الأمن السيبراني

زينة المزوغي
دكتورة متعاقدة بالمعهد العالي
للدّراسات القانونيّة والسياسيّة بالقيروان،
جامعة القيروان

ملخص

يعتبر الأمن السيبراني مفهومًا واسعًا ومعاصرًا يعاني من عدم وضوح تعريفه نظرًا لاتّساع نطاقه وتعدّد أبعاده التّقنية والتّنظيمية والإستراتيجيّة، الرّامية إلى حماية الشّبكات والبيانات والأنظمة المعلوماتيّة من الهجمات الإلكترونيّة المتنوّعة التي تهدّد الفضاء الرّقمي على الصّعيدين الوطني والدّولي. وقد أدّى تأزّم البيئة السيبرانيّة إلى البحث عن آليات حمائيّة فعّالة تضمن الأمن والاستقرار السيبرانيّ باعتباره أحد الرّكائز الأساسيّة للسّيادة الرّقمية وحماية المصالح الإستراتيجيّة للدّول.

Résumé

La cybersécurité est un concept contemporain aux dimensions technique, organisationnelle et stratégique, visant à protéger les réseaux, les données et les systèmes d'information contre les cyberattaques aux niveaux national et international. La complexité croissante du cyberespace a rendu nécessaires des mécanismes de protection efficaces, considérés comme un pilier essentiel de la souveraineté numérique et de la protection des intérêts stratégiques des Etats.

Abstract

Cybersecurity is a contemporary concept with technical, organizational, and strategic dimensions, aiming to protect networks, and information systems from cyberattacks at both national and international levels. The growing complexity of the cyberspace has made effective protective mechanisms necessary, considered a key pillar of digital sovereignty and the protection of states' strategic interests.

مقدّمة

«لقد رتّبنا حضارة تعتمد فيها العناصر الأكثر أهميّة بشكل كبير، على العلم والتّكنولوجيا». (كارل ساجان) «فلا يمكننا لوم التّكنولوجيا، حينما نرتكب نحن الأخطاء»[1]، حسب مخترع وعالم الحاسوب البريطاني، (تيم بيرنرز لي) Tim[2] .Berners– Lee

يشهد العالم تطوّرا سريعا ومكثّفا لاستعمال تكنولوجيات المعلومات والاتّصالات في جميع المجالات ومن قبل جميع الفئات، لا سيّما القطاع العام، الخاص، والمواطن في أغلب مجالات حياته اليوميّة.

فقد تسارع إيقاع التقدّم التّكنولوجي والتّقني الهائل الذي مثّل النّقطة الأبرز في القطع مع الماضي نحو بداية عصر جديد تبلور خاصة مع ميلاد ثورة جديدة أصطلح على تسميتها «ثورة المعلومات»[3]. وحسب Bill Gates مؤسس شركة

(1) شيماء المرزوقي، «لا تحمِّل التّكنولوجيا أخطاءك»، 14 مارس 2021:
https //www.alkhaleej.ae.

Shaima.author@hotmail.com

(2) تيم بيرنرز لي Tim Berners-.Lee هو اسم دخل التاريخ باعتباره مبتكر شبكة الويب العالميّة، وهي واحدة من أكثر الاختراعات ثورية في العصر الرقمي. لقد كان هذا المهندس البريطاني لاعبًا رئيسيا في تطوّر تكنولوجيا المعلومات، ولا يزال إرثه يؤثر على طريقة تواصلنا وتفاعلنا عبر الإنترنت. إذا تحدثنا عن اختراع شبكة الويب العالميّة، فلا بد أن نتحدث عن تيم بيرنرز لي، مبتكرها. كان هذا الفيزيائي البريطاني المولود في لندن عام 1955 مسؤولًا عن إنشاء لغة HTML وبروتوكول HTTP وعنوان URL، وهي الركائز الأساسيّة للويب الحالي، «تعرف على تيم بيرنرز لي، مبتكر شبكة الويب العالميّة»، https: //polaridad.es

(3) محمّد نجيب بن عمارة، «الحماية القانونيّة للبرامج المعلوماتية»، مجلّة القضاء والتشريع، أكتوبر 1998 ص.65

مايكروسوفت[4] «إنّنا نعيش فترة مثيرة من عصر المعلومات وهي بداية هذا العصر». تسمح طبيعة الإنترنت المفتوحة عبر شبكات التواصل الاجتماعي لكلّ مواطن بأن يعبّر عن أفكاره والاطّلاع على مختلف المعلومات والانفتاح عبر جميع الثقافات المختلفة[5].

إنّ مفهوم المعلوماتية يعدّ حديثا إذ لم يظهر إلاّ مع النصف الثّاني للقرن العشرين وهو يعرف إجمالا بعلم المعالجة العقلانيّة، لا سيّما بواسطة الآلات الأوتوماتيكيّة للمعلومة التي تعرف بأنّها كل «مادة معرفة قابلة لأن تتمثّل في إشارات متعارف عليها من أجل حفظها أو معالجتها أو بثّها والتي تعتبر مرتكزا للمعارف الإنسانيّة ولوسائل الاتّصال في المجال التقني، الاقتصادي والاجتماعي وتردّ المعلوماتية لأعمال الحاسوب الذي يضمّ الأعضاء الضروريّة لعمله المستقلّ، وهو يعمل من خلال التّرابط الشّديد بين وسائله المّادية وبرمجياته من خلال نظام متكامل يدعى النّظام الآلي للمعالجة الإلكترونيّة»[6].

خلقت تكنولوجيا المعلومات والاتّصال نمطا جديدا من العيش داخل المجتمعات، وأفرزت علاقات اجتماعيّة واقتصاديّة جديدة تطوّرت في إطار عالم لامادّي، فضاء مميّزا أطلق عليه تسمية «الفضاء السيبرانيّ». وقد أصبح هذا الفضاء يحتلّ مكانة هامّة في حياة الأفراد، استعملت فيها تكنولوجيا المعلومات والاتّصال الحديثة.

---

(4) بيل غيتس مبرمج حاسوب، ورجل أعمال أميركي، اشتهر كمؤسس لأكبر شركة برمجيات في العالم (مايكروسوفت)، التي أسهمت في خلق «ثورة الحاسوب الشّخصي»، نشر مؤسّس مايكروسوفت رسالة من 7 صفحات تحت عنوان «بدأ عصر الذكاء الاصطناعي»، والتي تحدد وجهة نظره حول مستقبل التقنية. وكتب أن تطوير هذه التكنولوجيا «أمر أساسي مثل إنشاء المعالج الدقيق والكمبيوتر الشخصي والإنترنت والهاتف المحمول»، لقد بدأ عصر الذكاء الاصطناعي، بيل جيتس، ترجمة القاضي طاهر أبو العيد، مستقبل الأمة، نشر في مارس 2023.

https: //ummah-futures.net

(5) عاطف حسن، «الأمن السيبراني حتمية فرضها التطوّر»،

https: //masrafeyoun.eb.gov.eg2022

(6) علي كحلون، «الإطار القانوني للإعلاميّة في تونس»، مجلّة القضاء والتّشريع، جويلية 2005، ص31.

لا يوجد تعريف ثابت لمفهوم الفضاء السيبراني وذلك نتيجة لاختلاف طبيعة ونظام الدّول حيث تمّ تعريفه على أنّه عالم يتداخل مع عالمنا المادّي يؤثّران ببعض بطريقة غير مباشرة ومعقّدة، حيث تعتبر العلاقة أنّها تكامليّة وتحتوي على نتائج ومخاطر سلبيّة. وهناك من وصفه باليد الرّابعة للجيوش وهنالك من يرى أنّه البعد الخامس للحروب وهو يتكوّن من أجهزة الحاسب الآلي وشبكات المعلومات[7].

السيبرانيّة لغة: يعود منشأ كلمة «السيبرانيّ» إلى اللّغة اليونانيّة، وبالذّات كلمة «كبيرنتيك» (Kebrentic) تحمل هذه الكلمة معنى يدمج بين المقصودين: التّوجيه (steering)، والحوكمة (gouvermance) حيث استخدم «نوربرت فينر» (Wiener Norbert)، مصطلح «السيبرانيّة» لأوّل مرة عام 1948، من أجل وصف نظام التّغذية الرّاجعة (Feedbak) الذّي يعمل على الاستفادة من مخرجات الأنظمة في ضبط مدخلاتها والتّحكم فيها، واستقرار أدائها ورأى «فينر» أنّه يمكن تطبيق هذا النّظام على نطاق واسع[8].

الأمن السيبراني أتى من كلمتي (Cyber Security)، وكلمة سيبر لاتينيّة الأصل ومعناها الفضاء المعلوماتي فيصبح المقصود بالأمن السيبراني أمن الفضاء المعلوماتي وهو تعبير أشمل وأعمّ من أمن المعلومات[9]. لذلك يمكن القول بأنّه عبارة عن مجموع الوسائل التقنيّة والإداريّة التي يتّم استخدامها لمنع الاستعمال غير المصرّح به وسوء الاستغلال واستعادة المعلومات الإلكترونيّة ونظم الاتّصالات والمعلومات التي تحتويها بهدف ضمان توافر واستمراريّة

(7) «أثر التّهديدات السيبرانيّة علي الأمن القومي»، مركز أضواء للبحوث والدراسات، 2020، https: //adhwaa.net

(8) سعد علي الحاج علي بكري، «الأمن السيبراني ومعضلة حمايته.. عولمة التّعليم العالي الرّقمي»، جريدة العرب الاقتصاديّة الدّوليّة، العدد 24، 25 أوت 2017، ص24، http: //www.univ-tebessa.dz

(9) أحمد عبيس نعمة الفتلاوي، «الهجمات السيبرانيّة: مفهومها والمسؤوليّة الدّولية النّاشئة عنها في ضوء التّنظيم الدّولي المعاصر»، مجلّة المحقّق الحلي للعلوم القانونيّة والسياسيّة، العدد الرّابع، السنة الثامنة، Echahid Cheikh Larbi Tebessi 2016 University- Tebessa. University. http: //www.univ-tebessa.dz

عمل نظم المعلومات وتأمين حماية وسريّة البيانات الشخصية للمواطنين.

ويعرّف الاتّحاد الدّولي للاتّصالات الأمن السيبراني بأنّه «مجموع الأدوات والسياسات ومفاهيم الأمن وضوابطه والمبادئ التّوجيهية والإجراءات والتّدريب وأفضل الممارسات وآليات الضّمان والتّكنولوجيات التي يمكن استخدامها في حماية البيئة السيبرانيّة وأصول المؤسّسات والمستعملين. وتشمل أصول المؤسسات والمستعملين أجهزة الحوسبة الموصولة بالشّبكة والموظّفين والبنية التّحتية والتّطبيقات والخدمات وأنظمة الاتّصالات ومجموع المعلومات المنقولة و/ أو المحفوظة في البيئة السيبرانيّة»[10].

إذ يتعلّق الأمن السيبراني بتأمين شامل للبيانات المعرّضة للخطر من خلال رفع مستوى تطوير تكنولوجيا المعلومات والاتّصالات وحماية مواقع تخزين المعلومات والبيانات والتقنيات المستخدمة لتأمينها وحمايتها من الفضاء السيبراني الذي عرّفه أيضا المشرّع التّونسي صلب المرسوم عدد 17 لسنة 2023 المتعلّق بإحداث الوكالة الوطنيّة للسّلامة السيبرانيّة بأنّه «فضاء رقمي يربط منظومات المعالجة الإلكترونيّة للمعطيات بشبكات المعلومات والاتّصال ويشمل عناصر ماديّة ولا ماديّة من حواسيب وأنظمة تشغيل وبرمجيّات وشبكات اتّصال ومحتوى رقمي والمستخدمين سواء كانوا مشغّلين أو مستعملين وجميع العمليّات التي تجري باستعمال هذه العناصر»[11].

الأمن السيبراني هو ممارسة حماية الأنظمة والشّبكات والبرامج من الهجمات الرقميّة التي تهدف عادة إلى الوصول للمعلومات الحسّاسة أو تغييرها أو إتلافها أو ابتزاز المال من المستخدمين أو مقاطعة العمليّات التّجارية، وقد وقع تعريفه بأنّه أمن الشبكات والأنظمة المعلوماتيّة، والبيانات، والمعلومات، والأجهزة

(10) إسماعيل زروقة، «الفضاء السيبراني والتّحول في مفاهيم القوّة والصّراع»، مجلّة العلوم القانونيّة والسياسيّة، المجلد 10، العدد1، ص.1016-1031، أفريل 2019، منشور على الرابط التالي: https: //www.asjp.cerist.dz

(11) المرسوم عدد 17 لسنة 2023 المؤرّخ في 11 مارس 2023.ر.ر.ج.ت عدد 26 الصادر بتاريخ 11 مارس 2023، ص 759.

المتّصلة بالإنترنت، وعليه فهو المجال الذي يتعلّق بإجراءات، ومقاييس، ومعايير الحماية المفروض اتّخاذها، أو الالتزام بها لمواجهة التّهديدات، ومنع التعدّيات، أو على الأقل الحدّ من آثارها[12].

في هذا السياق اعتبر فريتشارد كمرر Kemmerer. A Richard الأمن السيبراني «وسائل دفاعية من شأنها كشف وإحباط المحاولات التي يقوم بها القراصنة»[13].

رغم حداثة المصطلح يتّسم الأمن السيبراني بوجود تعارض في تعريفاته، ويتجلىَّ ذلك في رفض بعض الجهات الحكوميّة في عدد من الدّول الاتّفاق على مفردات مشتركة. كما يتغيّر معنى المصطلح عبر الزمن. في الوقت الحاضر تتعامل الدّوائر الحكوميّة العليا في الولايات المتّحدة وعدد من الدّول مع الأمن السيبراني باعتباره تحدّيا رئيسيّا للأمن القومي.

ويرى عدد من الباحثين أنّ عدم وجود تعريف موجز ومقبول على نطاق واسع يلتقط الأبعاد المتعدّدة للأمن السيبراني، من المحتمل أن يؤدّي إلى إعاقة التقدّم التّكنولوجي والعلمي، حيث يتمّ تعزيز النّظرة التّقنية السّائدة للأمن السيبراني مع فصل التخصّصات التي يجب أن تعمل بشكل متضافر لحلّ تحدّيات الأمن السيبراني المعقّدة[14].

إنّ خصوصيّة الفضاء السيبراني المميّز بطبعه اللاّمادي، وبعدم خضوعه فعليّا لسلطة أو سيادة بالمفهوم الكلاسيكي لسيادة الدّولة وإلى تطوّره وتغييره المتواصل، يقتضي وضع حلول تقنيّة وقانونيّة تتناسب مع هذه المميّزات لتضع حدّا أو على الأقلّ لتقلّص من التجاوزات الحاصلة جرّاء سوء استعمال الهواتف الذّكية أو التعسّف في استعمالها للإضرار بحقوق الغير أفرادا كانوا أو مؤسّسات

(12) منى الشقرجبور، «السيبرانيّة هاجس العصر»، المركز العربي للبحوث القانونيّة والقضائيّة، بيروت، 2017، ص25، المركز العربي للأبحاث والدراسات السياسيّة، https: //www.carjj.org

(13) انظر:

Richard A. Kemmerer, Cyber security, University of California Santa Barbara, Department of https: //industry.ucsb.edu, 1Computer Science, 2003

(14) الأمن السيبراني، «المفهوم والتداعيات في السياسة العالميّة»، مقال منشور في أفريل 2021، بمركز الحضارة للدراسات والبحوث على الرابط التالي: https: //hadara.center.com

أو دول، ومن سوء إدارتها أو تصرّف الدّول فيها لما ينجرّ عن الرقّابة المسلّطة من قبل بعضها من قمع للحقوق والحريّات[15].

وقد لعبت الإنترنت دورا أساسيّا في تطوّر هذا الفضاء المميّز لما يتّسم به من حريّة وسرعة في نشر المعلومة، وتجاوز للحدود الجغرافيّة المّادية التي عادة ما تمثّل عائقا للتّواصل والاتّصال. إلاّ أنّ تفشّي استعمال التّكنولوجيات الحديثة في جميع الميادين من تعليم، تجارة، اقتصاد ومعاملات بصفة عامّة، أدّى إلى ظهور إشكاليات قانونيّة جديدة. هذه الإشكاليّات أفرزت فرقا شاسعا بين النّصوص القانونيّة النّافذة والتّطبيق. وأفرزت بالتالي مساسا بالحقوق الأساسيّة للأفراد أحيانا، وتضاربا بين هاته الحقوق في الآن ذاته أحيانا أخرى.

والأنترنت كوسيلة للإبحار في الفضاء السيبراني، أعتبرت إحدى أهمّ الوسائل للتّعبير عن الرّأي. إلاّ أنّ هذه الحرية قد تمسّ من سمعة أو شرف أو كرامة الأشخاص، بما في ذلك من تعدّ على حياتهم الخاصّة. وقد زاد التّطور التّكنولوجي تفاقم التّعقيد القانوني، خاصة أمام ظهور العولمة السّحابية[16]، وما تمثله هذه التّقنية من مخاطر على أمن المعلومات وعلى أمن وسلامة المعاملات البنكيّة والتّجارية. فأضحى الحديث عن ضرورة تحقيق الحماية والأمن في الفضاء السيبراني، من أهمّ الضّروريّات التّي من شأنها أن تعزّز ثقة الأفراد في استعمال آمن لتكنولوجيا الاتّصال والمعلومات. من ذلك مثلا، البحث عن وسائل تقنيّة وقانونيّة لحماية حقوق الملكيّة الفكريّة في الفضاء السيبراني أو

(15) سلمى خالد، التقرير الختامي، «الإنترنت فضاء للحرية ومصدر للإشكاليات القانونيّة»، مخبر قانون العلاقات الدّوليّة والأسواق والمفاوضات DRIMAN، جامعة تونس المنار، منشورات DRIMAN، ص 193.

