية – المفاهيم الأساسية، الدار الجامعية، الإسكندرية، 2000.
- رشا مصطفى أبو الغيط، الحماية القانونية للكيانات المنطقية، دار الفكر الجامعي، الإسكندرية، 2003.

2. الكتب المتخصصة:

- أشرف السعيد أحمد، القرصنة الإلكترونية، دار النهضة العربية، القاهرة، 2013.
- منى الأشقر جبور، السيبرانية: هاجس العصر، المركز القانوني للبحوث القانونية والقضائية، القاهرة، 2018.
- عباس بدران، الحرب الإلكترونية، الاشتباك في عالم المعلومات، مركز دراسات الحكومة الإلكترونية، بيروت، 2010.
- عبد العال الديربي ومحمد صادق إسماعيل، الجرائم الإلكترونية، ط1، المركز القومي للإصدارات القانونية، القاهرة، 2012 .
- علاء عبد الرزاق السالمي، تكنولوجيا المعلومات، ط 3، دار المناهج، عمان، الأردن، 2000
- ذياب البداينة، الأمن وحرب المعلومات، الإصدار الثاني، ط1، دار الشروق، عمان، الأردن، 2006.

3. المقالات والبحوث:

- أنيس العذار، مكافحة الجريمة الإلكترونية، المجلة الأكاديمية للبحث القانوني، جامعة عبد الرحمن ميرة، بجاية، الجزائر، المجلد 17، العدد 1، سنة 2018.
- إسحاق العشعاش، الإرهاب السيبراني وتحديات الدول: دراسة مقارنة مع الاتفاقيات الدولية، مجلة بحوث، جامعة بن يوسف بن خدة، الجزائر، المجلد 12، العدد 1، سنة 2018.
- جمال بوازدية، الاستراتيجية الجزائرية في مواجهة الجرائم السيبرانية: التحديات والآفاق المستقبلية، مجلة العلوم القانونية والسياسية، جامعة الوادي، الجزائر، المجلد 10، العدد 1، أفريل/ أبريل 2019.
- جمال منصر، تحولات في مفهوم الأمن: من أمن الوسائل إلى أمن الأهداف، مجلة دفاتر السياسة والقانون، جامعة قاصدي مرباح، ورقلة، الجزائر، العدد 1، جانفي/ يناير 2009.
- جمال رضوان، الأمن السيبراني: أولوية في استراتيجيات الدفاع، مجلة الجيش، الجزائر، العدد 630، جانفي/يناير 2016.
- حكيم غريب، الإرهاب السيبراني والأمن الدولي: التهديدات العالمية الجديدة وأساليب المواجهة، المجلة الجزائرية للدراسات السياسية، المدرسة الوطنية العليا للعلوم السياسية، الجزائر، المجلد 5، العدد 2، سنة 2018.
- حسن بن أحمد الشهري، نحو قانون دولي موحد لمكافحة الجرائم المعلوماتية، مجلة دراسات وأبحاث، جامعة زيان عاشور، الجلفة، الجزائر، المجلد 1، العدد 1، سنة 2009.
- يحيى مفرح الزهراني، الأبعاد الاستراتيجية والقانونية للحرب السيبرانية، مجلة البحوث والدراسات، جامعة الوادي، الجزائر، المجلد 14، العدد 1، سنة 2017.
- لورنس سعيد الحوامدة، الجرائم المعلوماتية أركانها وآلية مكافحتها: دراسة تحليلية مقارنة، مجلة الميزان للدراسات الإسلامية والقانونية، جامعة العلوم الإسلامية العالمية، ماليزيا، المجلد 4، العدد 1، سنة 2017.
- محمد مختار، هل يمكن أن تتجنب الدول مخاطر الهجمات الإلكترونية، مجلة اتجاهات الأحداث، مركز المستقبل للأبحاث والدراسات المتقدمة، أبوظبي، العدد 6، جانفي/يناير2015.