(16) إن الحوسبة السحابية تعني توفير موارد تقنية المعلومات حسب الطلب عبر الإنترنت مع تسعير التكلفة حسب الاستخدام. فبدلًا من شراء مراكز البيانات والخوادم المادية وامتلاكها والاحتفاظ بها، يمكنك الوصول والاستفادة من الخدمات التكنولوجية، مثل إمكانات الحوسبة، والتخزين، وقواعد البيانات، بأسلوب يعتمد على احتياجاتك، وذلك من خلال جهة موفرة للخدمات السّحابية مثل: Amazon Web Services (AWS)

«ما هي الحوسبة السحابية؟ - خدمات الحوسبة السّحابية وفوائدها وأنواعها»،

Amazon Web Services

https: //aws.amazon.com

مسألة إيجاد حلول قانونيّة لتأمين سلامة المعاملات التّجارية على الإنترنت من خلال تقنيّة المصادقة الإلكترونيّة وما لها من آثار تقنيّة وقانونيّة[17].

وبناء على ذلك تعتبر السّلامة المعلوماتيّة علم «أمن المعلومات» ويقصد به حماية وتأمين كافّة الوسائل المستخدمة في معالجة المعلومات، ومن ذلك توفير الحماية اللاّزمة للمنشأة نفسها والأفراد العاملين بها ونظم التشغيل كأجهزة الحاسوب المستخدمة فيها وحماية برامجها وذلك في إطار جميع مراحل تواجد المعلومة من تخزين ونقل ومعالجة لتحقيق الهدف المنشود وهو التوقّي من الاعتداءات والتهديدات ضدّها[18].

فالسّياسات الأمنيّة مطلب ضروري لمعظم مواقع المنشآت الإلكترونيّة، فهي تلعب دورا هاما في تقليل المخاطر التي قد تتعرّض لها المنشأة وتؤثّر عليها تقنيّا عن طريق تدمير أنظمة المنشأة وخدماتها، أو معنويا وذلك بتشويه سمعتها في حال تسريب إحدى المعلومات السريّة التي تحتفظ بها المنشأة ممّا يؤدّي إلى انعدام ثقة عملائها بها[19].

تتزايد تحديات الأمن السيبراني مع تقدّم التكنولوجيا، خاصة مع تطوّر الذّكاء الاصطناعي. إذ يعد كلا من الذكاء الاصطناعي والأمن السيبراني من صور التطوّر التكنولوجي الهائل الذي نعيشه منذ سنوات، وقد اكتسب هذان المجالان شهرة هائلة في التّكنولوجيا الحديثة نظرا لأدوارهما الحاسمة في تشكيل العالم الرقميّ.

إذ تحمل مشاهد المخاطر المتغيّرة وتطوّر دور الذّكاء الاصطناعي في الدفاع السيبراني دروسا مهمّة جدا عن عملية الدّفاع في وجه الهجمات الإلكترونيّة[20].

(17) فرحات الحرشاني وسامي البسطانجي، «الإنترنت فضاء للحريّة ومصدر الإشكاليّات القانونيّة»، مخبر قانون العلاقات الدّوليّة والأسواق والمفاوضات، منشورات DRIMAN، تونس 2014، ص6.

(18) أشرف الطبري، السّلامة المعلوماتيّة في القانون التّونسي، رسالة لنيل شهادة الماجستير بحث في القانون التّونسي، كلية الحقوق والعلوم السياسيّة بتونس، 2016، ص 3.

(19) أشرف الطبري، السّلامة المعلوماتيّة في القانون التّونسي، رسالة لنيل شهادة الماجستير بحث في القانون التّونسي، كلية الحقوق والعلوم السياسيّة بتونس، 2016، ص 4.

(20) كشفت دراسة علمية للدكتور عادل عوض أستاذ ورئيس قسم الفلسفة جامعة المنصورة، أنّ الجريمة الإلكترونيّة تتمّ عن طريق الحاسوب والإنترنت أو تعرف بجريمة الأذكياء مقارنة بالأجرام

هناك علاقة وثيقة بين الذّكاء الاصطناعي أحد فروع علوم الكمبيوتر، والأمن الإلكتروني أو السيبراني، إذ يتمّ تطوير أنظمة الذكاء الاصطناعي التي يمكن استخدامها لتعزيزه، إلى جانب تنفيذ تدابير أمنيّة لحماية أنظمة الذّكاء الاصطناعي من الاختراق أو التلاعب إذ يتضمن الأمن السيبراني العديد من نقاط البيانات التي يمكن استخدامها للذّكاء الاصطناعي[21].

ولئن وفّرت هذه التّكنولوجيات بيئة رقميّة مترابطة فيما بينها اتّسمت بالمرونة والنّمو السّريع وتحقيق رفاهة لدى المواطن، إلاّ أنّ هذه الميزات لا تخلو من مخاطر تتربّص بالفضاء السيبراني، علاوة على التهديدات من الدّاخل والخارج التي تستهدف الحقوق والحرّيات والأمن القومي.

وهو ما دفع بالإنسان إلى وضع دراسات كثيرة للتنبّؤ بأحداث المستقبل القريب والبعيد ومحاولة التحكّم بأحداث المستقبل وتطوّراته في مجال المعلوماتيّة، خاصة في ظل ظهور أساليب عدة لمحاولة التجسّس على الدّول وذلك لمعرفة خططها الحالية والمستقبليّة والتجسّس على المعلومات السرّية وهو ما يعبّر عنه «بالقرصنة الإلكترونيّة» في الفضاء السيبراني الذي يمثّل تهديدا متصاعدا لأمن الدّول قد يصل إلى حدّ اختراق مجالها الأمني والعسكري، حيث أصبح التطوّر التكنولوجي مرتبطا بالمخاطر الأمنيّة المتزايدة بمعنى أنّه بتطوّر التكنولوجيا يزداد احتمال تعرّض الدّول لهجمات إلكترونيّة مختلفة الأساليب.

وبالتالي فإنّ الدافع الأساسي من وراء هذا البحث الرّاهن هو الأهميّة الكبرى التي يحظى بها الأمن السيبراني، حيث أصبح يشكّل اليوم جزء أساسيّا من أيّ سياسة أمنيّة وطنيّة حيث بات معلوما أنّ الدّول الكبرى كالولايات المتحدة الأمريكيّة، الاتّحاد الأوروبي روسيا، الصين أيضا الدّول العربيّة أصبحوا يصنّفون

التقليدي الذي يميل فيه المجرم إلى العنف، جاء ذلك في بحث بعنوان «دور الذكاء الاصطناعي في الأمن السيبراني»، على هامش المؤتمر الدّولي المنوط بالذكاء الاصطناعي والحد من التغيرات المناخيّة تحت شعار مستقبل أفضل للإنسانيّة، محمّد أيمن، «دور الذكاء الاصطناعي في الأمن السيبراني».. دراسة جديدة بجامعة المنصورة، نشر في سبتمبر 2023،

https: //m-youm7-com.cdn.ampproject.org

(21) الذكاء الاصطناعي والأمن السيبراني، نشر في 29 جانفي 2024، https: //bakkah.com

الأمن السيبراني كأولويّة في سياستهم الدّفاعية. ففي ضوء هذه البيئة المتغيّرة، ثمّة حاجة ملحة لاتّخاذ إجراءات على الصعيدين المحلّي والدّولي لحماية الاستهلاك والخصوصيّة ومجابهة تقنيّة المعلومات ضدّ جميع أشكال الجريمة السيبرانيّة عبر سنّ مجموعة من القواعد القانونيّة الدّولية والمحليّة لحماية الأمن السيبراني[22] كقضيّة ناشئة في حقل العلاقات الدّوليّة.

بخصوص حداثة هذا المجال، هناك تاريخ طويل من التخمينات حول دور التّكنولوجيا الرقميّة في الدّراسات الأمنيّة والتي يعود منشأها إلى حدّ ما مع (Arquilla) و1993 (Ronfeldt's) من خلال مفهوم حرب الإنترنت (netwar) والحرب السيبرانيّة (cyber war). وقد كان هناك تاريخ واسع من الاختبارات النّظرية والأخلاقيّة بشأن المخاوف المتعلّقة بالأمن السيبراني حيث إنّه ومع نهاية الحرب الباردة، حدثت تحوّلات تدريجيّة، ظهرت على مستوى التّفكير في الدّراسات الأمنيّة لأنّ النّظرة الضيّقة المتمركزة حول الدّولة (The narrow state centric way of viewing) كانت ثابتة ودائما ما تؤدي إلى انتقادات حول كيف كان الأمن مفهوما تقليديّا.

وقد سجّل أوّل ظهور للأمن السّيبرانيّ في عام 1970، حيث طرح مشروع الأمن السيبراني في الوسط بعد عدّة عقود من اختراع الحواسيب. إذ كان مجرّد فكرة نظريّة في ذلك الوقت، واستمرّت النّقاشات والتّحليلات خلال فترة السّبعينيات إلى أن ظهر الأمن السيبراني كمفهوم فعلي قابل للتّطبيق، حينما طرح الباحث بوب توماس برنامج كمبيوتر أُطلق عليه اسم (Creeper)، وقد تمكّن هذا البرنامج من التحرّك عبر شبكة (ARPANET)[23].

(22) سعيدة رشاش، مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري، مذكّرة مقدّمة بكليّة الحقوق والعلوم السياسيّة، قسم الحقوق الجزائر سنة 2018،
Echahid Cheikh Larbi Tebessi University- Tebessa. University. http: //www.univ-tebessa.dz)

(23) مواجهة التهديدات السيبرانيّة في عصر الذّكاء الاصطناعي، خطوات دفاعية بتوظيف نظمه المتطوّرة، منشور على الرابط التالي: الشرق الأوسط
https://awssaat.com.

ولكن رغم ذلك ازدادت الهجمات الإلكترونيّة والتّهديدات الجاسوسيّة في فترة الثّمانينات وظهرت مصطلحات جديدة مثل فيروسات الحاسوب (Trojan Horse)، لذا حدّدت وزارة الدفاع الأمريكيّة معايير لتقييم نظام الكمبيوتر الموثوق به عام 1985. ومع ذلك في عام 1986، اختُرقت بوّابة الإنترنت في كاليفورنيا، وتمّ تهكير400 جهاز كمبيوتر عسكري، بالإضافة إلى الأجهزة المركزيّة في مقر البنتاغون، وذلك بهدف بيع المعلومات. وبعدها في عام 1987 انطلق أوّل برنامج تجاري لمكافحة الفيروسات، ثمّ توالت شركات تطوير برامج مكافحة الفيروسات في الظّهور عام 1988، ومنها شركة (Avast)، وكان عمل المكافحة محصورا بالردّ على الهجمات الحاليّة، ويُذكر أنّ عدم وجود شبكة واسعة ساعد على الحدّ من نشر التّحديثات. وشهد هذا العقد تأسيس أوّل منتدى إلكتروني مخصّص لأمن مكافحة الفيروسات، بالإضافة إلى تأسيس مطبعة مكافحة الفيروسات، لحماية بيانات مستخدمي الفضاء السيبرانيّ من أي قرصنة إلكترونيّة إجراميّة، وهو ما مهّد لظهور الأمن السيبراني بعدها[24].

في عصرنا الرقميّ، تتزايد مخاطر التهديدات السيبرانيّة، وتتباين آثارها وانعكاساتها في العالم عامّة، حيث امتدّت هذه التهديدات لتطال مختلف القطاعات سواء العسكريّة، السياسيّة الاقتصاديّة، الاجتماعيّة والثقافيّة مهددّة بذلك الأمن القومي للدّول[25].

وفي ظل التدافع بين تنامي مهدّدات الأمن السيبراني وجهود تحقيقه، هناك دائما يقين واحد يتمثل في أنّ عالم الأمن السيبراني يواجه المزيد من محاولات الاختراق والتهديد التي تتطلّب الاستعداد للتصدّي لها.

(24) الأمن السيبراني Cyber security، العدد 14، أكتوبر 2022 الهيئة العامة لمكافحة الفساد، https: //www.nazaha.gov.kw

(25) اتضح من خلال مؤتمر **أمن المعلومات والأمن السيبراني caisec 23** أنّ تقرير المخاطر العالميّة لعام 2023 أثبت أنّ أهمّ المخاطر التي تواجه الاقتصاد العالمي يأتي من بينها الأمن السيبرانى في المرتبة الرّابعة من بين جميع المخاطر التي تواجه العالم وأبرزها على الأجلين القصير والطويل، فهناك 2 مليارات شخص يستخدمون الإنترنت، يمثلون 22% من العالم، ونحو 2.1 تريليون دولار تجارة إلكترونيّة؛ ستصل إلى 13 تريليون دولار في عام 2027 كما أن ثلث المديرين التنفيذيين تعرضوا لمخاطر هجمات سيبرانيّة.

نظرا للطّابع الكوني للأمن السيبراني، الذي تعدّ تهديداته عابرة للحدود ولا تعترف بالسّيادة الجغرافيّة للدّول فإنّ هذا البحث سيتناول الأمن السيبراني في أبعاده الشّاملة من منظور عام ودولي، من خلال مقاربة تجمع بين البعد الوطني بوصفه قاعدة التّنفيذ والبعد الدّولي باعتباره إطار التّنسيق والتّعاون المشترك. وفي هذا السّياق تتنزّل الإشكاليّة التّالية:

كيف يمكن حماية الأمن السيبراني في مختلف أبعاده من المخاطر التي تهدّده، عبر تطوير آليات حمائية فعالة؟

ومن هنا تبرز الحاجة الضّرورية لمعرفة الأمن السيبراني في مختلف أبعاده كإطار للإحاطة بالمخاطر والتحدّيات المعاصرة (**الجزء الأوّل**) والتطرّق إلى فعالية الآليات الحمائية للأمن السيبراني (**الجزء الثّاني**).

الجزء الأوّل: تعدّد أبعاد الأمن السيبراني كإطار للإحاطة بالمخاطر والتّحديات المعاصرة

لم يعد الأمن السيبراني مفهوما تقنيّا بحتا، بل أصبح إطارا شاملا تتداخل فيه الاعتبارات الأمنيّة، العسكريّة الاقتصاديّة، الاجتماعيّة، القانونيّة، السياسيّة... فمع التحوّل الرّقمي المتسارع واتّساع نطاق استخدام التّكنولوجيا في مختلف المجالات، برزت تحدّيات جديدة جعلت من الضّروري مقاربة الأمن السيبراني من زوايا متعدّدة، تعكس تشابكه مع مختلف مجالات الأمن القومي والتّنمية المستدامة.

وانطلاقا من هذا التّصور يمكن تكييف أبعاد الأمن السيبراني ضمن عنوانين رئيسيّين يعكسان طبيعته المركّبة، حيث سنتناول في فقرة أولى (الأبعاد الإستراتيجيّة للأمن السيبراني)، ثم سنتطرق في فقرة ثانية إلى (الأبعاد التّنظيميّة والتّنموية للأمن السيبراني).

الفقرة الأولى: الأبعاد الإستراتيجية للأمن السيبراني

تشمل الأبعاد الإستراتيجيّة للأمن السيبراني البعدين الأمني والعسكري، إلى جانب البعد السّياسي لما له من ارتباط مباشر بحماية سيادة الدّولة ومصالحها

الحيوية بهدف تحقيق منظومة أمن متكاملة تعمل على الحفاظ على الأمن القومي للدّولة من كل التّهديدات السيبرانيّة.

1 – البعد العسكري والأمني

«إنّ دراسة التّاريخ العسكري، شهدت تغيّرات جذريّة في السّنوات الأخيرة، فلم يعد نهج الطبول والأبواق القديم فعّالا، حيث حظيت عوامل كالاقتصاد والخدمات اللوجستيّة والاستخبارات والتّكنولوجيا بالاهتمام»[26]. (روبرت كاولي وجيفري باركر Robert L. Parker).

مع تطوّر مجال التّقنيات وتزايد اعتماد الدّول على الاتّصالات والشّبكات الإلكترونيّة في إدارة وتوجيه مختلف البنى والمفاصل الحيويّة لمؤسّسات الدّولة، المدنيّة منها والعسكريّة، بدأ في الظّهور بشكل متزايد خطر جديد، تمثّل في إمكانيّة لجوء بعض الفواعل إلى إلحاق الضّرر والأذى بل وحتّى تخريب الدّول عن طريق الفضاء السيبراني، الذّي أصبح يمثّل مصدرا رئيسيّا للمخاطر التي تهدّد الدّول، بعد أن تطوّرت استخداماته لتشمل المجال العسكري، ما جعله أكبر تأثير على أمنها وسلالمة أراضيها. في ظلّ عدم وجود اتّفاق واضح بين الفضاء السيبراني واستخداماته المشروعة، مع تزايد حدّة الصراعات الجيوسياسيّة[27]. بسبب انتشار التجسّس الإلكترونيّ والجريمة السيبرانيّة، حيث ساعد على خلق بيئة دوليّة مضطربة وغير مستقرّة.

إنّ فكرة الصّراع والحرب تقوم من بدايتها لنهايتها على المعلومات، فسبب الحرب ربّما معلومة خاطئة أو صحيحة عن خصم أو صديق أو جار، وبدأ الحرب يتمّ بناء على معلومات فالقائد المزوّد بمعلومات جيّدة عن نفسه وعن عدوّه يكون بين يديه ميزة قويّة لمعرفة مخطّط العدوّ واستراتجيتّه، لكن لم يكن لديه نظام آلي لمعالجة هذه المعلومات، إذ ظلّ التّخاطب العادي هو أبسط وأكثر وسائل

(26) https: //defense.tn/category/histoire» مجلّة التأريخ العسكري» عدد11 نوفمبر 2022.
(27) سالم سالم صابر، «انعكاسات البعد العسكري للفضاء السيبراني على الجغرافيا السياسيّة للدّولة»، العدد 17 السداسي الأوّل 2022، فيلي: ///U/ :C، البعد العسكري للفضاء السيبراني على الجغرافيا السياسيّة للدّولة

الاتّصال شيوعا لفترات طويلة، إلى جانب قرع الطبول واستخدام الإشارات المتّفق عليها وغير ذلك[28].

تطوّرت بدايات الأنترنت في بيئة عسكريّة، بشكل أساسيّ، لتضاف إليها فيما بعد البيئة الأكاديميّة المتمثّلة في أبحاث تخدم تطوير القدرات العسكريّة، والإنجازات العلميّة التي تحافظ على تفوّق بلد آخر.

تتجلّى خطورة الهجمات السيبرانيّة، والتجسّس والسّرقة والاختراق التي ترجمت ماديا، سواء باندلاع صراع مسلح لاحق، كالذي وقع بين روسيا وجورجيا، أو بانقطاع الاتّصال بالإنترنت في إستونيا، بين الدّولة والمواطنين والتشويش على الإدارات الحكوميّة، كما وجّه خبراء أمريكيين خطابا مفتوحا إلى الرئيس «جورج بوش» (George Bush. W) في سبتمبر 2007 محذّرين إيّاه من خطر الهجمات السيبرانيّة على البنية التحتيّة للخدمات الصحيّة والنّقل...[29].

يكمن الحفاظ على الوحدات العسكريّة في التّواصل عبر الشبكات العسكريّة، ممّا يسمح بتبادل المعلومات والأوامر وتدفّقها وإصابة الأهداف عن بعد، إلاّ أنّها تمثّل كذلك نقطة ضعف، خاصّة إذا لم تكن مؤمّنة جيّدا من الاختراق، الذي قد يؤدي إلى تدمير قواعد البيانات العسكريّة، أو قطع الاتّصال بين القيادة والوحدات العسكريّة، فضلا عن إمكانيّة التّحكّم في بعض الأسلحة وخروجها عن السّيطرة (طائرات بدون طيّار، صواريخ موجّهة، أقمار صناعيّة)... (ومنها ما يتعلّق بالأسلحة المستخدمة في الحروب الحديثة وهو نموذج (الصّاروخ كروز)[30].

(28) جمال محمّد غيطّاس، «أمن المعلومات والأمن القومي»، مرجع سابق الذكر، ص63.

(29) سعيدة رشاش، مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري، مذكرة مقدمّة بكلية الحقوق والعلوم السياسيّة، قسم الحقوق الجزائر، سنة 2018.
University.Tebessa -University Tebessi Cheikh Larbi Echahid
http: //www.univ-tebessa.dz

(30) جمال محمّد غيطاس «أمن المعلومات والأمن القومي»، مرجع سابق الذكر ص 65.
«يفترض أن ينطلق الصاروخ كروز من موقع معين كسطح سفينة بعرض البحر أو طائرة تحلق في الجو ليتخذ طريقه إلى هدف محدد من نقطة الانطلاق إلى نقطة الوصول وذلك بتزويده بقدر من المعلومات والبيانات عبر وجود شرائح إلكترونيّة توضع داخل الصاروخ لكي تخزن عليها المعلومات والخرائط التي تحمل موقع الهدف وأوامر التوجيه وتحديد المسار، وهنا تتدخل

وهنا تكون صناعة الاتّصالات وخطوط الاتّصالات قد دخلت طرفا في المعادلة ليصبح لدينا محتوى معلوماتي رقمي دائم التّوليد والتّدفق والاستخدام لحظة بلحظة قبل وأثناء إطلاق الصّاروخ وحتى وصوله لهدفه، لكن إذا ما تمّ فقدان السّيطرة على الصّاروخ أو تعطيل في البيانات فإنّ ذلك قد يؤدّي حتما إلى كارثة إنسانيّة بامتياز. وفي ظلّ تطوّر وتغلغل تكنولوجيا المعلومات والاتّصالات لم يعد الخطر يقتصر على الوسائل والمعدّات الحربيّة المبرمجة على غرار الطّائرات بدون طيّار أو الصّواريخ مثل ما رأينا صاروخ كروز، بل حتى الفيروسات أصبحت تشكّل تهديدا للأجهزة الأمنيّة والعسكريّة[31].

ويعتبر فيروس ستاكسنت Stuxnet بداية استعمال القوّة السيبرانيّة لتدمير البنيّة المّادية (هاجم حواسيب أجهزة الطرد المركزي الإيرانية).

ففي عصر تتسارع فيه وتيرة التطوّرات التقنيّة، أصبح الأمن السيبراني يشكّل أحد أهمّ الرّكائز في الاستراتيجيّات العسكريّة حول العالم، فمن المتوقّع أن يؤثّر الاعتماد العالي لحلول التخزين السّحابية على نموّ سوق الأمن السيبراني العسكري. كما أن الزّيادة في الاستثمارات التي تقوم بها مختلف الحكومات للحدّ من تهديد الهجمات السيبرانيّة والتأكّد من أنّ مستويات أفضل من الحلول

صناعة الإلكترونيات ولكي تعمل هذه المعلومات طبقا للأوامر المطلوبة لا بد من برمجتها بشكل معين، وهنا لابد من وجود برنامج معلومات متخصص يقوم بذلك، ومن ثم لابد أن تتدخل صناعة البرمجيات، ولكي يعمل البرنامج على الشريحة لا بد من وجود عقل إلكتروني دقيق يقوم بتشغيل البرنامج ومعالجة البيانات، وهنا تتدخل صناعة المعالجات الدقيقة السائدة في تصنيع الحاسبات، لأننا في الحقيقة نحتاج هنا إلى ما يشبه حاسبا آليا دقيقا محدد الوظيفة في رأس الصاروخ. وإذا انطلق الصاروخ وهو محمل بكل هذه الإمكانيات فهذا لا يكفي لتوظيف ما لديه من معرفة بشكل يتيح له الوصول بدقة للهدف، لأنه لا يزال محتاجا لمن يحدد له مكانه بدقة في كل لحظة من لحظات رحلته إلى الهدف لكي يعرف أنه في المسار السليم، وهذا الأمر يتطلب أن يتعاون عقله الإلكتروني الدقيق وما تحتويه ذاكرته من معلومات وخرائط مع طرف خارجي لديه القدرة على تحديد المكان، والطرف الخارجي هنا هو نوعية من الأقمار الصناعية التي تدور حول الأرض على مدار الساعة وتستطيع تحديد موقع أي هدف يتحرك على الأرض بطريقة لحظية والتي يمكن للصاروخ أن يكون على اتّصال دائم بها ويتلقى منها معلومات تحدد موقعه لحظة بلحظة حتى الوصول للهدف».

(31) منى الأشقرجبور، «السيبرانيّة هاجس العصر»، المركز العربي للبحوث القانونيّة والقضائيّة، 2017، بيروت، ص25، المركز العربي للأبحاث والدراسات السياسيّة، https: //www.carjj.org.

الأمنيّة من المتوقّع أيضًا أن تؤدّي إلى ازدهار نموّ سوق الأمن السيبرانيّ العسكريّ[32].

مع تزايد التّهديدات الإلكترونيّة وتعقيدها، تتّجه الأنظار نحو كيفيّة تحصين المؤسّسات العسكريّة لحماية البيانات والبنى التحتيّة الحيويّة.

تنبع أهميّة الأمن السيبراني في هذا البعد من خطورة الهجمات السيبرانيّة والاختراقات التي تؤدي إلى نشأة الحروب والصراعات المسلحة، واختراقات أنظمة المنشآت النووية، وما قد يحدث عنها من تهديدات لأمن الدّول[33]. إذ تواجه المؤسسات العسكريّة في العالم العربي تحدّيات متزايدة في مجال الأمن السيبراني، تتراوح بين الهجمات الإلكترونيّة المعقّدة وحروب المعلومات. فالاستثمار في التّقنيات المتقدّمة وتدريب الكوادر البشريّة أصبح ضروريّا لضمان مواكبة أحدث التّهديدات والتّكتيكات السيبرانيّة[34].

وفي ضوء ذلك، يمكن القول أنّ دور التّكنولوجيا والمعلومات والاتّصالات داخل الجيوش والمؤسّسات العسكريّة أصبح قريب الشّبه بوضع الجهاز العصبي داخل الجسم البشري، أي أنّها تضطلع بأن توفّر للمؤسّسة العسكريّة أيّا كان مستواها ونوعيتها منظومة قادرة على تداول المعلومات بغاية السرعة والكفاءة،

(32) سوق الأمن السيبراني العسكري مجزأ بسبب وجود لاعبين مختلفين يتطلعون إلى الحصول على حصص سوقية تنافسية. بعض اللاعبين البارزين في السوق يتكونون من:
شركة BAE Systems plc، وTHALES، وشركة Lockheed Martin وغيرها، Northrop Grumman Corporation وشركة، General Dynamics Corporation وشركة، Corporation وقامت هذه الشركات بتوسيع تواجدها في مناطق مختلفة لتقديم خدمات مرنة تتعلّق بالأمن السيبراني لمختلف أفراد الدفاع في جميع أنحاء العالم.
ومن المتوقع أن تزداد جاذبية السوق مع زيادة الإنفاق الدفاعي بالإضافة إلى زيادة الحاجة إلى تدابير الأمن السيبراني المتقدمة لمواجهة التهديد السيبراني المتزايد في جميع أنحاء العالم. سوق الأمن السيبراني العسكري - النمو والاتّجاهات وتأثيرCOVID-19 والتوقعات (2001 – 2005).
https://www.mordorintelligence.com/ar/industry-reports/militarycybersecurity-market

(33) عاطف حسن، «الأمن السيبراني حتمية فرضها التطوّر»،
https://masrafeyoun.eb.gov.eg2022

(34) حالة الأمن السيبراني في المجال العسكري»، 2023/12/29، LinkedIn · ObaDa HaTTab

وقادرة على الاستجابة السّريعة للطّوارئ والخروقات الأمنيّة. إذن نحن الآن أمام مؤسّسات عسكريّة وجيوش تلاحمت بعمق وبشكل حيوي مع تكنولوجيا الاتّصالات والمعلومات وأسند إليها القيام بوظيفة (الجهاز العصبي) الذي تستخدمه في الإحساس والإبصار والسمع والتفكير وإدارة علاقاتها الدّاخلية والخارجيّة وتنفيذها لمهامها في كلّ الأوقات سلما وحربا. ويأخذ هذا الجهاز صورة المنظومة أو النظام الرّقمي الذي يتألّف من ملايين الوحدات الطرفية المتنوّعة الأشكال والأحجام والوظائف، وآلاف من خطوط الاتّصالات السّريعة العاملة بتكنولوجيّات مختلفة ومئات من المراكز الرّئيسيّة المسؤولة عن استقبال المعلومات واستخدامها في التّفكير واتّخاذ القرارات[35].

لو نظرنا إلى المحتوى المعلوماتي الأمني الذّي تتعامل فيه أجهزة الأمن الدّاخلي سنجد حالته لا تختلف عن حالة المحتوى المعلوماتي المتداول بالمؤسّسات العسكريّة من حيث الانتقال شبه الكامل من الشّكل الشّفهي والورقي الذّي كانت له الهيمنة خلال الفترات الماضية إلى المحتوى المعلوماتي الرّقمي الذي يتزايد ويتضخّم مع الوقت بمعدّلات متسارعة فارضا حقائق جديدة تتطلّب اختلافا كبيرا في طبيعة سياسات أمن المعلومات المطلوبة حاليا ومستقبلا. حيث أصبح من الشّائع أن تعمد وزارة الداخليّة إلى إنشاء شبكات معلوماتيّة رئيسيّة تعمل على مستوى الوزارة ككل وتكون بمثابة القناة الرئيسيّة التي يجري من

(35) جمال محمّد غيطاس، «أمن المعلومات والأمن القومي»، مرجع سابق الذكر، ص 75.
«إذ يؤدّي مثلا استخدام التّشويش الرّاداري إلى شلّ قدرة العدوّ على الاتّصال أثناء تنفيذ هجوم جوّي، وتقوم به بعض الطّائرات المخصّصة لذلك، حيث تعيق الاتّصال بين محطّات الرّادار ومراكز القيادة والسّيطرة ومنصّات الصّواريخ، وهو ما يسمح للطّائرات المهاجمة باختراق المجال الجوّي للعدوّ.
بينما يتمّ استخدام الموجات الكهرومغناطيسيّة للتّشويش على المتفجّرات، التّي يتّم تفجيرها عن بعد، لمنع استخدامها ضدّ القوات البرّية أثناء الهجوم. مثالا عن ذلك، نظام التّشويش الرّوسي «بوريس أوغليبسك 5»، واحدا من أهم أنظمة الحرب الإلكترونيّة الرّوسية، ويتم استخدامه للتشويش على الاتّصالات بالأقمار الصناعيّة، وموجات الراديو، وكان له دورا فعّالا في شرق أوكرانيا، حيث عطّل استخدام الدرونز ضدّ القوات الرّوسية بالتشويش على نظام الملاحة «جي بي إس»، الذّي كانت تستخدمه. والنظام الثّاني هو «ماسكفا 3»، الذّي يمكّنه البحث عن مصادر الموجات الإلكترونيّة، في مدى 200 كم، ويعمل على كل التردّدات، ويمكن استخدامه في عمليات جمع المعلومات الاستخباراتيّة، والتشويش عند الحاجة، كما يوجد أنظمة أخرى عديدة منها نظام «كراسوخا 2» تحليل الموجات الرادارية، والتشويش عليها».

خلالها تداول المعلومات الرقميّة. فشبكات وزارة الداخليّة هي في الغالب شبكة عنكبوتيّه مترابطة من الاتّصالات والحاسبات ونظم المعلومات والبرمجيّات والتّطبيقات وقواعد البيانات وغيرها، إذ تعمل كشبكة لنقل وتبادل المعلومات من أجل دعم العمليات الأمنيّة وهذا يتطلّب آليات وسياسات مختلفة لتأمينه وحمايته من الهجمات السيبرانيّة[36].

خاصّة في ظلّ تنامي الإرهاب الإلكتروني كهاجس يخيف العالم الذّي أضحى عرضة لهجمات الإرهابيّين عبر الإنترنت، إذ يمارسون نشاطهم التّخريبي من أيّ مكان في العالم، وتتفاقم هذه المخاطر بمرور كل يوم لأن التّقنية الحديثة وحدها غير قادرة على حماية النّاس من العمليات الإرهابية الإلكترونيّة، ولقد سعت العديد من الدّول إلى اتّخاذ التّدابير والاحترازات لمواجهة الإرهاب الإلكتروني والحدّ من آثاره الجسيمة على الأفراد والمنظمات، الأمن القومي والسيادة الوطنيّة للدول[37]. إذ يتمّ استخدام الفضاء الإلكتروني في الإرهاب بصورة غير مباشرة عن طريق تسهيل عملية تنفيذ العمل الإرهابي من خلال توفير المعلومات والحصول على التّمويل. وكذلك استخدامه لنشر الفزع والرعب وبثّ الكراهيّة، باستعمال أدوات يصعب الفصل بينها، بمعنى أنه قد يتمّ اعتمادها في عمليّة واحدة.

حيث يتمّ الاختراق إلكترونيّا لتغيير محتوى تلك المعلومات أو سرقتها أو تعطيل الموقع عن العمل والسّيطرة عليه بشكل كامل، وبعد نجاح اختراق الموقع يضع المهاجمون رسائل فيه تعلن اختراقه. فالفضاء الإلكتروني له تأثير هائل على الرأي العام العالمي لأنّه يخاطب ملايين المستخدمين للشبكة العنكبوتيّة من شتى أنحاء العالم بوسائل مختلفة: «الصّوت- الصّورة- النّص»، وبالتّالي أيّ جماعه أو منظّمة يمكن لها إنشاء مواقع إلكترونيّة تروّج أفكارها وتنشرها في مختلف أنحاء العالم[38].

(36) جمال محمّد غيطاس، «أمن المعلومات والأمن القومي»، مرجع سابق الذكر، ص 79.

(37) رحمة قاسمي، كريمة بوخروبة، (الإرهاب الإلكتروني) التحديات والمواجهة، 44-25-0200 https: //dspace.univbba.dz/hand

(38) ورقة بحثية حول واقع الإرهاب في تونس «مركز الدراسات الإستراتيجية والدبلوماسية».www csds-center.com علي عدنان الفيل «الإجرام الإلكتروني منشورات زين الحقوقية، العراق، طبعة 2011، ص 84.

لقد نجحت العديد من الحكومات في استخدام تقييم تقنيات متطوّرة للتّجسس من خلال الشبكة العنكبوتية على الدّول أو المنظّمات ومراقبة المعلومات التي يتم تداولها حول العالم. حيث يوجد العديد من الأساليب التي تستخدم في التّهديد عبر تلك الشّبكة، وتتنوّع الأساليب بين تهديدات باغتيال شخصيات سياسيّة، تهديدات بتفجيرات في مراكز سياسيّة أو هيئات حكوميّة، أو التهديد بإطلاق الفيروسات) فيروسات الحاسب الآلي بسرعه كبيرة عن طريق شبكه الإنترنت وذلك يرجع إلى عدد الملفات الهائل التّي يتمّ تبادلها بين مستخدمي الشبكة العنكبوتية، وتتمثّل أضرارها في فقد الملفّات المخزّنة وتحطيم نظام التّشغيل وتدمير أنظمة المعلومات بالكامل[39].

أدّى الفضاء الإلكتروني إلى تحوّل الإرهاب كتهديد عالمي وجريمة عابرة للحدود القوميّة من حيث النّشاط والتّمويل والأعضاء وتصعد نشاط الجماعات الإرهابيّة عبر الفضاء الإلكتروني وتعزيز بعدها العالمي وتم استخدام المنجزات التّكنولوجيّة في ممارسة الإرهاب، والتي استطاع الإرهابيون من خلالها تحقيق أضرار غير متوقعّه وهائلة تتجاوز التّهديدات التي تمثلّها الدّول لبعضها البعض[40].

حيث، يتّسم الفضاء الإلكتروني باعتباره وسيلة إعلام عالميّة بالعديد من المزايا التي تجعله عنصر جاذب للإرهاب حيث يتميّز بانخفاض التّكلفة، وضعف الرّقابة وتنوّع وسائله وانتشاره وتخطّيه للحدود وقدرة الأفراد على التّأثير فيه، ومن ثم يستخدم الإرهابيّون الفضاء الإلكتروني في التّأثير على الرّأي العام وتجنيد أعضاء جدد من مختلف أنحاء العالم وتمويلهم، لبثّ رسالتهم والوصول إلى أكبر عدد ممكن من الجمهور وشنّ حرب نفسيّة ضدّ الأعداء والدّعاية. هذا الفضاء الإلكتروني يمثّل منبرا للجماعات الإرهابيّة يستخدم في نشر رسائل الكراهيّة والعنف والاتّصال ببعضهم البعض وبمؤيّديهم والمتعاطفين معهم، وترهيب الأعداء عن طريق الأفلام المرعبة التي تنشر عن إعدام الرّهائن والأسرى

(39) ورقة بحثية حول واقع الإرهاب في تونس «مركز الدراسات الإستراتيجية والدبلوماسية» www.csds-center.com علي عدنان الفيل، «الإجرام الإلكتروني»، مرجع سابق الذكر، ص 84.
(40) علي عدنان الفيل، الإجرام الإلكتروني، مرجع سابق الذكر، ص 85.

ومختلف العمليات الإرهابيّة التي يرتكبونها ضدّ أعدائهم. ولعب ذلك دورا كبيرا في تضخيم الصّورة الذّهنية عن حجم وقوّة تلك المجموعات، وعملية التّزاوج بين الإرهاب والإنترنت مثّلت سلاح ذو حدّين حيث يتمثّل الجانب السلبي في أنّها وسيلة لنشر الرعب من خلال نقلها للعمليات الإرهابيّة، حتى تعمل على إثارة الرّأي العام ولفت انتباهه إلى وجود ظاهرة الإرهاب[41].

وقد تحمل الهجمات السيبرانيّة[42] سمات عمل إرهابي بما في ذلك الرّغبة في زرع الخوف دعما لأهداف سياسيّة أو اجتماعيّة. ومن بين الأمثلة على الهجمات السيبرانيّة ما وقع في إسرائيل في جانفي 2012 من استهداف لعدّة مواقع شبكيّة إسرائيليّة ذات قيمة رمزيّة، مثل موقعي سوف تل أبيب للأوراق الماليّة وشركة الطيران الوطنيّة، وكشف غير مصرّح به عن تفاصيل البطاقات الائتمانيّة والحسابات البنكيّة لآلاف من مواطني إسرائيل[43].

إذ تعتمد الجماعات الإرهابية في استقطابها للأمنيّين والعسكريّين طريقتين، الأولى تعتمد على «الدّمغجة» وتبنّي الأفكار الجهاديّة، والثّانية على «الإغراء بمبالغ ماليّة» مقابل تقديم خدمات تتمثّل في تسريب أسرار الثّكنات والدّوريات القارّة والمتحرّكة وجميع المعلومات عن المداهمات وكشف مخطّطات أمنيّة وعسكريّة، كما يمكن لهؤلاء أن يسهّلوا على الجماعات الإرهابيّة استهداف

(41) المركز الديمقراطي العربي للدراسات الاستراتيجيّة والسياسيّة والاقتصاديّة، «أثر الإرهاب الإلكتروني على تغيير مفهوم القوة في العلاقات الدّوليّة، دراسة حالة، تنظيم الدّولة الإسلاميّة»، 24/07/2016،
http: //démocratie.de/?p=34528

(42) ويقصد بالهجمات السيبرانيّة، استغلال الشبكات الحاسوبية عن عمد باعتبارها وسيلة لشنّ هجوم. وتهدف هذه الهجمات عادة إلى تعطيل النّظم التي تستهدفها. وتتضمّن تلك الأهداف نظم الحاسوب والخواديم وبنيتها التحتية الأساسيّة، وذلك عبر استخدام الاختراق الحاسوبي التقنيات المتقدمة للتهديد المستمر أو فيروسات الحاسوب أوّل البرمجيات الضّارة أوّل الإغراق، أو غيرها من وسائل الدخول غير المصرح به أو ذي الأهداف الضارة. استخدام الإنترنت في أغراض إرهابية، مكتب الأمم المتحدة المعني بالمخدرات والجريمة، نيويورك 2013،
http: //www undoc.org/documents/terrorisme/publications.pdf

(43) استخدام الإنترنت في أغراض إرهابية، مكتب الأمم المتحدة المعني بالمخدرات والجريمة، نيورك 2013،
http: // www undoc.org/documents/terrorisme/publications.pdf

بعض الدّوريات أو العناصر الأمنيّة والعسكريّة أو استدراج زملائهم فضلا عن إمكانيّة تدخلهم لتسهيل تمرير شحنات من الأسلحة والأدوية والمواد الغذائيّة والعناصر الإرهابيّة والمفتّش عنهم من وإلى المعسكرات الإرهابيّة[44]. كما تتمثّل الخدمات التي يقدمها الأمنيين في مدّهم بقائمات لأسماء الإطارات الأمنيّة وعناوين منازلهم ومواقيت التحرّكات الأمنيّة والتّعزيزات، فضلا عن قائمات للمقرّات الأمنيّة وصور لها من الداخل ورسوم للثّكنات وهيكلة التّشكيلات الأمنيّة والعسكريّة وعددها[45].

إنّ المشكل الأهمّ في الخطر الإرهابي، هو عملية الاستقطاب والاستمالة في كثير من الفضاءات، والتي عادة ما تجري عبر شبكة الإنترنت وفي المؤسّسات التربوية والمساجد[46].

وبالتّالي هذا الواقع لم يكن كلّه فرصا ومميّزات بل أفرز تحدّيات جديدة أمام المؤسّسات العسكريّة والأمنيّة تمثّلت في التصدّي للهجمات السيبرانيّة وما ترتّب عنها من أضرار فادحة تعلّقت بالأمن والدّفاع وطالت حتى المجال السياسي للدّول.

2 – البعد السياسي للأمن السيبراني

تتمثّل الأبعاد السياسيّة للأمن السيبراني، بشكل أساسي في حقّ الدّولة في حماية نطاقها السياسي، كيانها، ومصالحها الاقتصاديّة، التي تعني حقها وواجبها في السّعي إلى تحقيق رفاه شعبها في وقت تؤثر التقنيات في موازين القوى داخل المجتمع نفسه.

(44) فتحية سعادة، «القضاء يصدر أحكامه في قضية اغتيال الشهيد شكري بلعيد»، 28 مارس 2024. جريدة المغرب https://ar.lemaghreb.tn

(45) النشرة الإلكترونيّة لجريدة الجمهوريّة: هكذا استقطبت الجماعات الإرهابية الأمنيين والعسكريين نشر في 2 جوان 2015،

http://www.jomhouria.com/art32962

(46) النشرة الإلكترونيّة لجريدة الجمهوريّة: هكذا استقطبت الجماعات الإرهابية الأمنيين والعسكريين نشر في 2 جوان 2015،

http://www.jomhouria.com/art32962

أصبح من الواضح بحلول منتصف العقد الأوّل من القرن 21 أنّ «الفضاء السيبراني» الذّي تم إنشاؤه عبر شبكة الإنترنت له تأثيرات هائلة في الديناميكيات والأنماط الأوسع للسياسة الدّوليّة، وبات مفهوم السياسة السيبرانيّة يشكّل أحد مجالات البحث الأكاديمي، حتّى أضحى الطّيف السيبراني جزءا لا يتجزّأ من الأمن القومي، ودخل في تغيير شكل الحروب وتقنياتها وأساليبها بسبب تغيّر طبيعة تهديداته وإلحاق الضّرر بالمؤسّسات والمراكز الحيويّة والإستراتيجيّة للدّول. فالفضاء السيبراني يؤثر في مختلف مجالات الحياة ومنها المجال السياسي حيث يسهم -عبر أدواته المختلفة- في إعادة رسم المشهد السياسي المحلّي والعالمي، ويعمل على إعادة تشكيل الوعي والإدراك السّياسي للأفراد والمجتمعات.

إذ بإمكان المواطن، أن يتحوّل إلى لاعب أساسي، في اللّعبة السياسيّة، كما أصبح بإمكانه الاطّلاع، على خلفيات ومبرّرات القرارات السياسيّة، التي تتّخذها حكومته، عبر الكمّ الهائل من المعلومات، التي يمكنه الوصول إليها، أو التي يمكن أن توزّع وتنشر على الأنترنت وبقية الأجهزة التي توصل به. بالمقابل لا يتوانى العاملون في الشأن السياسي عن الإفادة ممّا تقدمه هذه التّقنيات، للوصول إلى أكبر شريحة ممكنة من المواطنين، والتّرويج لسياساتهم في العالم، وغني عن البيان مدى التّأثير الذّي يتركه هذا الأمر، بغضّ النّظر عن صحّة السياسات، والمبادئ والمواقف، التي يروّج لها، فقد استخدم أوباما، مثالا، الشّبكات الاجتماعيّة بشكل كثيف، خلال حملته الانتخابيّة، كما تركت التّسريبات، آلاف الوثائق الدبلوماسيّة السريّة، عبر الويكيليكس، أثرا سلبيا على العلاقات بين الدّول، وعلى مصداقيته[47].

ضمن هذا السياق، يعدّ التدخّل الرّوسي السيبراني في الانتخابات الأمريكيّة أبرز دليل على ضرورة وأهميّة الأمن السيبراني في بعده السياسي، إضافة إلى التّسريبات للوثائق الحسّاسة والاختراقات التي غالبا ما تؤدي إلى أزمات دبلوماسيّة بين الدّول. كما أنّ الفضاء السيبراني أصبح بيئة خصبة للحملات الانتخابيّة والدّعاية لمختلف الفاعلين الدّوليّين. ويتجلّى البعد السياسي في مسؤوليّة الدّولة وسيادة الدّول:

(47) د. فارس العمارات، إبراهيم محمّد الحمامصة، «الأمن السيبرانيّ المفهوم وتحدّيات العصر»، 2022 books.google.tn https: //books.google.tn › books

* مسؤوليّة الدّولة: تقع على عاتق الدّولة مسؤولية كبيرة لتحقيق الأمن السيبراني، حيث لا ينبغي لعمل الدّولة أن يقتصر على مجرّد تعزيز وتشجيع البحث والتّطوير في مجال الأمن، وإنّما يجب أن يتعدّى ذلك إلى تعزيز ثقافة أمنيّة، ومن الضّروري على المستوى الاستراتيجي تأمين إدارة الوقاية، والإبلاغ وتقاسم المعلومات والإنذار وزيادة الوعي بأفضل الممارسات في مجال الأمن وإدارة المخاطر.

* سيادة الدّول: تتعارض الرّغبة في إتّباع البساطة والفعالية في الأمن، مع تعقّد الاحتياجات والبيئات، حيث يخلق هذا الاتّجاه درجة عالية من التّبعية والمخاطر الرئيسيّة للأمن وعلى الدّول أن تحاذر من أن تصبح مستهدفة وللحكومات دور في تقليل مدى خطورة التعرّض للهجمات السيبرانيّة والبحث عن الحلول الأمنيّة المناسبة[48].

لقد ساهمت الهيمنة السيبرانيّة في كافة التعاملات، على خلق بيئة تهديد لأمن وسلم الدّول. إنّ الجانب الآخر لهذا التطوّر، كشف عن خطر هائل، يهدّد الأفراد والشّركات والدّول على حدّ سواء. ذلك أنّ الخطر الذّي يتمثّل في الهجمات السيبرانيّة، لا تقلّ آثارها عن تلك الآثار التي تخلّفها النّزاعات المسلّحة التقليديّة. بل إنّها تعمل على تقويض الاستقرار الاقتصادي والسياسي، ممّا يهدّد بتوتّر العلاقات الودّية الدّولية[49]. فلئن وفّرت التّكنولوجيات بيئة رقميّة مترابطة فيما بينها بالمرونة والنّمو السّريع وتحقيق رفاهة لدى المواطن، إلاّ أنّ هذه الميزات لا تخلو من مخاطر تتربّص بالفضاء السيبراني، علاوة على التّهديدات من الدّاخل والخارج التي تستهدف الحقوق والحريات والأمن القومي.

يعتبر الأمن السيبراني حقل افتراضي يعتمد على أجهزة الحاسوب والشّبكات وقواعد المعلومات المخزّنة حيث يتّصف حاليا بأنّه عصر رقمي أي يعتمد على

(48) فارس محمّد العمارات، إبراهيم الحمامصة، الأمن السيبرانيّ: المفهوم وتحدّيات العصر، مرجع سابق الذكر.

(49) محمّد ربيع أحمد حسين، «الهجمات السيبرانيّة واستخدام القوّة في القانون الدّولي المعاصر»، كلية الحقوق - جامعة بنها، مقال منشور بمجلّة العلوم القانونيّة والاقتصاديّة، على الرابط التالي https: //jelc.journals.ekb.eg/article_283442.htm

التّكنولوجيا ليتمّ تنفيذ هذه الهجمات، وقد يصعب ملاحقة السبب الرّئيسي لمن قام بهذه الهجمات وتحديد هوية الشّخص، إذ يعرف الهجوم السيبراني[50] بأنّه الاستغلال المتعمّد لأنظمة الحاسب الآلي والشّبكات والجّهات التي يعتمد عملها على تقنية المعلومات والاتّصالات الرّقمية بهدف إحداث أضرار[51].

الفقرة الثّانية: الأبعاد التّنظيمية والتّنموية للأمن السيبراني

تتضمّن الأبعاد التّنظيمية والتّنموية للأمن السيبراني البعدين الاقتصادي والاجتماعي، إلى جانب البعد القانوني لما يمثّلونه من إطار مؤسسي وتشريعي يضمن إدارة الفضاء الرّقمي وتنميته في ظلّ احترام قواعد الأمن وحماية الحقوق والحّريات.

1 – البعد الاقتصادي للأمن السيبراني

على المستوى الاقتصادي، ساعدت تكنولوجيا المعلومات والاتّصالات على الانتقال السّريع نحو الاقتصاد الرّقمي المبني على المعرفة، ودخلنا بذلك للعصر الرقمي، إذ يتمّ استخدام البرمجيات والتطبيقات الذّكية لتحقيق نجاحات متعدّدة في ريادة الأعمال والإدارة، بالإضافة إلى تزايد استخدام الابتكارات التّكنولوجيّة في قطاعات اقتصاديّة حيويّة كالطّاقة، السّياحة، الخدمات الماليّة والمصرفيّة [52].

أساسا للمعاملات التّجارية، الماليّة والاقتصاديّة، تستعمل الحواسيب في تسيير وتطوير الصناعات وتحريك الاقتصاد، إذ أصبح الكلّ مترابطا عبر شبكات الكمبيوتر، ممّا يستدعي الحديث عن أهميّة تحقيق الأمن السيبراني في المجال الاقتصادي. فالتّرابط وثيق بين الاقتصاد والمعرفة، فأغلب الدّول تعتمد في

(50) عرّف الفصل 2 من المرسوم عدد 17 لسنة 2023 المتعلّق بالسلامة السيبرانيّة الهجمة السيبرانيّة بأنّها «جملة الإجراءات التقنية المتعمّدة وغير المرّخص لها التي تستغل الثغرات وتسبب ضررا بهدف اختراق، أو تعطيل، أو أضعاف، أو تشويش على عمل الأجهزة ونظم الشبكات والمعلومات أو بهدف الاستحواذ على البيانات أو تغييرها أو إتلافها».

(51) Éric Lavallée et Serena, «La cybersécurité et les dangers liés à l'Internet...», article publié le 11/11/2022, https: //www.droit-inc.com. Droit Inc

(52) أثر تكنولوجيا المعلومات والاتّصالات على النّمو الاقتصادي في الدّول العربيّة 2000 - 2020، المركز الديمقراطي العربي، منشور بتاريخ 2023/7/9. https: //democraticac.

تعزيز اقتصادها وازدهارها على إنتاج وتداول المعرفة والمعلومات على جميع المستويات مما يبرّر الدّور الخطير للأمن السيبراني في حماية الاقتصاد من السرقة والملكية الفكرية.

هناك ارتباطا وثيقا بين الأمن السيبراني والتّنمية المستدامة والنّمو الشّامل، فحماية المعلومات أمر في غاية الأهميّة لكلّ القطاعات، ووضع الحماية المعلوماتية يهدّد جميع أهداف التّنمية المستدامة بأبعادها الاقتصاديّة، الاجتماعيّة والبيئيّة. وقد أثبت تقرير المخاطر العالميّة لعام 2023 أنّ أهمّ المخاطر التي تواجه الاقتصاد العالمي يأتي من بينها الأمن السيبراني في المرتبة الرّابعة من بين جميع المخاطر التي تواجه العالم، وأبرزها على الأجلين القصير والطّويل. فهناك 5 مليارات شخص يستخدمون الإنترنت، يمثّلون 64٪ من العالم، ونحو 3.6 تريليون دولار تجارة إلكترونيّة ستصل إلى 13 تريليون دولار في عام 2027، كما أنّ ثلث المديرين التّنفيذيين تعرّضوا لمخاطر هجمات سيبرانيّة 25٪ من الهجمات السيبرانيّة كانت في قطاع الصناعة التحويليّة، ونحو 20٪ في القطاع المالي، ثم باقي القطاعات، وذلك على مستوى العالم، كما بلغت الخسائر 4.8 تريليون دولار في عام 2022، وتصل إلى 24 تريليون دولار في عام 2027»[53].

ووفق أحدث دراسة في سبتمبر 2023، حذّرت مديرة شركة «mips» الموزّع الرّسمي لأنظمة الحماية «كاسبيرسكي – kaspersky»، من خطورة عدم تحيين الشّركات التّونسية لأنظمة الحماية، لافتة إلى أن 20٪ من الشّركات التّونسية الصّغرى والمتوسّطة، لا تقوم بتحيين أنظمة الحماية الخاصّة بها، نفس الشيء بالنسبة إلى إدارة المؤسّسات العموميّة رغم سعيها لتحقيق الأمن السيبراني في المجال الاقتصادي[54].

تعدّ البنى التحتيّة الحديثة، والإدارة الفعّالة للأمن السيبراني، وخاصة لوائح حماية البيانات السليمة، من القضايا الحاسمة للتّنمية الشّاملة والمستدامة في

(53) أميرة صالح، «الأمن السيبراني في المرتبة الّرابعة بين أهمّ مخاطر الاقتصاد العالمي»، 2023/06/18.

(54) مؤتمر الشرق الأوسط وإفريقيا للأمن السيبراني 0202 وذلك بتاريخ 45 سبتمبر 0202 بفندق رويال أسبو Hotel Royal ASBU بتونس، http: //www.aicto.org/ar

بلدان بريكس[55]، خاصة وأنهم يراهنون بشكل كبير على الرّقمنة وعلى إمكانات التقنيات المترابطة والمتشابكة، مثل تقنية الجيل الخامس (2G) وإنترنت الأشياء. فالتحوّل الرّقمي عنصرا أساسيّا لمستقبل اقتصادات ومجتمعات بريكس، وهذا هو السبب الرئيسيّ وراء قيام البلدان الأعضاء في بريكس بوضع إستراتيجيات مفصلة للرقمنة وبعضها يطبق بالفعل هذه الإستراتيجيات[56].

تتمتّع مجموعة البريكس بمزايا كثيرة تؤهّلها للقيام بدور فاعل في مستقبل تحوّلات الاقتصاد العالمي، ولتقليل الهيمنة الأمريكيّة والغربية عليه، والتي استمرت لعقود لتنوع اقتصادات أعضائها، حيث تمتلك البرازيل اقتصادا يعتمد على الزّراعة، في حين أن روسيا مصدر رائد للطّاقة، والهند قوّة اقتصاديّة ناشئة لديها طبقة متوسّطة كبيرة ومتنامية، في حين أن الصّين قوّة عظمى اقتصاديّة وتصنيعيّة، وتعدّ دولة جنوب إفريقيا لاعبًا رئيسا في صناعة التّعدين، وهو ما يعطي المجموعة ميزة تنافسيّة قويّة، ويجعلها قادرة على منافسة الولايات المتّحدة الأمريكيّة وحلفائها مجموعة السبع (7) وامتلاك القدرة على إحداث تغييرات كبرى في النّظام الدّولي الحالي، من خلال وضع أسس لنظام اقتصادي دولي جديد[57].

إنّ جميع أعضاء المجموعة قد تبنّوا واقترحوا في السّنوات الخمس الماضية أطرا تنظيميّة لحماية البيانات الشخصيّة، وهذا يعدّ إشارة واضحة على الأهميّة الإستراتيجيّة لمراقبة البيانات وأمنها لكلّ من الحكومات وشعوب دول بريكس حيث يعيش 42٪ من سكان العالم، تملك 42٪ من أكثر موارد العالم قيمة: البيانات الشخصيّة لمواطنيها. وبالتالي، فإنّ تطوير السياسات الرّقمية، خاصّة فيما يتعلّق بالأمن السيبراني وحماية البيانات، يصبح أولوّية إستراتيجيّة عالية للتّنمية

(55) إنّ دول البريكس، وهي البرازيل وروسيا والهند والصين وجنوب إفريقيا، لديها فرصة للعب دور رئيسيّ في تشكيل أجندة التنمية العالميّة. وقد انضمّت في 4 جانفي 2024 إلى قائمة بريكس الأرجنتين، إيران، مصر، السعودية، الإمارات العربيّة، إثيوبيا «إعلان عاجل من جنوب أفريقيا لمناقشة الأمن السيبراني في قمة البريكس»، https: //www.elbalad.news

(56) لوكا بيلي، «من بريكس إلى بريكس السيبرانيّة: التعاون السيبراني الجديد»، 30/10/2019، http://www.chinatoday.co.

(57) «ملامح دور مجموعة البريكس في الاقتصاد العالمي ومستقبله»، 2023، https://www.idsc.gov.eg/Article/de

الاقتصاديّة والاجتماعيّة ولضمان سلامة النّاس، والبيانات التي ينتجونها، والبنى التّحتية الحيويّة التي يستخدمونها يوميّا»[58].

وفي هذا السياق، أوضح مستشار رئيس جنوب إفريقيا جوزيف بو في مقابلة مع وكالة تاس الرّوسية على هامش القمّة الروسية الإفريقيّة: «يجب مناقشة الأمن السيبراني، لأنّه هو المستقبل، وإنّه مثّل الطّاقة النوويّة تماما، لذلك يجب مناقشته في قمّة البريكس».

بشكل عام، تتّخذ بلدان بريكس مقاربة استباقيّة للاقتصاد الرّقمي. إنّهم يدركون الفرص التي يوفّرها الاقتصاد الرّقمي ويعملون على الاستفادة من النموّ والتّنمية. من خلال التّركيز على البنية التّحتية الرّقمية، الابتكار، الإدماج والأمن السيبراني، فإنّ بلدان بريكس في وضع جيد لتشكيل مستقبل الاقتصاد الرقميّ[59].

2 – البعد الاجتماعي للأمن السيبراني

إنّ كان المحتوى المعلوماتي العسكري والأمني الرّقمي أقرب للنّمطية والتّكرار في معظم دول العالم بحكم معياريه وتشابه الأسس والمنهجيّات التي تبنى على أساسها الجيوش وأجهزة الأمن، فإنّ المحتوى المعلوماتي الاجتماعي الرّقمي يبدو في أغلب الأحيان متفرّدا في خصائصه وأشكاله وقوالبه ما بين مجتمع وآخر وبعيدا تماما عن النّمطية والتّكرار، وذلك لكونه انعكاسا لمجتمعات هي بطبيعتها شديدة الاختلاف والتميّز عن بعضها البعض.

وفي ضوء ذلك يمكننا القول إنّنا أمام محتوى معلوماتي ضخم للغاية يتحرك في صورة تيّار أو تيارات متجددة طوال الوقت من المعلومات والبيانات الحيويّة. يتمثّل البعد الاجتماعي للأمن السيبراني في تهديدات الجرائم السيبرانيّة المستحدثة، وزيادة معدّلاتها، ومظاهر استهداف الأمن القومى، وتهديد القيم والأخلاق،

(58) «إعلان عاجل من جنوب أفريقيا لمناقشة الأمن السيبراني في قمة البريكس»،
https: //www.elbalad.news

(59) «الاقتصاد الرقمي: البريكس: احتضان ثورة الاقتصاد الرقمي»، 2024،
https: //fastercapital.com/arab

وتدمير البنيّة التحتيّة، وترسيخ أزمة عدم الثّقة لدى المواطنين، وغيرها من المخاطر الاجتماعيّة[60]. وتسمح طبيعة الإنترنت المفتوحة عبر شبكات التّواصل الاجتماعي لكلّ مواطن بأن يعبّر عن أفكاره والاطّلاع على مختلف المعلومات والانفتاح عبر جميع الثقافات المختلفة، وهنا تكمن أهمّية الأمن السيبراني في حماية وصيانة القيم الجوهريّة في المجتمع كالانتماء والعادات والتّقاليد[61].

ضمن هذا السياق جاء في تقرير الاتّحاد الدّولي للاتّصالات (UTI) بشأن الأبعاد الاجتماعيّة للأمن السيبراني أنّ الثّورة الرقميّة غيّرت كيفيّة التّعامل التّجاري وكيفيّة عمل الحكومات. وأدّت العولمة والتقدّم التّكنولوجي إلى إضعاف البنية التحتيّة وبالتّالي جعلتها هدفا محتملا لهجمات إرهابيّة، حيث تواجه البلدان مخاطر حقيقيّة للأعداء أن يستغلّوا مواطن الضّعف التي تعاني منها أنظمة المعلومات الدّقيقة. فهم يسعون إلى تعطيل البنية التحتية والموارد الأساسيّة من أجل تهديد الأمن القومي. وهنا تكمن المخاطر الاجتماعيّة التي يمكن تفسيرها من خلال استحداث الجرائم السيبرانيّة وزيادة معدلاتها[62].

في هذا الإطار، أظهرت دراسة حديثة، لحسابات شركة الاستشارات الرّقمية «كيبيوس» في تقريرها السنوي جويلية 2023، أنّ ما يقرب من خمسة مليارات شخص، أي ما يزيد عن 60 في المئة من سكان العالم، من مستخدمي الأنترنيت، منهم أكثر من 2.6 مليار يستخدمون مواقع التواصل الاجتماعيّ، مما يجعلها أكبر تجمع للتّفاعل البشري. ويفتح الباب واسعا لتبادل الأفكار والخبرات الجيّدة، لكن في المقابل يعرض أخلاقيّات المجتمع للخطر، نظرا لصعوبة مراقبة محتوى الأنترنيت، كما يعرض الهويات لعمليات اختراق خارجي قد تتسبب في تهديد

(60) إسلام فوزي، «الأمن السيبراني: الأبعاد الاجتماعيّة والقانونيّة تحليل سوسيولوجي»، المجلّة الاجتماعيّة القومية،

https: //jns.journals.ekb.eg/article_205220.html

(61) عاطف حسن، «الأمن السيبراني حتمية فرضها التطوّر»،

31/07/ https: //masrafeyoun.eb.gov.eg2022

(62) تقرير (UTI) المؤتمر العالمي لتنمية الاتّصالات، الاتّحاد الدّولي للاتّصالات المؤتمر العالمي لتنمية الاتّصالات 2022 (WTDC)، من خلال مكتبه لتنمية الاتّصالات (BDT).

السلم الاجتماعيّ للدّولة، وعليه فلا بدّ من العمل على توعية المواطن بهذه المخاطر لتحقيق الأمن السيبراني في بعده الاجتماعي[63].

لذلك تعتبر شبكات التواصل الاجتماعي بتعدّدها وتنوّعها حقيقة ملموسة اكتسحت كل بقاع العالم ولاقت نجاحا كبيرا لما توفّره من فرص متنوّعة لكافة الشّرائح الاجتماعيّة، كما شكّلت فضاءا فعّالا لثورات الرّبيع العربي حيث تم استعمالها كمنبر وأداة سياسيّة لشحذ العزائم بهدف الإطاحة بالأنظمة المستبدّة وكان لها بالتالي دور في نجاح هذه الثّورات.

تعالج شبكات التواصل الاجتماعي ويتداول فيها كمّ هائل من المعلومات المتعلّقة بجوانب من الحياة الخاصة لمستعمليها ومن معطياتهم الشخصية التي يحرصون على الاحتفاظ بها لخاصة أنفسهم وإخفائها عن اطّلاع وفضول الآخرين وهو ما يفرض توفير الحماية اللاّزمة داخل هذه الفضاءات. إلاّ أن المتمعّن في الشّأن يلاحظ غياب التّأطير القانوني الخّاص بها، وانعدام الرّغبة القويّة في القيام بذلك من قبل شقّ كبير من رواد الأنترنت. ومردّ ذلك موقفهم القديم الجديد الذي جسّدوه فيما يعرف بـ«إعلان استقلال الفضاء السيبرانيّ»[64]. وهو إعلان عبّروا فيه من خلاله عن رفضهم التّام لهذا التأطير ونفورهم منه وعدم استعدادهم للخضوع إلى أيّ قيد قانوني معتبرين أنّ القيود والمفاهيم القانونيّة المتعلّقة بالملكيّة وبحق التعبير وبالحياة الخاصّة لا تنطبق عليهم. فهي تهمّ حسب نظرهم العالم المّادي فقط وليس عالمهم الافتراضي.

وهو توجّه تغذّيه فلسفة جديدة، ينقلب فيها مفهوم الحياة الخاصّة في نظر عالم الأنترنت وأغلب الأشخاص المادّية والمعنويّة الفاعلين فيه تعتبر أنّ العالم الحاليّ لم يعد يكترث بالحياة الخاصّة وهو يدعم الانفتاح على الغير. لم يستطع

(63) «أكثر من 60% من سكان العالم يستخدمون وسائل التواصل الاجتماع ي منشور بتاريخ 21/07/2023.

https: //ar.lemaghreb.tn

(64) إعلان استقلال الفضاء السيبراني الصادر بتاريخ 8 فيفري 1996 عن جون باري بارلو مؤسسي. john Perry Barlow Frontier Fondation L'Electronic

هذا الموقف أن يصمد طويلا ولاقى العديد من الانتقادات. فالأنترنت ومواقع الشبكات الاجتماعية هي في الأخير اكتشاف وتحديث تكنولوجي، وليست بالعالم الموازي. وبالتالي فإنّ كل ما يتداول بالفضاء السيبراني الافتراضي يهمّ العالم الحقيقي الملموس سواء تعلّق الأمر بالاعتداء على الحقوق الفكريّة والأدبية للأشخاص، أو على أعراضهم، أو على حياتهم الخاصّة وعلى معطياتهم الشخصيّة بل يمكن الجزم في بعض الأحيان بأنّ الاعتداءات على الأشخاص المرتكبة في الفضاء السيبراني هي أكثر وقعا على المتضرّر، لما يمكن أن تخلّفه له من أضرار، نظرا لخاصيات هذا الفضاء وما يسمح به من انتشار للمعلومة بسرعة فائقة وعلى أوسع نطاق كترسيخها وتأييدها في بعض الأحيان(65).

خاصة وأنّ ما تضعه الشّبكات الاجتماعيّة من آليات تقنيّة وبرمجيات على ذمّة مستعمليها يجعل هؤلاء يتدافعون على كشف عناصر عديدة من حياتهم الخاصّة على أوسع جمهور ممكن بكلّ طواعية، سواء بدافع البروز أو التّنافس، أو حتى بدافع تسلية النّفس. حيث يخير عدد كبير منهم فتح مجال الاطّلاع على حسابهم الخاصّ للأصدقاء وحتى للعموم واطّلاع الجميع عليها وعلى أدقّ أسرارهم. وقد ينجرّ عن هذا التصرّف عواقب وخيمة على المستخدمين لشبكات التّواصل الاجتماعيّ وعلى حقوقهم الأساسيّة مستقبلا لأنّه قد يعمد أحدهم على شبكة التّواصل الاجتماعيّ النّيل من الحياة الخاصّة والمعطيات الشّخصية لمستعمل آخر بتسريب ونشر جوانب متعلّقة بحياته الخاصة وبحميميته، والتي يحرص المعني على الاحتفاظ بها لخاصّة نفسه، وعلى إخفائها عن اطّلاع وفضول الآخرين. فإتيان مثل هذا التصرّف يشكّل جرائم يمكن على أساسها تقديم شكاوى جزائية. لذلك يجب توجيه أفراد المجتمع وتوعيته بمخاطر التّواصل الاجتماعي والمشاركة المفرطة للمعلومات الشّخصية.

ينبغي أن يحذّر من خطورة مشاركة تفاصيل حياتهم الشّخصية على منصّات التّواصل الاجتماعي ّوضرورة حماية خصوصيتهم. هذا ما يؤكّد ضرورة تعزيز

(65) محمّد الكاظم زين العابدين «شبكات التّواصل الاجتماعيّ: حماية الحياة الخاصّة والمعطيات الشخصية»، مخبر قانون العلاقات الدّوليّة والأسواق والمفاوضات DRIMAN، تونس 2014، ص23.

الوعي بالأمان السيبراني على وسائل التواصل الاجتماعي والالتزام بيقظة عند استخدام هذه المنصّات.

فالخوف من المجال العام الافتراضي هو الذي دفع باتّجاه التّفكير بضرورة سنّ التّشريعات اللاّزمة لحماية المجتمع من الإرهاب السيبراني والجريمة الإلكترونيّة والحدود الأخلاقيّة لمجتمع المعلومات تتسبّب حتما في تهديد السلم الاجتماعيّ للدّولة، وعليه فلا بد من العمل على توعية المواطن بهذه المخاطر لتحقيق الأمن السيبراني في بعده الاجتماعي(66).

3 – البعد القانوني للأمن السيبراني

تعتبر حماية البيانات الشّخصية وحماية الخصوصيّة من خلالها، حاجة ملحّة، لاسيّما وأن للاعتداء على الخصوصيّة جوانب قانونيّة نتيجة تجلّيها في عدد من الجرائم منها: انتحال هويّة الشّخص، انتحال الصّفة، اختراق أنظمة المعلومات، الوصول إلى الأسرار المهنيّة والتّجارية، الرصد غير المشروع لحركة الأشخاص والأموال، التّمييز العنصري أو العقائدي أو الدّيني. كذلك يعتبر الحفاظ على البيانات الشّخصية، من أساسيّات حماية الخصوصيّة وتعزيز الثّقة في الفضاء السيبرانيّ(67).

إنّ التّطوّرات التّكنولوجية المتسارعة، تفرض مواكبة التّشريعات القانونيّة لها، من خلال وضع أطر وتشريعات للأعمال القانونيّة وغير القانونيّة في الفضاء السيبراني، فالملاحظ أنّ الجريمة السيبرانيّة تفتقد في معظم البلدان إلى الأطر القانونيّة الصّارمة للتّعامل معها ممّا يستوجب ضرورة تفعيل التّعاون الدّولي المشترك لمكافحتها.

ضمن هذا الإطار أعلن المستشار القانوني للّجنة الدّولية للصليب الأحمر «لوران جيسل» (Gisil Laura) أنّ المادّة 12 من البروتوكول الأوّل لسنة 1977، يلزم

(66) سليم دحماني، أثر التهديدات السيبرانيّة على الأمن القومي، مذكرة لنيل شهادة الماجستير أكاديمي، جامعة محمّد بوضياف –المسيلة، 2017-2018، ص23.

(67) منى الأشقر جبور «حماية البيانات الشّخصية، وسائل الحماية» منشور في مخبر قانون العلاقات الدّولية والأسواق والمفاوضات «الإنترنت فضاء للحرّية ومصدر للإشكاليات القانونيّة»، تونس 2014، ص 123/122.

الدّول الأطراف بأن تكون الأسلحة الجديدة متوافقة مع أحكام القانون الدّولي، إلاّ أنّ عدم تنظيم استخدام الفضاء السيبراني لا يعني تركه لمشيئة المتعاقدين، فهناك أحكام عامة تفرضها قواعد الأخلاق، والمبادئ الإنسانيّة، وهناك أيضا نصوص مدوّنة بشأن الهجمات الجوّية والبحرية، تلائم طبيعة التّهديدات السيبرانيّة، ويمكن أن تطبق عليها. حيث كشفت تسريبات الحكومة الأمريكيّة 3.4مليار دولار سنويا، على العمليات السيبرانيّة سنة 2011، وتمّ إعلان أكثر من 130 دولة حول العالم عن تخصيص أقسام قانونيّة خاصّة بالتّهديدات السيبرانيّة[68]. يقتضي الفضاء السيبراني الآمن اتّخاذ قوانين وطنيّة، إقليميّة، عربيّة ودوليّة. فالاتّفاقيات الدّولية في هذا الموضوع هامة. وهي التي يمكن أن تنسجم أكثر مع طبيعة الفضاء الإلكترونيّ، الذي يعدّ الفضاء الذّي لا تضبطه حدود جغرافيّة. ولعلّ اتّفاقيّة بودابست هي النّموذج العالمي الأمثل، لشمولها على تحديد النّماذج التّجريمية وإجراءات حفظ الدّليل وكيفيّة إثباته. وقد تمّ التّعرض إلى الاتّفاقات اللاّحقة لها ومدى أهميتّها، كاتّفاقيّة المرفأ الآمن، واتّفاقيّات الخصوصيّة والحماية والمحتوى غير المشروع وغير المرغوب به وفي هذا الإطار تبرز أهميّة الاتّفاقيات العربيّة[69].

إنّ الحقّ في سريّة الحياة الخاصّة هو من بين الحقوق التي لا مجال للمساس بها نظرا للمكانة التي حظيت بها دوليا عبر ما نصت عليه المادة 12 من الإعلان العالمي لحقوق الإنسان على أنّه: «لا يجوز تعريض أحد لتدخل تعسفي في حياته الخاصّة أو في شؤون أسرته... أو مراسلاته ولا حملات تمسّ شرفه وسمعته لكلّ شخص الحقّ في أن يحميه القانون مثل ذلك التّدخل أو تلك الحملات».

(68) سعيدة رشاش، مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري، كلية الحقوق والعلوم السياسيّة، مذكرة مقدمّة ضمن متطلبات نيل شهادة ماجستير في العلوم السياسيّة، السنة الجامعية 2017/2016.

University http: //dspace.univ-tebessa.dz

(69) فرحات الحرشاني وسامي البسطانجي، «الأنترنت فضاء للحرية ومصدر الإشكاليّات القانونيّة»، مخبر قانون العلاقات الدّوليّة والأسواق والمفاوضات، منشورات DRIMAN، تونس 2014 ص1 وما بعد.

فقد نصّ الدّستور التّونسي لسنة 2022 على مبدأ سريّة المراسلات[70] الذّي كرّسته أغلب المجلاّت القانونيّة منها المجلّة الجزائية بالفصل 253[71] وكذلك الفصل 29 من مجلّة البريد[72]. وتضمّنت أيضا مجلّة الاتّصالات تجريما لإفشاء المبادلات المرسلة عبر شبكة الاتّصال مهما كان شكلها المنصوص عليها بالفصل 85[73] ورتّب عليها العقاب المنصوص عليها بالفصل 253 من المجلّة الجزائية. علاوة على نصوص أخرى ومنها نذكر المرسوم عدد 54 لسنة 2022 المؤرّخ في 13 سبتمبر 2022 المتعلّق بمكافحة الجرائم المتصلة بأنظمة المعلومات والاتّصال[74] ويطرح هذا المرسوم العديد من الإشكاليات القانونيّة والحقوقيّة، ويهدف للتّصدي للجرائم السيبرانيّة. إلاّ أنّ «هذا المرسوم يظلّ عاجزا عن التصدي لهذه الجرائم نظرا لتصادمه المتواصل مع أهمّ حقوق الإنسان الكونيّة والعديد من المبادئ الجزائية، إذ يمكن للمشرّع القيام بتنقيح القوانين الحالية والذي من شأنه وقايتها من التحوّل إلى أخرى مهجورة لا هي ملغاة ولا هي مطبّقة. ولتحديد أيّ القوانين المشمولة بالتّنقيح، يمكن بداية الاستناد إلى مختلف أبواب المرسوم تباعا. فالمشرّع في تبويبه لهذا المرسوم قد تأثّر بالاتّفاقيات الدّولية في المجال إلاّ أنّه أساء الصياغة أحيانا وتعسّف على الحقوق أحيانا أخرى»[75].

(70) الفصل 30 «تحمي الدّولة الحياة الخاصّة وحرمة المسكن وسرّية المراسلات والاتّصالات والمعطيات الشّخصية».

(71) نص الفصل 253م.ج.: «الإنسان الذّي يذيع مضمون مكتوب أو تلغراف أو غير ذلك من الكتاتيب التي لغيره بدون رخصة من صاحبها يعاقب بالسجن لمدة ثلاثة أشهر».

(72) الفصل 24 من مجلّة البريد: «فيما عدا الحالات المنصوص عليها بالفصل10 من هذه المجلّة أو بقوانين أخرى يعاقب طبقا لأحكام الفصل 253 م.ج. كل من يفشي أو يحث أو يشارك في إفشاء محتوى مراسلة على ملك الغير».

(73) الفصل 85 من مجلّة الاتّصالات الصّادرة بمقتضى القانون عدد 1 لسنة 2001: «يعاقب طبقا لأحكام الفصل 521 من المجلّة الجزائية كل من يفشي أو يحثّ أو شارك في إفشاء محتوى المكالمات أو المبادلات المراسلة...».

(74) يهدف هذا المرسوم إلى ضبط الأحكام الرّامية إلى التّوقي من الجرائم المتّصلة بأنظمة المعلومات والاتّصال وزجرها وتلك المتعلّقة بجمع الأدلّة الإلكترونيّة الخاصّة بها ودعم المجهود الدّولي في المجال، في إطار الاتّفاقيات الدّولية والإقليمية والثنائيّة المصادق عليها من قبل الجمهوريّة التّونسيّة.

(75) ياسمين عبد اللّطيف، «المرسوم عدد 54» بين التصدي للجرائم السيبرانيّة وانتهاك حقوق الإنسان»، 2 جوان 2023 https: //houloul.org/ar/

وبالتالي تتجسّد المخاطر القانونيّة، في ظلّ غياب الأمن القانوني، أو حتى في تناقض الأحكام والقوانين، وتنازع الأنظمة القانونيّة، المؤدّية إلى ارتفاع منسوب المخاطر، مع انعدام ملاحقة فاعلة تتلاءم وطبيعة الأعمال والجرائم والاعتداءات السيبرانيّة، العابرة للحدود وللأنظمة القانونيّة، بحيث تطال أيّ مواطن في أية بقعة من الأرض، بما يطال الدّول وأمنها واستقرارها.

تعدّ تلك المخاطر التي يتعرّض لها الأفراد والدّول مخاطر هائلة وغير مقيدة بالأطر القانونيّة الجارية التي لا تستوعب العصر السيبراني بالقدر الكافي. وهناك حاجة عاجلة إلى الخطى السّريعة التي تقيم بها البلدان القيادات السيبرانيّة وتوسيع قدراتها العسكريّة لتشمل النزاع السيبراني، ويجب أن تتوازن بعدم تعارض القوانين والتشريعات[76].

وتجدر الإشارة، في هذا الإطار، إلى أنّ التطوّر المتزايد لمجال المعلومات والتّقنيات الحديثة قد أدّى إلى اضطرابات عدّة، ومشاكل متنوّعة فيما يتعلّق بالمسائل القانونيّة الواسعة. فالثّورة الرّقمية في الفضاء الرّقمي تعتبر مكسبا هاما للبشرية جمعاء.

وتستوجب بذلك دراسة معمّقة، وتدعيمها وتطويرها للقاعدة القانونيّة ولنظم الحماية. كما تستلزم كذلك تطويع القوانين لاحتواء متطلّبات ومتغيّرات هذا العالم الرّقمي سريع التّطور، وذلك بتبنّي قواعد قانونيّة جديدة تكون أكثر تلاؤما مع التّطور العلمي والفكري خاصّة. فالرّقمي «كقوّة لا ممركزة، قوّة معولمة، قوّة منسّقة، وأخيرا قوّة منتجة للسّلطة»[77] يستوجب آليات فعّالة تضمن أمنه واستقراره.

(76) جوهر الجموسي، «الشبكات الاجتماعية الإلكترونيّة»...، منشورات مخبر قانون العلاقات الدّوليّة والأسواق والمفاوضات، «الإنترنت فضاء للحرية ومصدر للإشكاليات القانونيّة»، تونس 2014، ص62.

(77) NEGROPOINT Nicolas, «L'homme numérique», Paris, édition Laffont, 1995, p.281.

الجزء الثّاني: فعالية الآليات الحمائية للأمن السيبراني على المستويين الوطني والدّولي

سبق وتطرّقنا في الجزء الأوّل إلى أنّ العالم يشهد اهتماما كبيرا بالحروب الإلكترونيّة في السّنوات الأخيرة، وذلك يعود للتقدّم التكنولوجي السريع في مجال الاتّصالات وتبادل المعلومات، والذّي أدّى إلى تزايد الاعتماد على البنيّة الرقميّة والإنترنت في مختلف جوانب الحياة. وتمتدّ الحروب الإلكترونيّة إلى مجالات أبعد من الجوانب العسكريّة، حيث يمكن أن تشمل استهداف البنيّة التحتيّة الحيويّة مثل الكهرباء والمياه والاتّصالات، وكذلك الهجمات التي تستهدف القطاعات الاقتصاديّة والماليّة. وإنّ ما يميّز هذا النّوع من الحروب هو توجيهها أحيانًا نحو الجوانب المجتمعيّة والسياسيّة، بهدف زعزعة استقرار المجتمع من الدّاخل[78]. ممّا يستدعي تأمين البيانات والمعلومات، لبثّ الثقة والأمان في التّعاملات في البيئة الرقميّة المفتوحة التي نعيشها اليوم، والتي تعدّ المعلومات من أهمّ ركائزها ومقوّماتها»[77]. لذلك ظهرت الحاجة إلى تطوير آليات حمائيّة متماكلة تهدف إلى الوقاية، الكشف المبكّر والاستجابة الفعّالة للهجمات السيبرانيّة. وتشمل هذه الآليات جهودا وطنيّة تتمثّل في التّشريعات والمؤسّسات المتخصّصة، إضافة إلى التّعاون الدّولي الذي يسهم في تعزيز القدرات الوطنيّة لمواجهة التّهديدات العابرة للحدود، بما يضمن صمود الفضاء الرّقمي واستدامته.

الفقرة الأولى: الآليات الحمائيّة الوطنيّة للفضاء السيبرانيّ

لا شكّ في أنّ الأمن السيبراني يمثّل الدرع الرّقمي الذي يحمي عالمنا المتّصل بالإنترنت. وفي عصر تكنولوجيا المعلومات حيث تتداخل حياتنا مع الشبكة العنكبوتية، فيصبح الأمن السيبراني أمرا حيويا للحفاظ على خصوصياتنا وأمان بياناتنا.

(78) انصر سفاح كربم، «الحروب الإلكترونيّة وأثرها على الأمن القومي». قسم الدراسات التكنولوجيّة والأمن السيبراني 26 ديسمبر 2023

https: //www.alnahrain.iq/post/1031

وفي ضوء التطوّر التّكنولوجي المتسارع وتنامي دور الفاعلين من نشطاء وجيوش إلكترونيّة في المجال السيبراني زادت التّهديدات، حيث شملت لا فقط المواقع والخدمات الإلكترونيّة المدنيّة وإنّما أيضا البيانات والمنشآت العسكريّة. بالإضافة إلى البنية التحتيّة الحرجة كالمفاعلات النوويّة وهو تطوّر يفرض تحدّيات على الأمن القومي للدّول. ويقصد بالدّفاع الإلكتروني: «مجموعة القدرات النّظامية التي تمتلكها القوات المسلحة للحماية من تأثيرات الهجمات الإلكترونيّة والتخفيف من حدّتها والتعافي منها بسرعة»[79]. لا تقتصر التحديات الأمنيّة السيبرانيّة في المجال العسكري على الهجمات الخارجيّة فحسب، بل تشمل أيضا الثّغرات الدّاخلية والأخطاء البشريّة. فالحاجة إلى توعية وتدريب الأفراد على أفضل الممارسات الأمنيّة، وتطوير سياسات واضحة لإدارة الأزمات السيبرانيّة، تعتبر من الأولويّات القصوى.

شهدت السّنوات الأخيرة الكثير من المعارك الرقميّة والتهديدات السيبرانيّة، ممّا يحتّم على الدّول ضرورة تطوير تقنياتها، ورفع درجة جاهزيّتها واستعدادها المبكّر، لتجنّب مخاطر ونتائج تلك المعارك السيبرانيّة التي لن تنتهي بأيّ حال من الأحوال، الأمر الذي يتطلّب أيضا إنشاء فرق عمل دوليّة لمكافحة الهجمات السيبرانيّة، ومشاركة المعلومات بنشاط بين القطاعين العام والخاص واتّخاذ خطوات مشتركة لإيقاف الجهات الفاعلة والضّارة للأمن السيبراني[80] على وجه الخصوص يتوسّع مشهد التّهديد المحيط بالذّكاء الاصطناعي بشكل كبير حيث يستخدم المهاجمون تقنيات لغويّة متطوّرة، بما في ذلك زيادة حجم النّص وعلامات التّرقيم وطول الجملة. وعلى الرّغم من أنّ الأمن السيبراني أصبح الآن قضيّة على مستوى عال، إلاّ أنّ هناك حاجة إلى مشاركة أكبر على مستوى المجلس التّنفيذي من خلال قيادة إدارة مخاطر الأمن السيبراني واللّجان التّوجيهية للمساعدة

(79) إيهاب خليفة، رئيس وحدة التطوّرات التكنولوجية – مركز المستقبل للأبحاث والدراسات المتقدمة، تنامي التهديدات السيبرانيّة للمؤسسات العسكريّة، 9 أكتوبر، 2017.
https://futureuae.com

(80) كاثرين جويل، «حل الأمن السيبراني القائم على الذكاء الاصطناعي من شركة Flexxon يعد بالتصدي للجرائم السيبرانيّة»، نوفمبر 2023، wipo.int

في تقليل المخاطر المفروضة على الشّركة أو الكيان الحكومي[81].

ووفقا لبعض التقديرات، من المتوقع أن ترتفع تكلفة الجرائم الإلكترونيّة إلى 10.5 تريليون دولار أمريكي بحلول عام 2025. والنُهج التقليديّة للأمن السيبراني تجعل المستخدمين مسؤولين عن الحفاظ على الأمن السيبراني ومراقبة التهديدات. وتوفّر حلول الأمن السيبراني الرّائدة القائمة على الذّكاء الاصطناعي من شركة «فلكسون» مستويات جديدة من الحماية ضدّ التهديدات السيبرانيّة المتطوّرة[82]. فقد أصبحت الحوادث السيبرانيّة التي تشكّل اضطرابات في العمليّات الروتينيّة للتّقنيات الرّقمية، تحتّل مكانة بارزة في سياسة الأمن الوطني والدّولي، حيث تحاول الجهات الفاعلة الحكوميّة إيجاد إجابات مناسبة لمواجهة التهديد الجديد، إلى جانب العديد من المنظمات والشّركات الخاصّة.

تشّكل الهجمات الإلكترونيّة تهديدا مكلفا ومتناميا للشّركات والحكومات والمجتمع. فتضمن شهادة ISO 27001 ما يتها وتحسين أدائها. ولمواجهة تحديات الأمن السيبراني تحتاج المؤسسات إلى تحسين قدرتها على الصّمود وتنفيذ تدابير التّخفيف من حدّة التّهديدات السيبرانيّة. ضمن هذا السياق يندرج معيار ISO 27001 الذي يهدف إلى ضمان سرّية وسلامة وتوافر معلومات المنظمة وكذلك الأنظمة والتّطبيقات التي تتعامل معها [83]حيث تم تطوير هذا المعيار من قبل المنظّمة الدّولية للتّوحيد القياسي (ISO) واللجنة كهروتقنية الدّوليّة (IEC)[84].

في الأوقات التي يتمّ فيها تداول البيانات والمعلومات مثل السّلع، من الضروريّ حمايتها وتتمثّل إحدى طرق القيام بذلك في تنفيذ إدارة أمن المعلومات بناءا على سلسلة معايير أمن المعلومات ISO /IEC 2700x هذه مجموعة معايير

(81) 12 تريليون دولار تكلفة الجرائم الإلكترونيّة بحلول عام 2025 2024/01/-23.
https: //www-aljarida com.cdn.ampproject.org/v

(82) كاثرين جويل، «حل الأمن السيبراني القائم على الذكاء الاصطناعي من شركة Flexxon يعد بالتصدي للجرائم السيبرانيّة»، نوفمبر 2023، wipo.int

(83) «ISO 27001 ،https: //dcybersecurity.sa/iso-27001-information-security نظام إدارة أمن المعلومات

(84) شهادة أمن نظم المعلومات ISO/IEC 27001 –https: //international.afnor.com/ar

دوليّة لأمن تكنولوجيا المعلومات وأمن المعلومات في المنظّمات الخاصّة أو العّامة أو غير الهادفة للرّبح. استنادًا إلى ISO 27001، يمكن تنفيذ نظام إدارة أمن المعلومات ISMS والذي يمكّن المنظّمات والسّلطات العّامة إنشاؤه وتشغيله واعتماده لحمايتهم(85). ويحدّد هذا المعيار العوامل البيئيّة للمؤسّسة، الدّاخلية والخارجيّة وعمليات أصول المنظّمة (السياسات والإجراءات والعمليات وما إلى ذلك)، وكيف يتم تخطيط نظام إدارة أمن المعلومات وتنفيذه والتحقّق منه والتحكّم فيه، بناء على أداء تحليل المخاطر وتخطيط وتنفيذ الاستجابة لها من أجل التّخفيف. ويتوافق المعيار مع ISO 27002، الذي يحدّد سلسلة من ممارسات إدارة أمن المعلومات الجيّدة لجميع المهتمين والمسؤولين عن نظام إدارة أمن المعلومات(86).

فبما أنّ التّهديدات السيبرانيّة لا تفرّق بين مدني وعسكري سعت الدّول إلى تشكيل هيئات متخصصّة في الأمن السيبراني تكون مهمّتها إعداد الاستراتيجيّة الوطنيّة للأمن السيبراني والإشراف على تنفيذها وذلك في إطار بناء الثّقة والاطمئنان والأمن في استعمال الاتّصالات وتكنولوجيا المعلومات فضلا عن حماية البيانات الشخصيّة وهي من الأولويات التي تستدعي تعاونا وتنسيقا بين الحكومات والمنظّمات ذات الصلة وشركات القطاع الخاص وكل الهياكل المعنية بمجال بناء القدرات وتبادل أفضل الممارسات من أجل وضع السياسات العامّة والتّدابير القانونيّة، التّنظيمية والتّقنية التي تتناول حماية البيانات الشخصيّة. لضمان موثوقيّة أمن شبكات وخدمات تكنولوجيا المعلومات والاتّصالات لتأمين السلامة السيبرانيّة.

(85) Gert Krueger - نظرة عامة، «الخبير»، https: //www.dqsglobal.com/ar، معايير أمن المعلومات

(86) تتعامل المعايير الفرديّة لأمن المعلومات في سلسلة ISO 27001 مع مواضيع متنوّعة في مجال أمن المعلومات. على سبيل المثال تحدّد المواصفة القياسية الدّولية ISO 27001 نظام إدارة أمن المعلومات (ISMS، ISO 27701) نظام إدارة حماية البيانات، يوفّر ISO 27017 إرشادات حول تدابير أمان المعلومات للحوسبة السحابية، ويوفر ISO 27005 إرشادات لإدارة مخاطر أمن المعلومات، «نظام إدارة أمن المعلومات ISO 27001»، https: //dcybersecurity.sa/iso-27001-information-security

وفيما كانت تونس سبّاقة ومن أوائل الدّول التي أنشأت وكالة مختصّة للسّلامة المعلوماتيّة يرجع تأسيس بذرتها الأولى لسنة 1999، وبعثت رسميا سنة 2004[87]، إلّا أنّ جهودها تلاشت اليوم وباتت تتبوأ مركزا ضعيفا في هذا المجال في ظلّ ضعف الإمكانيّات والإجراءات، حيث احتلّت تونس المرتبة 42 عالميا في مؤشر الأمن السيبراني[88]، وفقا لتقرير أعدته أكاديميّة الحكومة الإلكترونيّة في إستونيا[89]. وأمام تزايد الجرائم الإلكترونيّة، التي شهدت ارتفاعا مقلقا في تونس خلال الآونة الأخيرة، من أعباء الحكومة التي باتت مطالبة ببذل المزيد من الجهود لحماية أمنها السيبرانيّ فأحدثت الوكالة الفنيّة للاتّصالات منذ سنة 2013[90]، ورغم كل هذه الجهود، شهدت محاولات الاختراق والهجمات السيبرانيّة في تونس ارتفاعا خلال السّنوات الماضية، وذلك بنسبة تتجاوز 30٪.

(87) في سنة 1999، طبقا للأمر عدد 2768 لسنة 1999 المؤرّخ في 6 ديسمبر 1999 تم إحداث «**وحدة تصرف حسب الأهداف لإنجاز مشروع تطوير السلامة الإعلامية** تخضع لإشراف كتابة الدّولة للإعلامية وتضطلع بمتابعة آخر التطوّرات المتعلّقة بمجال السلامة المعلوماتية والسهر على تحسين سلامة التطبيقات والبنى التحتية الوطنيّة الحساسة.

وفي سنة 2002تم تحوير دور هيكلة الوحدة إلى «**إدارة عامة**» تضطلع بتطوير استراتيجيّة وطنيّة ومخطط وطني في مجال السلامة المعلوماتية في سنة 2003، تم إقرار إحداث وكالة بمقتضى قرار رئاسي مهمتها تطوير آليات الحماية ووضع برامج التدقيق وتفعيل التكوين والرسكلة في مجال السلامة المعلوماتية.

سنة 2004 أحدثت «**الوكالة الوطنيّة للسلامة المعلوماتية**» بمقتضى القانون عدد 5 لسنة 2004 المؤرّخ في 3 فيفري 2004. ر.ر.ج.ت عدد 10 بتاريخ 2004/02/03.ص251.

انظر الموقع الرسمي لوزارة التكنولوجيا والاتّصال: https: //www.mtc.gov.tn

(88) «مؤشر يقيس مدى جاهزيّة الدّول لمنع التّهديدات الإلكترونيّة واستعدادها لإدارة الحوادث السيبرانيّة»، وقد قامت مؤسّسة أكاديميّة الحكومة الإلكترونيّة «e-Governance Academy Foundation (eGA)» بتحديث المؤشر الوطني للأمن السيبراني أو مؤشر NCSI. ويقيس هذا المؤشر جاهزية الدّول في منع التهديدات وتدبير الحوادث السيبرانيّة ويشكل قاعدة بيانات متاحة للجمهور تحتوي على معلومات حول الجهود التي تبذلها الدّول لتعزيز القدرات الوطنيّة في مجال الأمن السيبراني.

https: //www.dgssi.gov.ma

(89) مؤشر «الأمن السيبراني»، 2018، حسب التقرير الذي أعدته أكاديمية الحكومة الإلكترونيّة في أستونيا.

https: //www.hespress.com

(90) الأمر عدد 4506 لسنة 2013 المؤرّخ في 6 نوفمبر 2013 يتعلّق بإحداث الوكالة الفنية للاتّصالات وبضبط تنظيمها الإداريّ والماليّ وطرق سيرها ر.ر.ج.ت عدد 90 الصادر بتاريخ 2013/11/12، ص 3175-3179.

وعليه، وتبعا لمداولات مجلس الأمن القومي المنعقد في 05 جويلية 2018، تمّ بعث فريق عمل تابع للجنة أمن المعلومات والاتّصالات المنبثقة عن هذا المجلس وتحت إشراف المستشار الأوّل للأمن القومي، لإعداد الإستراتيجية الوطنيّة للأمن السيبراني التي تهدف إلى حماية الفضاء السيبراني الوطني وتطويره من خلال بناء القدرات الوطنيّة وضمان الثّقة الرّقمية في تفاعل مع جملة الإستراتيجيّات القطاعيّة والخاصّة وتنفيذ الخطط في المجال بالتنسيق مع جميع الأطراف المتداخلة، وذلك في إطار احترام الحقوق والحرّيات وفق مقتضيات وأحكام الدّستور والاتّفاقيات والمعاهدات الدّولية.

وبمقتضى فعاليات الدّورة الثّالثة والعشرين لمنتدى المدرسة العليا للمواصلات بتونس تحت شعار (Technoworld Security) بحضور مدير الدّراسات بالمدرسة العليا للمواصلات بتونس، وعدد من ممثّلي الشّركات المختصّة بالسّلامة السيبرانيّة والخبراء، إضافة إلى عدد من الطّلبة والباحثين والفاعلين في المجال الرّقمي، تمّ التّأكيد على تطوير البنية التحتيّة ومراجعة النّصوص القانونيّة والترتيبيّة للأمن السيبرانيّ والسّيادة الرّقمية وما يفرضه الانفتاح على المنظومات والتّطبيقات الرّقمية العالميّة من تحدّيات ومخاطر يمكن أن تعترض مسار التّحول الرّقمي في تونس[91]. ووعيا بخطورة تلك التّهديدات والمخاطر أكّد بدوره وزير تكنولوجيات الاتّصال التّونسي أنّ الحكومة تعمل على مراجعة النّصوص القانونيّة، وتطوير التّشريعات المتعلّقة بمجال الأمن السيبراني[92].

ورغم أنّ تونس أقرّت في أكتوبر 2019 الإستراتيجيّة الوطنيّة للأمن السيبراني بهدف تعزيز خطّ الدّفاع التّكنولوجي والرّقمي، إلاّ أنّه في غياب أطر تنظيميّة وتشريعيّة ناجعة إضافة إلى نقص الكفاءات المختصّة في هذا المجال لم تتمكّن من مجابهة مخاطر الحرب السيبرانيّة. ففي إطار تواصل المجهودات الوطنيّة

(91) الإستراتيجية الوطنيّة للأمن السّيبرني 2020 – 2025، وزارة تكنولوجيات الاتّصال، الكتابة القارة للجنة أمن الاتّصالات والمعلومات، (ncss@tunisia.gov.tn)

(92) الإستراتيجية الوطنيّة للأمن السّيبرني 2020 – 2025، وزارة تكنولوجيات الاتّصال، الكتابة القارة للجنة أمن الاتّصالات والمعلومات، (ncss@tunisia.gov.tn)

لحماية الفضاء السيبرانيّ الوطني وحماية مستعملي تكنولوجيّات المعلومات والاتّصال من الاعتداءات والهجمات السيبرانيّة التي تهدف إلى النّيل من أنظمة المعلومات والبيانات المعلوماتيّة أو استعمالها دون وجه حق، أو المساس بالأمن العام، ساهم المرسوم المتعلّق بمكافحة الجرائم المتّصلة بأنظمة المعلومات والاتّصال المؤرّخ 13 سبتمبر 2022[93] في «ضبط الأحكام الرّامية إلى التوقيّ من الجرائم المتّصلة بأنظمة المعلومات والاتّصال وزجرها وتلك المتعلّقة بجمع الأدلّة الإلكترونيّة الخاصة بها ودعم المجهود الدّولي في إطار الاتّفاقيات الدّولية والإقليميّة والثنائيّة المصادق عليها من قبل الجمهوريّة التّونسيّة»[94]. والهدف من ذلك تحقيق النّجاعة الكافية عند التعامل مع الجرائم الإلكترونيّة. ورغم كل هذه المحاولات تمّ تصنيف تونس في مراتب متأخّرة في مؤشّر الأمن السيبرانيّ العالميّ.

وهذا ما دفعها لاتّخاذ خطوة هامّة في هذا المجال، حيث أحدثت مؤخرا بمقتضى المرسوم عدد 17 لسنة 2023 مؤسّسة عموميّة لا تكتسي الصّبغة الإداريّة تتمتّع بالشخصيّة المعنويّة والاستقلال المالي تخضع لإشراف الوزارة المكلّفة بتكنولوجيات الاتّصال يطلق عليها اسم «الوكالة الوطنيّة للسّلامة السيبرانيّة»، حيث يهدف هذا المرسوم إلى تنظيم مجال السّلامة السيبرانيّة وضبط المهام الموكولة لهذه الوكالة، والآليات المخوّلة لها لضمان سلامة الفضاء السيبراني الوطني في إطار مشمولاتها[95]، وتعزيز السيّادة الرقميّة والذي يعتبر جزءا من الإستراتيجيّة الوطنيّة الرقميّة.

(93) المرسوم عدد 54 لسنة 2022 المؤرّخ في 13 سبتمبر 2022 المتعلّق بمكافحة الجرائم المتصلة بأنظمة المعلومات والاتّصال ر.ر.ج.ت عدد 103 الصادر بتاريخ 2022/09/16، ص2948.

(94) الفصل الأوّل من المرسوم عدد 54 لسنة 2022 المؤرّخ في 13 سبتمبر 2022 المتعلّق بمكافحة الجرائم المتّصلة بأنظمة المعلومات والاتّصال سالف الذكر.

(95) تمّ في 2023/09/28 بمقرّ وزارة تكنولوجيات الاتّصال، توقيع مذكرة تفاهم بين الوكالة الوطنيّة للسّلامة السيبرنيّة ونظيرتها الإيطالية، وتهدف إلى إرساء ودعم التعاون الثنائيّ بين البلدين في مجال السلامة السيبرنية وخدمات الثقة الرّقمية، إضافة إلى تعزيز تبادل التجارب والخبرات بين المؤسستين وتطوير الكفاءات المختّصة في مجال الأمن السيبراني،
https: //www.mtc.gov.tn

إذ عرّف المشرّع التّونسي السّلامة السيبرانيّة صلب المرسوم المذكور، بأنّها مختلف التّدابير والآليات التقنيّة وغير التقنيّة، التي يقع تركيزها بغرض حماية الفضاء السيبراني وتعزيز القدرة على الاستباقيّة والتوقّي من المخاطر السيبرانيّة والتفطّن السّريع للحوادث والهجمات السيبرانيّة والقدرة على الاستجابة في حالات الطوارئ، بهدف الحدّ من التّداعيات وضمان استمراريّة النّشاط عند حدوث الأزمات السيبرانيّة. وعرّف المرسوم هذه المخاطر، باحتمال تجاوز التهديد السيبراني العرضي أو المفتعل لآليات السّلامة السيبرانيّة، عبر استغلال الثّغرات الموجودة بمكوّن أو أكثر من مكوّنات الفضاء السيبراني مع إمكانيّة إحداث ضرر. وقد أوكل المرسوم عدد 17 لسنة 2023[96] مجموعة من المهام ذات الطّابع الوقائي للفضاء السيبراني لفائدة الوكالة الوطنيّة للسّلامة السيبرانيّة، على غرار تطوير سياسات وآليات حوكمة أمن الفضاء الإلكترونيّ الوطنيّة وتحديثها، وإبلاغها إلى الإدارات والهيئات ذات الصّلة، متابعة تنفيذ الخطّة الوطنيّة لتنفيذ أمن الفضاء الإلكتروني، واتّخاذ تدابير فعّالة لتجنّب التّهديدات العرضيّة والمفتعلة للفضاء السيبراني الوطني، مع القيام بالإجراءات الوقائيّة ضدّ مخاطر الإنترنت والإبلاغ عن الحوادث والهجمات الإلكترونيّة. علاوة على الاستجابة الحينيّة في حالات الطوارئ للردّ على الهجمات الإلكترونيّة لضمان استمراريّة النّشاط من خلال الاستقصاء والتحرّي الرّقمي لتشخيص الحوادث وتحديد المسؤوليّة المتعلّقة بالأمن السيبراني، ومتابعة تنفيذ القدرات من خلال المشاركة في إعداد البرامج الأكاديمية المهنيّة وتنظيم دورات تدريبية مهنيّة والنّماذج والمبادئ التّوجيهية التي يجب أن تعتمدها الوكالات العامّة والخاصّة، أيضا وضع مؤشّرات لقياس مستوى الأمن السيبراني الوطني وإجراء حملات اتّصال وتوعية خاصّة أثناء الأزمات السيبرانيّة.

كما نصّ المرسوم سالف الذّكر على ضرورة ضمان اليّقظة التّكنولوجية ومواكبة التطوّرات في مجال الأمن السيبراني من خلال التّعاون والتّنسيق الدّولي مع الجهات الرّسمية المختصّة وفق الاتّفاقيّات المبرمة لهذا الغرض على

(96) المرسوم عدد 17 لسنة 2023 المؤرّخ في 11 مارس 2023 سالف الذكر.

المستويات الثّنائية والإقليميّة والدّولية بشكل عام»[97]. وحذّر من الآثار المترتّبة عن الهجمات السيبرانيّة كاضطرابات الأعمال وتوقّف الخدمات التّجارية بسبب أعمال التّخريب أو إيجاد كلمات المرور للمستخدمين، الخسائر الماليّة والمتمثّلة في خسائر في الإيرادات وفقدان السّرية، الشّفافية والنّزاهة وإتاحة المعلومات لأفراد غير مسموح لهم بالاطّلاع على المعلومات. علاوة على اختراق الأمن السيبراني بسبب فيروسات أو ثغرات الحاسوب أو توقّف الخدمة وبعض الأنظمة وما ينجرّ عنه من فقدان السّمعة نتيجة لفقد ثقة العملاء في المؤسّسة وتسليط العقوبات الإداريّة والعقوبات الماليّة والقوانين المنظّمة لذلك بسبب إفشاء المعلومات التي أصبحت متاحة بسبب اختراقات الفيروسات.

وبالتّالي يمكن أن نلاحظ مدى الاهتمام الذي توليه تونس لحماية الأمن السيبراني من خلال ما تضمّنه هذا المرسوم من آليات وأساليب وقائية متعدّدة. وفي هذا السياق فإنّ السؤال يطرح نفسه هل ستتمكّن تونس فعلا من تنفيذ هذه الإستراتيجيّة على أرض الواقع أم أنّها ستبقى مجرّد قواعد مكتوبة، نتيجة ضعف الإمكانيات المّادية والموارد البشريّة المختصّة في هذا المجال؟ خاصّة وأن البلدان المتقدّمة مثل الولايات المتحدة الأمريكيّة، أستراليا، إنجلترا... خصّصت أموالا طائلة لمعالجة مسائل الأمن السيبراني، فالعلاقات الدّولية مهددّة في كل لحظة نتيجة الاختراقات والاعتداءات على الشّبكة العالميّة للمعلومات وعلى الأنظمة المعلوماتيّة، وهذا يتطلّب حتما تضافر الجهود الدّولية للتّصدي للمخاطر السيبرانيّة[98].

ويمكن التّصدي للهجمات السيبرانيّة التي تستهدف تونس من خلال اتّخاذ مجموعة من الإجراءات، منها تعزيز الأمن السيبراني، وذلك من خلال تبني معايير عالميّة، وتدريب الكوادر الوطنيّة، ورفع مستوى الوعي العام بكيفيّة حماية البيانات والمعلومات الشخصيّة، لكن تبقى الجهود الوطنيّة الرامية لحماية الأمن

(97) الفصل 5 من المرسوم عدد 17 لسنة 2023 المتعلّق بالوكالة الوطنيّة للسلامة السيبرانيّة سالف الذكر.

(98) صلاح الدين كريمي، «الأمن المعلوماتي لأجهزة الدّولة ومؤسساتها... ضعيف ومخيف»، 2021/07/03

/https: //www.assabahnews.tn

السيبراني محدودة ومقيدة، مما يستدعي تعزيز التعاون الدّولي لتطوير آليات وأساليب حماية أكثر فاعلية.

الفقرة الثّانية: الآليات الحمائية الدّوليّة للأمن السيبراني

أصبح الفضاء السيبراني عنصرا مؤثّرا في النّظام الدّولي، وكشف عن محاور جديدة للصّراع الدّولي يعرف بصراع الفضاء الإلكترونيّ، من شأنه أن يسبّب خسائر عسكريّة اقتصاديّة، وماليّة فادحة، لهذا أصبح هذا الفضاء يدخل ضمن أولويّات السّياسة الخارجيّة للدّول وضمن إستراتيجيّات الأمن القومي لديها، حيث دفعت التّهديدات المتزايدة لأمن الفضاء السيبراني العديد من الدّول للعمل على بذل الجهود للحدّ من هذه التّهديدات[99].

فنظرا لطبيعة مجتمع الفضاء السيبراني العابرة للحدود لا بدّ من الإقرار بأهميّة التّعاون الدّولي في تعزيز الموثوقيّة في استخدام تكنولوجيات المعلومات والاتّصالات وتوافر هذه التكنولوجيات وأمن استخدامها والمساعدة في التّحقيق والأحكام الإجرائيّة والموضوعيّة المشتركة لمعالجتها على نحو ملائم. علاوة على ذلك فإنّه من المتّفق عليه أنّ التّعاون الدّولي يمثّل أحد المتطلّبات الرّئيسية لضمان الأمن السيبراني على الصّعيد العالمي. وفي هذا السّياق تندرج التّحديات الكبيرة التي تواجهها عديد الدّول العربيّة في مجال الأمن السيبراني وعلى رأسها حماية المعطيات الشخصيّة للمستخدمين والمؤسّسات الحكوميّة كانت أو خاصّة. وقد تم التأكيد عل أهميّة تعزيز التعاون بين الدّول العربيّة في مجال الأمن السيبراني[100].

ولا يمكن في سياق تأثيرات تطبيقات التّواصل الاجتماعي على الأمن الوطني، تجاهل خطورة الحروب السيبرانيّة الواقعة حاليا بين الدّول، والتي تحتاج جهودا

(99) حسين حياة، «الفضاء الإلكتروني وتحديات الأمن العالمي»، مجلّة العلوم القانونيّة والسياسيّة، volume 12 عدد1، ص، 1066-1089، 2021/04/28، https: //www.asjp.cerist.dz/en/arti

(100) الأيام العربيّة للأمن السيبراني وذلك يومي 05-06 ديسمبر 2023 بتونس العاصمة، ورشة عمل السيادة الرقمية العربيّة، مقرّ اتّحاد إذاعات الدّول العربيّة، تونس العاصمة «حماية البيانات الشخصية في عصر البيانات الضخمة والذكاء الاصطناعي.

جبّارة لمعالجتها واحتوائها كحكومات، مؤسّسات، أفراد ومجتمع مدني. وتتعمّق خطورة هذه الحروب السيبرانيّة إذا ما أضفنا إلى الفضاء الاتّصالي المعلوم، عالم الحوسبة السّحابية Cloud Computing، وانتشار تطبيقاتها، وما أفرزه ذلك من نشأة تعقيدات جديدة، تخطّت كلّ وسائل الوقاية والتّوعية التقليديّة، وتجاوزت بذلك كل المجهودات المنفردة للدّول في مجال حماية فضائها السيبراني[101].
لقد تأكّد من خلال الحروب السيبرانيّة، أنّ الوسائل الذّاتية التّقليدية للدّول في مكافحة الجرائم السيبرانيّة قد فقدت فعاليتها، وأصبحت الدّول واتّحاداتها بحاجة إلى مقاربات جامعة للحدّ من تأثير هذه الحروب ومن ضمنها وضع آليات مواجهة للتحدّيات الجديدة التي تفرضها الحوسبة السّحابية، لا سيما على المستويات التالية: تشجيع التزام الشركات بقواعد الحماية والأمن، تحديد مسؤولية المتعاقدين مع موفّري الخدمة الأساسيّين، نوعية الخدمة، طبيعة المسؤوليات، مستويات الحماية، نقل البيانات إلى بلاد يمكن أن تكون على عداء مع العالم العربي. لذلك تمّ إقرار توصيات من خلال جامعة الدّول العربيّة، تقرّ المبادئ العامّة لحماية البيانات الشّخصية وينسجم مع الاتّجاه الدّولي في هذا المجال.

كما تمّ إقرار الأطر التّشريعية والتّنظيمية الملائمة على المستوى الوطني وأطر أخرى لتبادل البيانات الخاصّة بمجالات الأمن والجزاء بين الدّول العربيّة. ومن هذه التوصيات إنشاء هيئات تنسيق وتعاون عربيّة تتولّى متابعة التّنفيذ على المستوى العربي، والدّولي، لا سيما في حالات انتقال بيانات تخصّ مواطني أكثر من دولة عربيّة[102]، وفي سياق ذلك يتعيّن تعزيز الوعي في المجتمع العربي بكل قطاعاته المدنيّة، والمهنيّة والحكوميّة، لأهميّة حماية البيانات الشخصيّة، ودورها في حماية الفرد والمجتمع. وشملت التّوصيات التّعاون على إيجاد آليات حماية

(101) عماد جاب اللّه، التقرير الافتتاحي: «واقع التحديات والسياسات»، منشور في منشورات DRIMAN مخبر قانون العلاقات الدّوليّة والأسواق والمفاوضات، الأنترنت فضاء للحرية ومصدر للإشكاليّة القانونيّة، تونس 2014، ص12.

(102) عماد جاب اللّه، التقرير الافتتاحي: «واقع التحديات والسياسات»، منشور في منشورات DRIMAN مخبر قانون العلاقات الدّوليّة والأسواق والمفاوضات، الأنترنت فضاء للحرية ومصدر للإشكاليّة القانونيّة، تونس 2014، ص12.

تسمح للمواطن بممارسة حقّه في الاطّلاع على البيانات وطلب تصحيحها، لدى الدّول الأخرى التي تتولّى معالجتها، وملاحقة المؤسّسات أو الهيئات التي تمتنع عن تطبيق القوانين الخاصّة بالحماية، على غرار ما هو معمول به في مجال ملاحقة المجرمين، ومكافحة الإرهاب، والجرائم العابرة للحدود بكلّ أشكالها.

حيث يمثّل الأمن السيبراني أهمّ التّحديات على المستوى الإستراتيجي لما له من تأثير وطني، إقليمي ودولي يستدعي من الدّول العربيّة العمل على تضافر وتوحيد جهودها لإيجاد حلول شاملة ومشتركة بشكل يضمن النجاح المشترك في التّعامل مع المخاطر السيبرانيّة في إطار مقاربة تشاركية متكاملة، بالإضافة إلي إطار تشريعي ملائم مع الحرص على امتلاك الخبرات والآليات والتقنيات المناسبة، لضمان حماية أصولها ومواردها الرّقمية وحماية أمن البيانات وخصوصيّة مواطنيها.

وقد أطلق المرصد العربي للأمن السيبراني[103] في إطار التعاون العربي في مجال الأمن السيبراني حملة توعوية واسعة، تستهدف المؤسسات الحكوميّة والخاصة، وجميع أفراد المجتمع، حول أهميّة أخذ الحيطة والحذر لتفادي الوقوع ضحية لهجمات التصيد والاحتيال الإلكتروني، التي تستخدم التكنولوجيا لخداع المستخدمين الرقميين للحصول على معلوماتهم وبياناتهم الشخصيّة. للأمن السيبراني دورا حاسما في الحفاظ على الخصوصيّة وأمن المعلومات وضمان إستدامة الأعمال والمؤسّسات، إضافة لدعم التطوّر التّكنولوجي والابتكار من خلال تعزيز الثّقة باستخدام الأنترنت والتكنولوجيا الرّقمية[104] والتّقليل من مخاطر الانفتاح الرّقمي حيث أن نسبة 80٪ من المخاطر السيبرانيّة[105] تأتي بسبب

(103) المرصد العربي للأمن السيبراني هو مبادرة تهدف إلى تعزيز التعاون العربي في مجال الأمن السيبراني من خلال توفير منصة لتبادل المعلومات والموارد بين الدّول العربيّة يعتبر جزءا من الجهود المبذولة لبناء بيئة رقمية آمنة ومستدامة في المنطقة.

(104) المركز الوطني للأمن السيبراني، «اختتام شهر التوعية بالأمن السيبراني2023»، 2024/02/14. https: //ncsc.jo/AR/NewsDetails

(105) المركز الوطني للأمن السيبراني، «اختتام شهر التوعية بالأمن السيبراني2023» 2024/02/14، مرجع سالف الذكر.

أخطاء بشريّة لعدم الوعي والمعرفة بأساسيّات التّعامل مع الإنترنت وأدوات التّكنولوجيا[106].

تعترف حكومات عديدة بأنّ التّعليم العام وتوعية الجمهور من الأساليب القويّة للدفاع السّيبراني. وتساعد قواعد بيانات المعلومات وبرامج التّوعية الوطنيّة على تعزيز الوعي على مستوى القاعدة الجماهيريّة، فعلى سبيل المثال تنظّم الولايات المتّحدة شهرا لتنمية الوعي بالأمن السيبراني القومي في أكتوبر من كلّ سنة. كل هذه التحدّيات تستوجب العمل على تطبيقها فعليّا وهذا يستدعي توحيد وتحديث كافة التّشريعات المتعلّقة بتكنولوجيا المعلومات والاتّصالات في البلدان العربيّة، ووضع أطر تشريعيّة، ماليّة وتقنيّة إقليميّة عربيّة موحّدة تسمح بتوجيه كافة الجهود الفرديّة نحو حماية شاملة للفضاء العربي السيبرانيّ[107]. ويبقى الوعي بمخاطر الأمن السيبراني جزءا أساسيا من أي إستراتيجيّة أمنيّة ناجحة.

وهذا ما يجعلنا ندرك أهميّة تطوّر الأوضاع الحالية ممّا يستوجب وضع الآليات اللاّزمة وسنّ التشريعات الضّرورية لمجابهة هذه المخاطر التي تهدّد الأمن السيبراني بما يتناسب مع التطوّرات التّكنولوجية التي أدّت إلى ظهور مفاهيم جديدة لم يعهدها القانون الدّولي وقانون العلاقات الدّولية على غرار «القوّة السيبرانيّة» أو ما يعرف إعلاميّا بالقوّة الإلكترونيّة، فهل استخدامها أو التهديد باستخدامها يندرج تحت نطاق «القوة العسكريّة» المحضورة بموجب المادة 2 فقرة 4 من ميثاق الأمم المتحدة، أم أنها خارج نطاق الحضر المقصود؟ وهنا لا بد أن نفرّق بين الهجمات السيبرانيّة ذات الطّابع العسكري التي تستهدف

(106) قام قطاع التعليم العام بوزارة التربية قام من خلال التوجيه الفني العام للحاسوب بتنفيذ العديد من الخطوات الهامة لنشر ثقافة المعرفة بالأمن السيبراني لدى الميدان التربوي بكافة فئاته، وذلك من منطلق دور التوجيه الفني العام للحاسوب في نشر وتعزيز الوعي بالأمن السيبراني لمواجهة تحديات العصر الرقمي، في سبيل العمل على تعزيز مستوى الوعي بالأمن السيبراني للمتعلمين والمعلمين، المركز الوطني للأمن السيبراني، «اختتام شهر التوعية بالأمن السيبراني 2014».
https: //ncsc.jo/AR/NewsDetails

(107) عماد جاب اللّه، التقرير الإفتتاحي: «واقع التحديات والسياسات»، منشور في منشورات DRIMAN مخبر قانون العلاقات الدّوليّة والأسواق والمفاوضات، الأنترنت فضاء للحرية ومصدر للإشكاليّة القانونيّة، تونس 2014، ص13.

البنى التّحتية الرّقمية الحيويّة للدّولة والمتمثّلة في «الأنظمة المعلوماتيّة التي تأوي الأصول والخدمات الحسّاسة على المستوى الوطني والتي يمكن أن يؤثّر توقّفها أو المسّ من سلامتها على الأمن القومي «والهجمات السيبرانيّة ذات الطّابع غير العسكري والتي تشمل الحرب الإعلاميّة، نشر الإشاعات والفكر المتطرّف، حيث يصعب إيقاف الهجمات السيبرانيّة ولكن يمكن التقليل منها عن طريق وضع أساليب جديدة وإعادة تكييف هذه المفاهيم ذات الطابع التقليدي لكي تتطابق مع المجالات الجديدة.

أصبحت الدّول تهتمّ بالمخاطر الأمنيّة لما تشهده من تطوّرات واسعة في مجال التّكنولوجيا، وتعدّ قضيّة الأمن السيبراني والقرصنة من أهمّ القضايا الدّولية التي يتمّ دراستها من قبل الأمن الدّولي وفقهاء القانون الدّولي وذلك لكي يكون هنالك خطط تتبعها الدّولة في محاولة منها لحفظ الأمن والنّظام العام في الدّولة وكذلك سعي المنظّمة الدّولية للحفاظ على السّلم والأمن الدّوليّين[108]، لأنّ السّباق نحو التسلّح السيبراني يندرج ضمن السياسات الدّفاعية التي تخلق توتّر واحتقان العلاقات الدبلوماسيّة بين الدّول بسبب التدخل في الشّؤون الدّاخلية وكل هذه التّداعيات تؤدي حتما إلي اندلاع الأزمة السيبرانيّة.

(108) الرّؤية العربيّة للأمن السيبراني: الاستراتيجيّة العربيّة للأمن السيبراني». الكتاب بصيغة PDF، مركز التّطوير الرّقمي https: //www.ddc.iq