- محمد وائل القيسي، مستقبل الأمن الاستراتيجي العالمي في ظل التحديات التكنو– معلوماتية والفضاء السيبراني، مجلة دراسات إقليمية، جامعة الموصل، العدد 44، أفريل/ أبريل 2020.
- محمود محارب، إسرائيل والحرب الإلكترونية، قراءة في كتاب حرب في الفضاء الإلكتروني: اتجاهات وتأثيرات على إسرائيل، المركز العربي للأبحاث ودراسة السياسات، بيروت، 2011.
- نبيل إدريس، الجريمة السيبرانية بين المفاهيم والنصوص التشريعية: الجزائر أنموذجاً، مجلة القانون والمجتمع، جامعة أحمد دراية، أدرار، الجزائر، المجلد 5، العدد 2، سنة 2007.
- سامر مؤيد عبد اللطيف، الحرب في الفضاء الرقمي رؤية مستقبلية، مجلة رسالة الحقوق، مركز الدراسات القانونية والدستورية، جامعة كربلاء، العراق، السنة السابعة، العدد 2، سنة 2015.
- سيف نصرت الهرمزي، رصف المقاربات لمنظورات الفاعل الرقمي والانكشاف الاستراتيجي في ظل الفضاء السيبراني، مجلة آداب الفراهيدي، جامعة تكريت، العراق، العدد 37، مارس 2019.
- سمير بارة، الأمن السيبراني في الجزائر: السياسات والمؤسسات، المجلة الجزائرية للأمن الإنساني، جامعة باتنة1، الحاج الأخضر، باتنة، الجزائر، المجلد 2، العدد 2، سنة 2017.
- سعيد درويش، الحروب السيبرانية وأثرها على حقوق الإنسان: دراسة على ضوء أحكام دليل تالين، المجلة الجزائرية للعلوم القانونية والاقتصادية والسياسية، جامعة الجزائر1، المجلد 54، العدد 5، جوان/ يونيو 2018.
- عبد العزيز بن فهد بن محمد بن داود، الجرائم السيبرانية: دراسة تأصيلية مقارنة، مجلة الاجتهاد للدراسات القانونية والاقتصادية، جامعة تمنراست، الجزائر، المجلد 9، العدد 3، سنة 2020.
- عبد الغفار عفيفي الدويك، الأزمات والحروب السيبرانية... تهديدات تتجاوز الفضاء الإلكتروني، مركز الأهرام للدراسات السياسية والاستراتيجية، القاهرة، العدد 82، سنة 2019.
- غانم محمد صالح، أمن الخليج العربي، بين الاحتكار الأمريكي ورغبة المشاركة الأوروبية، مجلة العلوم السياسية، كلية العلوم السياسية، جامعة بغداد، العدد 32، جانفي/ يناير 2008.

- فاطمة بيرم، السيادة الوطنية في ظل الفضاء السيبراني والتحولات الرقمية: الصين أنموذجاً، المجلة الجزائرية للأمن الإنساني، جامعة باتنة1، الحاج الأخضر، باتنة، الجزائر، المجلد 5، العدد1، جانفي/ يناير 2020.
- فتيحة ليتيم ونادية ليتيم، الأمن المعلوماتي للحكومة الإلكترونية وإرهاب القرصنة، مجلة المفكر، جامعة محمد خيضر، بسكرة، المجلد 10، العدد 12، سنة 2015.

4. ندوات ومؤتمرات علمية:

- منى الأشقر جبور، الأمن السيبراني: التحديات ومستلزمات المواجهة، المركز العربي للبحوث القانونية والقضائية، جامعة الدول العربية، الندوة الأولى للمختصين في أمن وسلامة الفضاء السيبراني، بيروت، 28/27 أغسطس 2012.
- سالم مدني، مدى إمكانية تطبيق الحدود على الجرائم الإلكترونية، ورقة عمل مقدمة إلى ندوة المجتمع والأمن: الجرائم الإلكترونية الملامح والأبعاد، الرياض، 2007.
- عبد الله بن عبد العزيز بن فهد العجلان، الإرهاب الإلكتروني في عصر المعلومات، المؤتمر الدولي الأول حول حماية المعلومات والخصوصية في قانون الإنترنت، القاهرة، 2-4 جوان/ يونيو 2008.

5. المواقع الإلكترونية:

- إيهاب خليفة، القوة الإلكترونية: كيف يمكن أن تدير الدول شؤونها في عصر الإنترنت، 2017، ص 5، تاريخ الاطلاع: 2020/9/5، متاح على الرابط الآتي:
https://middle-east-online.com
- إسماعيل قادير، إدارة الحروب النفسية في الفضاء الإلكتروني: الاستراتيجية الأمريكية الجديدة في الشرق الأوسط، أبحاث الندوة الدولية: عولمة الإعلام السياسي وتحديات الأمن القومي للدول النامية، تاريخ الاطلاع: 2020/05/31، البحث موجود على الرابط الآتي:

https://manifest.univ-ouargla.dz/documents/Archive/2016-2017/FDSP/11-04-

- جورج لبكي، المعاهدات الدولية للإنترنت، مجلة الدفاع الوطني، لبنان، العدد 83، كانون الثاني/ يناير 2013، تاريخ الاطلاع: 2020/09/11 متاح على الرابط الآتي:

https://www.lebarmy.gov.lb/ar/content/%D8%A7%D9%84%D9

- حمدون إ. توريه، الاستجابة الدولية للحرب السيبرانية: البحث عن السلام السيبراني، الاتحاد الدولي للاتصالات، يناير 2011، تاريخ الزيارة: 2019/8/31، متاح على الرابط الآتي:
www.itu.int › S-GEN-WFS.01-1-2011-MSW-A.docx
- يوسف بوغرارة، الأمن السيبراني: الاستراتيجية الجزائرية للأمن والدفاع في الفضاء السيبيري، مجلة الدراسات الإفريقية وحوض النيل، المركز الديمقراطي العربي، برلين، ألمانيا، المجلد1، العدد 3، سبتمبر 2018.
- ليلى الجنابي، فعالية القوانين الوطنية والدولية في مكافحة الجرائم السيبرانية، مجلة الحوار المتمدن 34، 2017، تاريخ الاطلاع: 2019/09/11، متاح على الرابط الآتي: http://www.ahewar.org/debat/show.art.asp?aid=571423&r=0
- موسى محمد آل طويرش، الصراع السيبراني: مفهومه وأثره في العلاقات الدولية، مؤتمر كلية العلوم السياسية، الجامعة المستنصرية، العراق، 27 فبراير2019، ص 2، متاح على الرابط الآتي:
https://uomustansiriyah.edu.iq/media/attachments/11/11_2019_04_16!10_41_58_AMpdf.
- محمد فخر الدين، حدود المجال الخامس: ما هي الحروب السيبرانية، مؤتمر حروب الفضاء السيبراني، 2020/09/07، البحث موجود على الرابط الآتي: https://bit.ly/3rvr1zk
- نسرين فوزي اللواتي، التفاعل بين الإنسان والحاسوب: التحدي الأكبر في العصر الرقمي، مجلة لغة العصر، بوابة الأهرام، القاهرة، تاريخ الاطلاع: 2020/08/14، متاح على الرابط التالي:
http://aitmag.ahram.org.eg/News/77860/
- عبد المعطي زكي، الأمن القومي قراءة في المفهوم والأبعاد، المعهد المصري للدراسات السياسية والاستراتيجية، البحث موجود على الرابط الآتي:
https://eipss-eg.org/wp-content/uploads/2016/02/
- علي عبد الرحمن العبودي، هاجس الحروب السيبرانية وتداعياتها على الأمن والسلم الدوليين، موجود على الرابط الآتي:
https://www.iasj.net/iasj/download/ea15ee56e82595de

- ربيع محمد يحيى، كتاب إسرائيل وخطوات الهيمنة على ساحة الفضاء السيبراني في الشرق الأوسط، دراسة حول استعدادات ومحاور عمل الدولة العبرية في عصر الإنترنت (2002-2013)، تاريخ الاطلاع: 11-09-2020 متاح على الرابط الآتي:
http://strategicvisions.ecssr.com/ECSSR/ECSSR_DOCDATA_PRO_EN/Resources/P

ثانياً: باللغة الأجنبية

- Bing, Christopher, Suspected Russian Hackers Spied on U.S. Treasury Emails – Sources, Reuters, Dec. 13, 2020, Available at : https://www.reuters.com/article/us-usa-cyber-treasury-exclsuive-idUSKBN28N0PG, Accessed on: Dec. 21, 2020.
- 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.
- David J. Smith, How Russia Harnesses Cyber Warfare, Defense Dossier, American Foreign Policy Council, Issue 4, August 2012, Available at: http://www.insidethecoldwar.com/files/august2012.pdf.
- Dorothy E. Denning, Cyber terrorism, Global Dialogue, Autumn, 2000, p. 01, Available at: http://palmer.wellesley.edu/~ivolic/pdf/Classes/Handouts/NumberTheoryHandouts/Cyberterror-Denning.pdf.
- Edward Amoroso, Cyber Security, Silicon Press, 2007.
- Gregory Asmolov, "Russia: New Military Doctrine and Information Security"Global Voices, 2010, Available at: http://globalvoicesonline.org/2010/02/23/russian-military-doctrine/
- ITU, Cyber security, Geneva: International Telecommunication Union (ITU),2008.
- James Carroll, House of War: The Pentagon and the Disastrous Rise of American Power, Houghton Mifflin Harcourt, 2016.

- Jan-Jaap Oerlemans, Investigating cybercrime, Doctoral Thesis, Leiden University, Netherlands, 2017.
- Jinghan Zeng and Tim Stevens and Yaru Chen, China's Solution to Global Cyber Governance: Unpacking the Domestic Discourse of "Internet Sovereignty", P&P Politics & Policy, Volume 45, Issue 3, June 2017, Available at : https://onlinelibrary.wiley.com/doi/abs/10.1111/polp.12202.
- Jennie M. Williamson, Information Operations: Computer Network Attack in the 21s Century. Carlisle Barracks, PA, U.S. Army War College. 2002. Also available online at: http://handle.dtic.mil/100.2/ADA402018.
- Joseph S.Nye JR, Cyber Power, Harvard Kennedy School, 2010.
- Kenneth V. Peifer, Ananalysis of unclassified current And Pending Air Force Information Warfare And Information Operations Doctrine And Policy, A Master Thesis, Graduate School of Logistics And Acquisition Management, Air Force Institute of Technology, Kaduna, Nigeria, December 1997,
- Kevin Coleman, Russia's Cyber Forces, Available at: https://www.military.com/defensetech/2008/05/27/russias-cyber-forces –
- Marcelo Mendonça Teixeira, Cyberculture: From Plato To The Virtual Universe, The Architecture of Collective Intelligence, Munich: GrinVerlag, 2012.
- Mark R. Shulman, Discrimination in the Laws of Information Warfare, School of Law, Faculty Publications, Pace University, Columbia Journal of transnational Law 1999, Available at: http://digitalcommons.pace.edu/lawfaculty/224.
- Martin C. Libicki, Conquest in Cyberspace: National Security and Information Warfare", New York, Cambridge University Press, 2007.
- Michael Wynne, "Flying and Fighting in Cyberspace", Space Power Journal & Air fall 2007, Available at: http://www.airpower.au.af.mil/apjinternational/apj-a/2007/fal07/wynne.pdf.

- Ellen Nakashima and Craig Timberg, Russian Government Spies Are Behind A Broad Hacking Campaign That Has Breached U.S. Agencies And A Top Cyber Firm, National Security Dec.13, 2020, Available at : https://web.archive.org/web/20201213220635/https://www.washingtonpost.com/national-security/russian-government-spies-are-behind-a-broad-hacking-campaign-that-has-breached-us-agencies-and-a-top-cyber-firm/2020/12/13/d5a53b88-3d7d-11eb-9453-fc36ba051781_story.html , Accessed on Dec.22nd 2020.
- NATO Glossary of Terms and Definitions, AAP-06 Edition 2012Version 2. (NATO) defines terrorism as "the unlawful use or, threatened use of force or violence against individuals or property to coerce or intimidate governments or societies to achieve political, religious or ideological objectives", Available at: https://ccdcoe.org/cyberdefinitions.html31 31-8-2019.
- Richard A. Kemmerer, Cyber security, University of California Santa Barbara, Department of Computer Science, 2003.
- The International Télécommunication Union, ITU Toolkit for CybercrimeLégislation, Geneva, 2010.

المحتوى: