مجلة البحوث الاقتصادية المتقدمة: المجلد (07)، العدد (02) / 2022
PISSN : 2572-0198 / EISSN : 2676-1572

أهمية حوكمة الأمن السيبراني لضمان تحول رقمي آمن للخدمات العمومية في الجزائر

Importance of cybersecurity governance for ensuring a secure digital transformation of the public services in Algeria

زمورة جمال [1]، بن عيسى ليلى [2]

[1] جامعة محمد خيضر– بسكرة، مخبر مالية، بنوك، إدارة أعمال (الجزائر)
[2] جامعة محمد خيضر– بسكرة، مخبر مالية، بنوك، إدارة أعمال (الجزائر)

تاريخ الاستلام: 2022/01/22 **تاريخ القبول**: 2022/09/30 **تاريخ النشر**: 2022/09/30

ملخص:

في ظل تحول الجزائر إلى الحكومة الإلكترونية من خلال التحول الرقمي التدريجي للخدمات العمومية، وما يصاحبه من انفتاح على الفضاء السيبراني، كان لزاما الأخذ بعين الاعتبار لمتغير الأمن السيبراني الذي يشكل الهاجس الأكبر للدول والشركات الكبرى. إن تبني برامج وإستراتيجيات واضحة وشفافة لحوكمة الأمن السيبراني ضرورة حتمية تمليه المصلحة العليا للوطن ترتكز على نماذج وأطر عملية يمكن الوثوق بفعاليتها، خاصة وأن نقائص ملحوظة تشوب المجهودات المبذولة مقارنة مع المعايير والتصنيفات الدولية المعتمدة. إن الاستفادة من تجارب الدول الرائدة في هذا الميدان إقليميا ودوليا، مع تدعيم الإجراءات التنظيمية والتحكم في التقنيات المتطورة في ميدان الأمن السيبراني بالاعتماد على الموارد البشرية ذات الكفاءة والمهارة العالية، لتحقيق الأمن السيبراني للوطن وللخدمات العمومية الرقمية الموجهة للمستخدمين خاصة.

الكلمات المفتاحية: الأمن السيبراني؛ حوكمة الأمن السيبراني؛ التحول الرقمي؛ الخدمة العمومية.

تصنيف JEL: G30؛ G38؛ H00؛ K00

Abstract:

At the dawn of Algeria's transformation to e-government through the gradual digital transformation of public services, and the attendant openness to cyberspace, it was necessary to take into account the cybersecurity variable that is the greatest concern for countries and large companies. the adoption of clear and transparent programs and strategies for cybersecurity governance is imperative, dictated by the supreme interest of the country based on practical models and frameworks whose effectiveness will trust, especially since there are noticeable shortcomings in the efforts made compared to the approved international standards and classifications. Benefiting from the experiences of the leading countries in this field regionally and internationally, while strengthening regulatory rules and controlling advanced technologies in the field of cybersecurity, relying on highly qualified and skilled human resources, to ensure cybersecurity for the country and for digital public services directed to users in particular.

Keywords: *Cybersecurity; Cybersecurity Governance; Digital Transformation; Public Service.*

Jel Classification Codes: *G30;G38;H00.K00*

* **المؤلف المرسل**: جمال زمورة، djamel.zemoura@univ-biskra.dz

1. المقدمة

إن تعميم الوصول إلى الخدمات العمومية الرقمية من خلال ما يوفره الفضاء الرقمي من موارد وتكنولوجيات متطورة، يؤثر بشكل متزايد على المستخدمين في حياتهم اليومية، لقد أحدث بالفعل تحولا عميقا في أنماط الحياة الفردية والجماعية في جميع أنحاء العالم. بينما يوفر التحول الرقمي فرصًا لا حصر لها للتنمية الاقتصادية والاجتماعية والسياسية، فقد مكّن أيضًا الجهات الفاعلة الحكومية من امتلاك أدوات جديدة تمكنهم من إجراء عمليات المراقبة، وجمع واستغلال كميات هائلة من البيانات الشخصية، والتأثير على العملية السياسية، والالتزام بمحاربة جميع أشكال الجرائم ومنها الجرائم السيبرانية. تتطلب هذه التحديات استجابات متعددة تجمع الحكومات (القطاع العمومي) والقطاع الخاص والمجتمع لمواجهة تحديات الأمن السيبراني. بالإضافة إلى ذلك، يجب أن تتكيف الأطر التشريعية والسياسية والحوكمة من أجل احترام حقوق الإنسان بشكل أفضل، مع مكافحة تطور الجريمة السيبرانية بكل أشكالها. وهذا ما سيعزز فضاء رقمي آمن ومستقر ومفتوح.

وبخصوص الجزائر يمكن اعتبار الأمن السيبراني من أولوياتها حاليا خاصة بعدما تبنّت خيار الحكومة الإلكترونية من خلال التحول الرقمي التدريجي للعديد من الخدمات العمومية لقطاعات كثيرة (وزارة الداخلية، العدل، التعليم العالي والتربية...). هذا التوجه صاحبه تبني سياسات تعتني بإدارة المخاطر السيبرانية والمعروفة بحوكمة الأمن السيبراني، والتي تشير إلى الأساليب المستخدمة من قبل العديد من أصحاب القرار (حكومات ومؤسسات) لتحديد وتأطير وتنسيق الأمن السيبراني، فلا يمكن تصور تحول رقمي للخدمات العمومية في ظل غياب استراتيجية واضحة وشفافة لضمان الأمن السيبراني. انطلاقا من هذه المقدمة، سنحاول من خلال هذه الدراسة باتباع منهج وصفي تحليلي الإجابة عن التساؤل الموالي:

لماذا من المهم للجزائر أن تتبنى حوكمة الأمن السيبراني لضمان تحول رقمي آمن للخدمة العمومية؟

فرضية الدراسة

وللمساهمة في الإجابة عن التساؤل وجب طرح الفرضية التالية:

إن التمكين القوي لحوكمة الأمن السيبراني في ظل ضوابط أساسية من شأنه مواجهة التهديدات والمخاطر السيبرانية في ظل التوجه نحو التحول الرقمي للخدمة العمومية في الجزائر.

أهداف الدراسة

تهدف الدراسة إلى إبراز أهمية تصور واضح المعالم لحوكمة الأمن السيبراني من خلال سياسة وطنية لإدارة مخاطر الأمن السيبراني وأمن المعلومات مع ضمان أداة دعمها من خلال توفير الوسائل التقنية، البشرية، القانونية والتشريعية تجعل تحديد ومواجهة التهديدات والمخاطر أكثر فعالية، والتي تمس مختلف القطاعات العمومية السيادية والقطاعات الصناعية والتجارية العامة منها والخاصة وحتى بيانات الأفراد والشخصيات العمومية، كل هاته الكيانات تعتبر جزء لا يتجزأ من الأمن القومي.

هيكل الدراسة

لمعالجة هذه الدراسة سنتطرق لمحورين، المحور الأول يتناول الإطار المفاهيمي لحوكمة الأمن السيبراني والمحور الثاني يتعلق بجهود الجزائر لحوكمة الأمن السيبراني لضمان تحول رقمي آمن للخدمات العمومية.

2. المحور الأول: الإطار المفاهيمي لحوكمة الأمن السيبراني والتحول الرقمي

1.2. ماذا يعني الأمن السيبراني؟:

أنتج عصر الإنترنت الكثير من المصطلحات ومنها مصطلح "الأمن السيبراني". وفيما يلي بعض الأمثلة لتعريفات الأمن السيبراني: (kohnke et al., 2016, p. 5)

أ. حالة الحماية من الاستخدام الإجرامي أو غير المصرح به للبيانات الإلكترونية، أو الإجراءات المتخذة لتحقيق ذلك. (قاموس أكسفورد الإنجليزي)

التدابير المتخذة لحماية الكمبيوتر أو نظامه (كما هو الحال على الإنترنت) من الوصول أو الهجوم الغير مصرح به (Merriam Webmaster).

ب. مجموعة التقنيات والعمليات والممارسات المصممة لحماية الشبكات وأجهزة الكمبيوتر والبرامج والبيانات من الهجوم أو التلف أو الوصول غير المصرح به (WhatIs.com).

ت. يشير إلى الأساليب الوقائية المستخدمة لحماية المعلومات من السرقة أو الاختراق أو الهجوم (Technopedia).

أما وزارة الدفاع الأمريكية (البنتاغون) فأعطت التعريف التالي: "جميع الإجراءات التنظيمية اللازمة لضمان حماية المعلومات بجميع أشكالها المادية والإلكترونية، من مختلف الجرائم سواء أكانت: الهجمات، التجسس، التخريب والحوادث" (Guerra, 2019).

يتكون الأمن السيبراني من ثلاثة عناصر رئيسية، تمثل منظومة الأمن السيبراني، وهي:

–القوة السيبرانية: يعتبر Joseph S. Nye, Jr أستاذ العلاقات الدولية الأب الروحي لمصطلح القوة السيبرانية ومن أهم من تحدثوا عنه، باعتباره شكل من أشكال القوة، حيث عرفها بما يلي: "القدرة على الحصول على النتائج المرجوة من خلال استخدام مصادر المعلومات المرتبطة بالفضاء السيبراني، أي أنها القدرة على استخدام الفضاء السيبراني لخلق مزايا، والتأثير في الأحداث المتعلقة بالبيئات الواقعية الأخرى، وذلك بواسطة أدوات إلكترونية"(Joseph S. Nye, Jr., 2010, p. 4). يعرفها Daniel T.Kuehl "بأنها القدرة على استخدام الإنترنت لخلق مزايا والتأثير على الأحداث في البيئات التشغيلية كافة من خلال أدوات القوة" (Daniel T. Kuehl, 2009).

–الدفاع السيبراني: عبارة عن آلية للدفاع عبر شبكة الكمبيوتر والتي تتضمن الاستجابة للإجراءات وحماية البنية التحتية الحيوية وضمان لمعلومات للمؤسسات والجهات الحكومية والشبكات الأخرى الممكنة. يركز على منع وكشف وتوفير الاستجابات في الوقت المناسب للهجمات أو التهديدات بحيث لا يتم العبث بالبنية التحتية أو المعلومات(techopedia - what is cyberpower?, 2021) . ويعرفه البرلمان الأوروبي بأنه "عملية تطبيق الإجراءات الأمنية من أجل الحماية من الهجمات السيبرانية، والتعامل معها، بما تستهدف تأمين البنية التحتية لنظم الاتصالات والسيطرة" (Cirlig, 2014).

–الردع السيبراني: التعريف الأكثر تداولا لمصطلح الردع هو تعريف الجنرال André Beaufre الذي عرف الردع بأنه "منع دولة معادية من اتخاذ قرار باستخدام أسلحتها أو منعها من العمل أو الرد إزاء موقف معين باتخاذ مجموعة من التدابير والإجراءات التي تشكل تهديدًا كافيًا حيالها، والنتيجة التي يراد الحصول عليها بواسطة التهديد هي نتيجة سيكولوجية نفسية(Beaufre, 1964)". أما فيما يخص الردع السيبراني فيمكن تعريفه على أنه:"منع الأعمال الضارة ضد الأصول الوطنية في الفضاء والأصول التي تدعم العمليات الفضائية"(Krepon, 2013). الردع السيبراني هو في حقيقته استراتيجية تظهر من خلاله الدولة الحريصة على الدفاع عن أمنها ومصالحها، نيتها في إقناع أي خصم بالتخلي عن النشاط السيبراني المدمر من خلال استهداف منظومة صنع القرار والتأثير فيها بهدف إثارة الخوف والرعب (Iasiello, 2018, p. 37).

2.2. تعريف حوكمة الأمن السيبراني:

تشير "حوكمة الأمن السيبراني" أو "حوكمة تكنولوجيا المعلومات" إلى وسائل إدارة أمن المعلومات وكذلك وسائل تنظيم الأنظمة الأمنية المطبقة في المنظمة لتحقيق أهدافها. من هذا المنطلق، فإن حوكمة الأمن السيبراني هي عملية مستمرة وتشكل جزءًا لا يتجزأ من ثقافة المنظمة، وتدمج إدارة المخاطر وتتوافق استراتيجيًا مع أهدافها. يحدد القواعد الأمنية التكتيكية والتشغيلية، مثل تنفيذ الضوابط المناسبة. ولذلك فهي تضمن الامتثال للمعايير المعمول بها والاتساق في تنفيذ الإطار المعياري. سواء أكانت تخضع لـ NIST 800-53[1] أو ISO 27000[2] أو معيار أمان بيانات صناعة بطاقات الدفع (PCI DSS)، يجب على المنظمات الالتزام بمتطلبات محددة واعتماد أفضل الممارسات الأمن السيبراني. يعد تطوير السياسات والمبادئ التوجيهية والإجراءات نقطة البداية لإطار عمل الحوكمة، وإنشاء برنامج أمان شامل لضمان تطبيق مبادئ وتدابير وضوابط الأمان داخل المنظمة (« Gouvernance & Conformité | Sécurité de l'information | Okiok », 2018).

يعرّف معيار ISO / IEC 27001، من المنظمة الدولية للتوحيد القياسي (ISO) واللجنة الكهرو تقنية الدولية (IEC)، حوكمة تكنولوجيا المعلومات على أنها "النظام الذي توجه المنظمة من خلاله وتتحكم في حوكمة الأمن، ويحدد إطار المساءلة ويوفر الإشراف على ضمان التخفيف من المخاطر بشكل مناسب، بينما تضمن الإدارة تنفيذ الضوابط للتخفيف من المخاطر" (Swinton & Hedges, 2019). تشير كذلك حوكمة قطاع الأمن السيبراني على وجه التحديد إلى تطبيق مبادئ الحوكمة لتوفير وإدارة ومراقبة الخدمات الأمنية، في سياق وطني معين. بالإضافة إلى ذلك، يستند مفهوم حوكمة الأمن السيبراني على فكرة أن قطاع الأمن يجب أن يخضع لنفس المعايير العالية مثل تلك المفروضة على مقدمي خدمات القطاع العمومي الآخرين. ولهذا، فإن عدم استيفاء قطاع الأمن لهذه المعايير يمكن أن يقوض الاستقرار السياسي والاقتصادي والاجتماعي للدولة (V.Puyvelde & F.Brantly, 2019).

3.2. التصورات المختلفة لحوكمة الأمن السيبراني:

تشكل حوكمة الأمن السيبراني واحدة من أربع قضايا لسياسة حوكمة الإنترنت، والتي تتضمن: تنظيم النزاعات السيبرانية، حماية البنية التحتية للمعلومات الحيوية، والجرائم الإلكترونية، والإرهاب السيبراني(Kurbalija, 2014). باتباع نفس المنهجية، اعتبر كل من Raymond & DeNardis حوكمة الأمن السيبراني على أنها واحدة من ست مجالات وظيفية متميزة لحوكمة الإنترنت، وتشمل: التحدي المتمثل في تأمين البنى التحتية الأساسية المشتركة لحوكمة الإنترنت، تحديد معايير الإنترنت، تنسيق الوصول والربط البيني، حوكمة الأمن السيبراني، وساطة المعلومات، الملكية الفكرية القائمة على هندسة إنفاذ الحقوق (DeNardis & Raymond, 2013, p. 588). وعلى وجه التحديد، اعتبرا أن المهام التالية تقع ضمن اختصاص حوكمة الأمن السيبراني: تأمين البنية التحتية للشبكة؛ تصميم معايير التشفير؛ اعتماد اللوائح؛ تصحيح الثغرات الأمنية للبرامج؛ إدارة دورات الترقيع، تأمين التوجيه والعنونة (Routing & Addressing) ونظام أسماء النطاقات (DNS)، الاستجابة لمشاكل الأمن، واعتماد وسطاء المصادقة (DeNardis & Raymond, 2013, p. 589) . بمجرد الأخذ بعين الاعتبار النطاق الكامل للتأثيرات التقنية والاجتماعية والسياسية والاقتصادية، تصبح فكرة وجود هيكل حوكمة واحد للأمن السيبراني أمرًا لا يمكن الدفاع عنه. لا يوجد نموذج واحد للحوكمة قادر على معالجة جميع الجوانب المختلفة للأمن السيبراني بشكل فعال. فحسب Dutton "من يحكم الأجزاء المختلفة من هذه الفسيفساء يختلف بشكل كبير. بعض المجالات يسيطر عليها الخبراء الفنيون، والبعض الآخر من قبل الوكالات الحكومية، والبعض الآخر من قبل المسؤولين

[1] عبارة عن منشور يوصي بضبط الأمن لأنظمة المعلومات والمؤسسات الفيدرالية والضوابط الأمنية.

[2] هو المعيار الذي تطبقه الشركات لضبط جودة أمن المعلومات.

التنظيميين، والبعض الآخر من قبل المستخدمين، والقائمة طويلة"(H. Dutton & Peltu, 2005). تستلزم حوكمة الأمن السيبراني أنماطًا متعددة للحوكمة، بما في ذلك الأنماط الهرمية والقائمة على أصحاب المصلحة المتعددين وكذلك على السوق (Leigh Keast et al., 2006). وللتوضيح، تصف الحوكمة الهرمية نمطًا من أعلى إلى أسفل للتنظيم (P. Osborne, 2010) وتتميز الحوكمة الهرمية بظهورها في سياق الأزمات وعدم اليقين الكبير، وبأنها أنظمة فردية القيادة وتتميز كذلك بالسيطرة المركزية، فضلاً عن إجراءات صارمة للمساءلة الداخلية والخارجية. يهيمن عليها متخذي القرار الحكوميون والتابعون للدولة. وعلى النقيض من الحوكمة الهرمية، تشير حوكمة السوق إلى نوع من التنظيم التصاعدي، منظم وفقًا لمبادئ المنافسة والكفاءة؛ التفكير الخدمي وإضفاء الشرعية على المخرجات هما محور هذا النوع من الحوكمة. في شكلها المثالي النموذجي، تمثل حوكمة السوق اللامركزية وإنشاء وحدات مستقلة وذاتية (الجهات الفاعلة الخاصة) (Meuleman, 2008). فيما تمثل حوكمة أصحاب المصلحة المتعددين منتصف الطريق بين الحوكمة الهرمية وحوكمة السوق، وتعتمد على علاقات التبادل بين مجموعة واسعة من أصحاب المصلحة الحكوميين أو غير الحكوميين كطريقة لتحقيق أهداف مشتركة(Leigh Keast et al., 2006). تتشكل ساحة حوكمة الأمن السيبراني الحالية من جوانب جميع أشكال التوجيه الثلاثة، بحيث تتضمن القرارات الإدارية للقطاع الخاص والعقود فيما بينها، بقدر ما تقوم بجهود الترتيب الهرمي والمقاربة القائمة على أصحاب المصلحة المتعددين. أحيانا، تتداخل هذه الأشكال المختلفة من التفاعل مع توفير الأمن السيبراني؛ وأحيانا أخرى، تظهر في شكلها المثالي (Ryan Ellis & Vivek Mohan, 2019, p. 82).

3.2. الطريق إلى النضج السيبراني:

في بيئة تزداد فيها تعقيدات التهديدات والمخاطر، تكافح العديد من المنظمات في تنفيذ وفرض حوكمة فعالة للأمن السيبراني. يوضح انفوجرافيك "إدارة مخاطر الأمن السيبراني: أزمة ثقة" الذي أعده معهدي CMMI وISACA أنه "بينما يدرك قادة المؤسسات أن الأمن السيبراني الناضج ضروري للازدهار في الاقتصاد الرقمي اليوم، فإنهم غالبًا ما يفتقرون إلى الرؤى والبيانات للتأكد أن المنظمة تدير المخاطر الإلكترونية بكفاءة وفعالية " (Managing Cybersecurity Risk, 2020). كما يُظهر أن الأضرار الناجمة عن الجرائم الإلكترونية من المتوقع أن تكلف العالم 6 تريليونات دولار سنويًا بحلول عام 2021، ارتفاعًا من 3 تريليونات دولار مقارنة لعام 2015، وفقًا لـ Cybersecurity Ventures في حين أن 87٪ من المتخصصين في C Suite وأعضاء مجلس الإدارة يفتقرون إلى الثقة في قدرات الأمن السيبراني لشركتهم. إذن كيف يمكن لمتخذي القرار أن يثقوا في هذا المشهد الغير مؤكد خاصة في ظل جائحة كورونا (covid-19)؟ يتمثل أول طلب موجه لمعظم المنظمات يكمن في التمكين لبرنامج حوكمة قوي للأمن السيبراني (Pam Nigro, 2020).

4.2. خطوات حوكمة الأمن السيبراني:

سبع خطوات يجب أن يتبعها متخذي القرار لبرنامج حوكمة الأمن السيبراني:

أ. تحديد الوضع الحالي: تقييم المخاطر الإلكترونية لفهم الثغرات وإنشاء خارطة طريق لسد تلك الفجوات.

ب. إنشاء، مراجعة، تحديث جميع سياسات ومعايير وعمليات الأمن السيبراني، على مستوى هذه الخطوة وجب أخذ الوقت الكافي لإنشاء هيكل وتوقعات حوكمة الأمن السيبراني.

ت. مقاربة الأمن السيبراني من منظور المؤسسة: تحديد ما هي البيانات التي يجب حمايتها؟ وكيف تتماشى المخاطر السيبرانية مع إدارة مخاطر المؤسسة؟ كذلك ما هي الأولوية النسبية للاستثمار في الأمن السيبراني مقارنة بأنواع الاستثمارات الأخرى؟

ث. زيادة الوعي والتدريب في مجال الأمن السيبراني: ربما ساهمت جائحة كورونا COVID-19 في بلورة هذا التوجه خاصة فيما يخص التدريب، مع وجود الكثير من الأشخاص الذين يعملون من المنزل والتعليم عن بعد، فمن الأهمية بمكان أن يعي الجميع أن الأمن السيبراني من مسؤولياتنا ومن هذا المنطلق ظهر ما يعرف بالنظافة السيبرانية (Cyber Hygiene) (Abi tyas, 2021).

ج. تحليلات المخاطر السيبرانية: كيف يتم وضع نماذج التهديدات والمخاطر وتقييمها؟ عند إنشاء نموذج المخاطر، يجب الأخذ بعين الاعتبار جميع المخاطر التي تتعرض لها المنظمة (الخارجية والداخلية).

ح. المراقبة والقياس والتحليل والإبلاغ والتحسين: القيام ببرمجة فترات تقييم منتظمة، والقيام بقياس ما يهم، ومن ثم تحليل البيانات وإنشاء خطة تحسين. مع تقديم تقرير إلى متخذي القرار حول النضج السيبراني وموقف المخاطر السيبرانية.

خ.أخيرًا، القيادة مهمة: "Tone at the top – النغمة في القمة" إن جعل الأمن السيبراني وحوكمة الأمن السيبراني أولوية لدى القيادة العليا وذلك بأن تعمل كل السياسات والمعايير والعمليات على مواءمة حوكمة الأمن السيبراني مع أولويات الأمن السيبراني بحيث لا يتغير التركيز مع تغير المبادرين بها(Pam Nigro, 2020).

5.2. مفهوم التحول الرقمي:

لتوضيح مفهوم التحول الرقمي سوف نتطرق إلى بعض تعاريف شركات الأبحاث والاستشارات الرائدة عالميا، والهيئات المتخصصة والمنظمات العالمية:

تعريف التحول الرقمي:

يمكن أن يشير التحول الرقمي إلى أي شيء: من تكنولوجيا المعلومات الحديثة (مثلا الحوسبة السحابية) إلى التحسين الرقمي، إلى اختراع نماذج أعمال رقمية جديدة. يستخدم المصطلح على نطاق واسع في مؤسسات القطاع العمومي للإشارة إلى المبادرات المتواضعة مثل وضع الخدمات على الإنترنت أو التحديث القديم. وبالتالي، فإن المصطلح يشبه "الرقمنة" أكثر من "التحول الرقمي للأعمال" (*Definition of Digital Transformation - Gartner Information Technology Glossary*, 2021) . أما Deloitte فعرفته كما يلي: التحول الرقمي هو استخدام التكنولوجيا لتحسين أداء أو ارتقاء مؤسسة بشكل جذري. في الأعمال التجارية التي تم تحويلها رقميًا، تمكّن التقنيات الرقمية من تحسين العمليات وتفاعل المواهب ونماذج الأعمال الجديدة(Verina & Titko, 2019, p. 721). أما منظمة التعاون الاقتصادي والتنمية (OECD) فعرفته كما يلي: "يشير التحول الرقمي إلى الآثار الاقتصادية والمجتمعية لـ digitization وdigitalization. فيما يخص digitization فهي تحويل البيانات والعمليات التناظرية إلى تنسيق يمكن للآلة قراءته. أما digitalization فهي استخدام التقنيات والبيانات الرقمية وكذلك ربطها مما يؤدي إلى تغييرات جديدة أو تغييرات في الأنشطة الحالية "(OECD, 2018).

6.2. نحو التحول الرقمي للخدمة العمومية:

يعد التحول الرقمي بأشياء عظيمة للقطاع العمومي والجهات المكونة التي يخدمها، من انخفاض التكاليف وزيادة الكفاءة إلى الخدمات في الوقت الفعلي، والتواصل السلس، وتعزيز فعالية البرنامج، إضافة إلى جودة الخدمة والرضى الذي تتلقاه من مختلف المستخدمين (الجمهور والشركات). يوفر التحول الرقمي التكلفة والجهد بشكل كبير ويحسن الكفاءة التشغيلية وينظمها، كما أنه يعمل على تحسين جودتها وتبسيط إجراءات الحصول على الخدمات المقدمة ويخلق فرص لتقديم خدمات مبتكرة وإبداعية ستساهم بدورها في خلق حالة من الرضى والقبول من الجمهور تجاه الخدمات التي تقدمها في هذا الصدد منظمات القطاع العمومي، وتعتبر تطبيقات المحمول أو المواقع الالكترونية والأرضيات الخاصة إحدى هذه الطرق، وبمجرد تطبيق هذه المفاهيم سيتكون كم هائل من البيانات والمعلومات التي

ستساعد بدورها متخذي القرار في هذه المنظمات على مراقبة وتقييم الأداء وتحسين جودة خدماتها بالإضافة إلى تحليل هذه البيانات والمعلومات التي ستسهل اتخاذ القرار وتحديد الأهداف والاستراتيجيات(عامر, 2018). ولكن لن تتحقق هذه المكاسب إلا إذا كانت القيادة والموظفون على جميع المستويات على قدر المهمة، حيث أن هناك عمل ليس بالسهل يتعين على الجميع القيام به لتحقيق الأهداف المسطرة. التحول الرقمي في بيئة رقمية متطورة يدفع المنظمات إلى العمل بسرعة أكبر لاستكشاف الفرص الجديدة التي تتيحها الرقمنة المتقدمة. يجب أن تركز المنظمات على توليد أفكار مبتكرة وذلك بخلق قيمة للجمهور والعملاء، وتصميم الخدمات الممكّنة رقميًا بسرعة باستخدام التكنولوجيا المتطورة وبناء القدرة التنظيمية لتقديم مثل هذه الخدمات لتلبية توقعات المستخدم النهائي والعملاء على حد سوى (R Tanniru, 2018). وفي نفس الوقت يتطلب ذلك وجود قائد يتمتع باتخاذ قرارات سريعة وصحيحة يمكنه التأثير على تصرفات الآخرين للحث على الأداء المرغوب فيه والفعال طبعا بكل تأكيد. يتطلب اتخاذ القرار والتصميم الأسرع وتقديم هذه الخدمات الرقمية مرونة في استعمال تكنولوجيا المعلومات تحت القيادة المشتركة لمديري تكنولوجيا المعلومات، والقائد الرقمي، مع دور مركزي لهذا الأخير في اتخاذ القرار بسرعة للدفع نحو التغيير (De Waal et al., 2016). على القائمين على القطاع العمومي أن يعوا أن أي تحول رقمي ناجح لا يتم بدون ثقافة مؤسسية جديدة، بل يجب عليه دمج ثقافة التغيير في هياكله. وفي هذا الصدد لا يمكن الحديث عن التحول الرقمي وثقافة التغيير دون الحديث عن الابتكار. في الواقع، الابتكار عامل مهم لتسريع التحول الرقمي. يسمح الابتكار التشاركي للمنظمة بإشراك مجتمعها بأكمله لتقديم المشورة وإثراء عملية صنع القرار من أجل الاستجابة بشكل جماعي وبأفضل طريقة ممكنة لمختلف مشاكل المؤسسة العامة. يواجه هذا التحول الرقمي العديد من العقبات وللتغلب عليها يجب على القطاع العمومي تركيز جهوده من خلال الاستثمار بشكل أساسي في العامل البشري الذي يمثل المحور المركزي لهذا التحول. بعدها، يجب أن يكون الابتكار والتغيير جزءًا من ثقافة المنظمة. والهدف من ذلك هو تطوير ثقافة تنظيمية أكثر انفتاحًا وابتكارًا، وبالتالي تسهيل وتعزيز التغيير داخل القطاع العمومي. يمكن اعتبار الرأس المال البشري هو المحرك الحقيقي لهذا التحول، والجانب التكنولوجي لا يمثل سوى بُعد واحد من العملية. وفقًا لدراسة أجرتها كل من (IBM, BCG, EBG)خلال عام 2018، تعتقد 61٪ من الشركات أن العامل البشري مهم وسيكون له تأثير كبير على التحول الرقمي خلال السنوات المقبلة. ورغم ذلك تفشل 70٪ من مشاريع التحول الرقمي داخل الشركات لأن العامل البشري غالبًا ما يتم تجاهله. إذن من المهم، وقبل الشروع في أي مشروع تحوّل، على القطاع العمومي التفكير أولاً في تدريب موظفيه. ليكونوا قادرين على إتقان أساليب العمل الجديدة والأدوات التكنولوجية الجديدة التي سيستخدمونها(Beuve et al., 2021) .

7.2. الأمن السيبراني حجر الأساس في التحول الرقمي للخدمة العمومية:

قد يعتبر البعض أن الأمن السيبراني مشكلة تقنية وفقط، لكن واقعيا الحلول تتطلب مقاربة متكاملة تغطي الأشخاص والعمليات والتكنولوجيا. فالأشخاص يمكن اعتبارهم مفتاح مهم لتحسين الأمن السيبراني ويمكن تمييز ثلاث مجموعات رئيسية من الأشخاص المعنيين: المستخدمون وصناع القرار وخبراء الأمن السيبراني. يجب أن يزداد الوعي لدى هؤلاء بالمخاطر المهددة، وذلك بتزويدهم بمعلومات حول الإجراءات الممكنة، علما أن حملات التوعية والتدريب والتمارين تساعد المستخدمين. يواجه صناع القرار التحدي المتمثل في ترجمة المخاطر السيبرانية إلى مخاطر أعمال واتخاذ الإجراءات المناسبة. يعد الحصول على الحقائق وتفسير أهمية هذه الحقائق من التحديات المهمة، حيث أن مصدر الاختراق غالبًا ما يكون عالي التقنية. أما فيما يخص خبراء الأمن السيبراني فأي نقص في كفاءتهم ومهاراتهم يعد مصدر قلق خطير لكل من الشركات والحكومات. إذ بدونهم من يستطيع التفوق على المخترقين؟ أما العمليات والتنظيم فهي مكونات مهمة في تحسين الأمن السيبراني. وهذا يشمل القيادة والسياسات واللوائح والعمليات والميزانيات وإدارة استمرارية الأعمال وآليات تخطيط-إجراء-التحقق-التنفيذ (Plan-Do-Check-Act) (Hoorweg & de Graaf, 2012) وهي صلب حوكمة الأمن السيبراني. وأخيرا جانب التكنولوجيا

الذي يكمن اعتباره الجانب الواضح والذي يهمين على النقاشات حال تناول الأمن السيبراني. هناك العديد من الميادين المهمة والمستعجلة، كتكامل الشبكة، وما يعرف بـ (BYOD: Bring Your Own Device) أي احضر جهازك الخاص وأنظمة التحكم في العمليات وتطبيقات الويب. كما أن تحسين الوعي بالأوضاع داخل وخارج شبكات المنظمات من خلال الكشف والذكاء السيبراني، سيساهم في قدرة المنظمات على الاستجابة للهجمات الإلكترونية. أي نظام معلومات المستعمل والمعتمد عليه يوميًا والمترابط، ومفتوح للمستخدمين سواء أكانوا جمهور المواطنين أو مختلف الهيئات والمؤسسات، ويستقبل مختلف البيانات من بيئات متعددة: الحوسبة السحابية، والاتصالات المتنقلة، وإنترنت الأشياء وغيرها، بوابة محتملة للهجمات السيبرانية. هذه الهجمات يتزايد عددها وأصبحت أكثر تعقيدًا، لذا فإن أمن البيانات وأمن الشبكة بأكملها يصبح مسؤولية وجب التخطيط الفعال لضمانها، لإعطاء الثقة اللازمة لمستخدميها. فالمقولة تقول "بدون الثقة، لا يوجد تحول رقمي. وبدون الأمن السيبراني، لا توجد ثقة"(Talel, 2019). هذا يعني الثقة في استخدام البيانات وفي الأنظمة التي تنتجها، والتي استضافتها أو وزعتها، وفي نهاية المطاف، الثقة في مختلف الجهات الفاعلة من شركات وشركاء والموردين والخدمات العمومية. من منطلق الرغبة في خلق بيئة ثقة، وإيمانًا بضرورة تأمين المستقبل الرقمي لمختلف شرائح المستخدمين وكذلك في الالتزام بتحقيق الثقة لذلك لن يتم كل هذا إلا من خلال الأمن السيبراني(Towers Clark, 2020).

3. المحور الثاني: جهود الجزائر لحوكمة الأمن السيبراني لضمان تحول الرقمي آمن للخدمة العمومية

1.3 ضرورة حوكمة الأمن السيبراني في الجزائر:

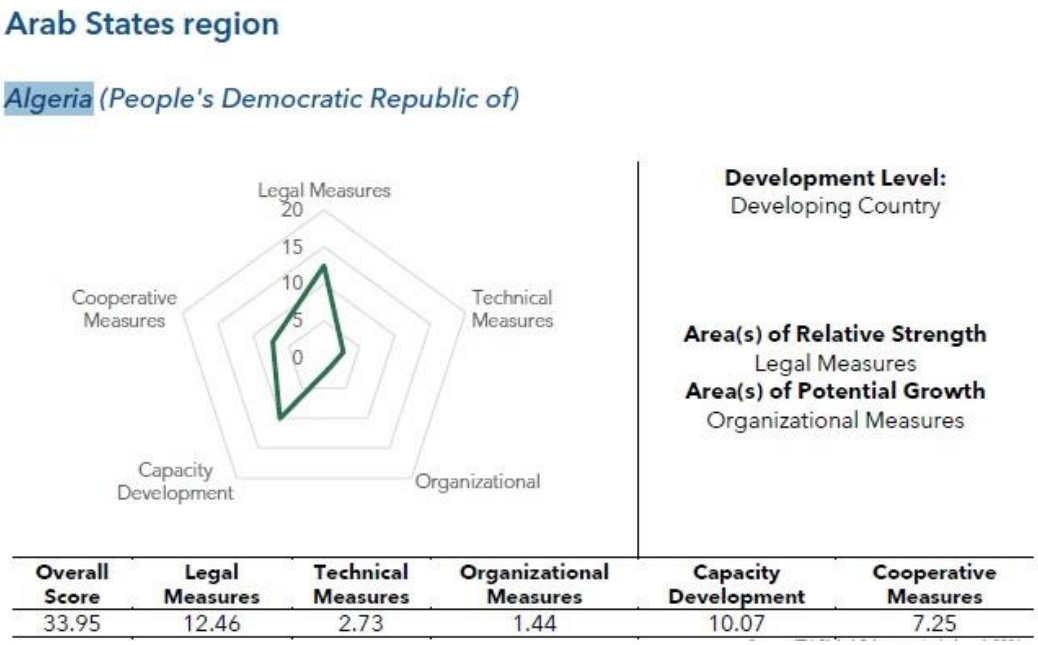
إن زيادة وتوسع التحول الرقمي يقابله الحاجة في التمكين لحوكمة أمن سيبراني قوي وشفاف يضمن الفعالية والثقة للخدمات العمومية الرقمية الموجهة للجمهور ويشجع على التشابك بين مختلف مصالح وإدارات القطاع العمومي والهيئات السيادية للدولة الجزائرية (حسب دراسة لمعهد كلارد–جامعة ماريلاند تحدث هجمات سيبرانية كل 39 ثانية) (Pancholi & Strobl, 2018). والجزائر بوقعها الجيو–إستراتيجي يجعلها عرضة لمختلف التهديدات والمخاطر المختلفة وعلى رأسها المخاطر الأمنية التي يمثل جزء من في المخاطر السيبرانية العابرة للحدود والتي تقف ورائها في كثير من الأحيان قوى خفية هدفها الاستقرار السياسي والاجتماعي والاقتصادي للجزائر. وما قضية بيغاسوس الإسرائيلي عنا ببعيدة، وكانت صحيفة لوموند الفرنسية ومنصة Forbidden Stories ذكرتا أن المغرب كانت واحدة من أكثر دول العالم استخداماً لبرنامج "بيغاسوس– Pegasus " الإسرائيلي، **الذي أثيرت حوله فضيحة تجسس كبيرة في الأيام الأخيرة. هذه الحوادث تمثل ناقوس الخطر للاستعداد لمواجهة أصعب التحديات في مجال الأمن، باعتبار أن كل الدول تعتمد للحد من خطورة ما يحمله الفضاء السيبراني على سياسات وبرامج وقائية أو ردعية سواء تعلق الأمر بالأليات القانونية تتكفل بتنفيذها الجهات المخولة (المؤسسات الأمنية والقضائية) أو أليات تعتمد على التحكم في تكنولوجيا المعلومات والاتصالات من خلال كل التقنيات المتعلقة بالأمن، التصدي والمتابعة.**

2.3 واقع الأمن السيبراني في الجزائر:

حسب المؤشر العالمي للأمن السيبراني (GCI) (ITU-Global Cybersecurity Index 2020 Measuring commitment to cybersecurity, 2021, p. 26 & 29) الذي يصدره الاتحاد الدولي للاتصالات(ITU) ، التابع للأمم المتحدة، فإن الجزائر تحتل المرتبة 104 عالميا من مجموع 182 بلد و12 عربيا من مجموع 22 بلد عربي (للإشارة أن الولايات المتحدة تحصلت على العلامة الكاملة 100 نقطة، وهذا ما يؤشر على نجاعة الحوكمة في هذا الميدان)، وهي مرتبة متأخرة مقارنة بالإمكانيات البشرية والمادية التي تمتلكها، لذا وجب عليها إعطاء أهمية قصوى لما له من تأثير خطير على الأمن الوطني. وحسب نفس القرير فإن مؤشر الأمن السيبراني للجزائر تحصل

على 33.95 نقطة من مجموع 100 نقطة، حسب المجالات التالية: الإجراءات القانونية 12.46 نقطة من مجمع 20 نقطة ويمكن اعتبارها نتيجة مرضية، الإجراءات التقنية 2.73 نقطة ومن هنا تظهر هشاشة الأمن السيبراني في هذا المجال، الإجراءات التنظيمية 1.44 نقطة وهو أضعف تنقيط، رغم المحاولات والمجهودات المبذولة في ميدان وضع هياكل إدارية وتنظيمية لإدارة الأمن السيبراني، أما مجال تنمية القدرات فتحصل على 10.07 ويمكن قراءتها على أنها تنقيط متوسط إلى إيجابي وأخيرا مجال إجراءات التعاون فكان تنقيطه 7.25 وهو تنقيط دون المتوسط.

الشكل رقم (01): مؤشر الأمن السيبراني للجزائر



Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
33.95	12.46	2.73	1.44	10.07	7.25

المصدر:(ITU-Global Cybersecurity Index 2020 Measuring commitment to cybersecurity, 2021, p. 71)

كما أشار آخر تقرير لمنصة (datareportal.com) المتخصّصة في جمع البيانات الإحصائيات في شتى المجالات، حيث أوضحت أخر الإحصائيات الخاصة بالجزائر، أن عدد المتصّلين بالأنترنت في الجزائر، بلغ عددهم حتى جانفي 2021 حوالي 26.35 مليون شخص بارتفاع قدره 3.6 مليون مشترك جديد مقارنة بنفس الفترة من العام الماضي. ويوّضح نفس المصدر أن نسبة استخدام الأنترنت في الجزائر بلغت 59.6 ٪ من مجموع السكان الذي يبلغ عددهم 44.23 مليون. كل هذه الأرقام تدل على تطور الانترنت في وخدماتها في الجزائر، ويمكن اعتبارها خطوة مهمة نحو بناء مجتمع معلوماتي أكثر توسعا، ولكنها في نفس الوقت تبرز الحاجة الملحة لزيادة الحماية الالكترونية على المستوى الوطني لتعزيز الأمن السيبراني في الجزائر. (*Africa*, 2021) وحسب نفس التقرير فإن أهم مؤشرات الأمن السيبراني في الجزائر تتمثل في: الاستعداد للهجمات السيبرانية: 0.262 من 1 ونسبة الهواتف المحمولة المصابة ببرامج ضارة: 26.47 ٪، ونسبة أجهزة الكمبيوتر المصابة ببرامج ضارة: 19.75. نسبة المستخدمين الذين تعرضوا لهجمات البرمجيات الخبيثة المالية: 0.5 ٪، النسبة في الجزائر تعتبر مقبولة مقارنة بأفضل نسبة وتحصلت عليها الدنمارك 0.1٪، ويعود السبب في حقيقة الأمر أن الجزائر لا تمتلك بعد منظومة نقدية إلكترونية موسّعة بشكل كبير وغالباً ما يتم نشر هذه البرمجيات عن طريق مواقع إلكترونية مخترقة أو احتيالية أو رسائل البريد غير المرغوب فيها. هذا الترتيب المتدّني للجزائر، يمكن ربطه بالثقافة المجتمعية الجزائرية في الفضاء السيبراني بشكل عام، فالمستخدم الجزائري في

غالب الأحيان لا يفرق بين التطبيقات المرخصة أو الخبيثة، حيث يقوم بتحميل تطبيقات أو برامج من أماكن غير موثوقة قد تحتوي على برامج للتجسس وسرقة البيانات، وحتى على مستوى العالم هناك إحصائية، مفادها أن 95٪ من الاختراقات في العالم تتم بسبب خطأ بشري. كل هذه المؤشرات تعطي انطباع أن التحول الرقمي للخدمة العمومية نجاحه مرتبط بنجاعة وفعالية برنامج وإستراتيجية حوكمة الأمن السيبراني في إطار التوجه نحو الحكومة الإلكترونية.

3.3 جهود الجزائر في تبني تصور لحوكمة الأمن السيبراني :

رغم حداثة هذا المفهوم في الجزائر وعدم تعميمه في أروقة الإدارات والهيئات المختلفة، إلا التحديات الأمنية في هذا المجال يحتم على الجزائر إعادة النظر في برامجها وخططها تماشيا مع تنوع وتعدد أنواع ومصادر الهجمات السيبرانية، مما يوحي بحجم المخاطر التي تواجهها الجزائر لتحقيق الأمن السيبراني حاضرا ومستقبلا. كما أن الأمن السيبراني بمفهومه الواسع سواء تعلق الأمر بجانبه التقني، أو التشريعي والقانوني، والهياكل الساهرة على تطبيقه، والأليات والخطط والبرامج المدرجة للوصول إلى فعالية في الأمن والحماية، كل هذه المتغيرات تبقى مهمة وعلى صنّاع القرار الاهتمام بها واعتبارها من الأولويات الملحة، خاصة وأن الجزائر تبنّت خيار الحكومة الإلكترونية لتسهيل التعاملات سواء الإدارية أو المالية والتجارية أو توفير الخدمات الإلكترونية العمومية للمواطن لتسهيل وتطوير حياته اليومية، تكون ذات جودة، سهلة الاستعمال مع توفير الحماية اللازمة للبيانات التي تتداولها هذه الخدمات. فمع الرجوع إلى مفهوم حوكمة الأمن السيبراني والذي يمثل مجموعة من الأنشطة التي تمكن المنظمات من اتخاذ قرارات سليمة في مجال الأمن السيبراني. سنحاول التطرق إلى هذه الجهود من خلال النقاط التالية:

– **الجانب القانوني والتشريعي:** لقد أقر المشرع الجزائري جملة من القوانين والتنظيمات، التي تؤطر النشاطات المتعلقة بتكنولوجيا المعلومات أو بالأمن السيبراني: (شماخ, 2018)

قانون رقم 09 – 04 لسنة 2009: يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها يهدف هذا القانون الى وضع قواعد خاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها.

التّصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحرّرة بالقاهرة بتاريخ 21 ديسمبر سنة 2010 مرسوم رئاسيّ رقم 14 – 252 مؤرّخ 8 سبتمبر سنة 2014 يتضمّن التّصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحرّرة بالقاهرة بتاريخ 21 ديسمبر سنة 2010 تنطبق هذه الاتفاقية ما لم ينص على خلاف ذلك على جرائم تقنية المعل ومات بهدف منعها.

قانون رقم 15 – 04 مؤرخ في سنة 2015: يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين يهدف هذا القانون إلى تحديد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين.

قانون رقم 18 – 04 لسنة 2018: يتضمن القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية: كتحديد وتطبيق معايير إنشاء واستغلال مختلف الخدمات، وأمن وسلامة شبكات الاتصالات الإلكترونية.

القانون رقم 18 – 07 يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي: يهدف هذا القانون إلى تحديد قواعد حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

القانون رقم 05 – 18 المؤرخ في 10 ماي 2018 المتعلق بالتجارة الإلكترونية: يحدد القواعد العامة للتجارة الالكترونية للسلع والخدمات والتي تتم عن طريق اقتراح أو توفير سلع وخدمات من طرف مورد إلكتروني لمستهلك إلكتروني، عن بعد وعن طريق الاتصالات الإلكترونية.

– **الجانب الهيكلي والمؤسساتي:** لضمان التنفيذ الفعلي والجدي لمختلف التدابير الهادفة لتحقيق المن السيبراني، أوكل متخذي القرار في الجزائر هذه المهمة إلى هيئات ومراكز متخصصة ضمن المؤسسات السيادية للدولة، نذكر منها:

المصلحة المركزية لمكافحة الجريمة المعلوماتية: وهي مصلحة تابعة لوزارة الداخلية (المديرية العامة للأمن الوطني)، يمتد نشاطها خارج الجزائر من التعامل مع أنتبول، أفريكوم أو مصالح الشرطة لكبرى الدول، وعلى المستوى الوطني تتواصل هذه الهيئة مع الشرطة العلمية والمكاتب اللامركزية المختصة في الاجرام.

مركز الوقاية من جرائم العلام الآلي والجرائم المعلوماتية: وهو مركز يتبع القيادة العامة للدرك الوطني (أي وزارة الدفاع الوطني)، يكاد لا تختلف مجال نشاطها ومهامها عن نظيرتها التابعة للأمن الوطني سواء محليا أو وطنيا، ويتم التنسيق بينهما تحت المسؤولية المباشرة للنائب العام على مستوى دائرة الاختصاص.

المعهد الوطني للأدلة الجنائية وعلم الجرام للدرك الوطني: التابع للقيادة العامة للدرك الوطني، يعتمد المعهد في أداء مهامه على الخبرة العلمية والتجارب المخبرية الدقيقة، مع استعمال التكنولوجيات الحديثة في كشف ملابسات الجريمة وتوقيف مقترفيها لتقديمهم للعدالة.

– الجانب الإداري والتنظيمي: لتحديد الصلاحيات والمسؤوليات وتفادي تداخلها، حرص متخذي القرار من خلال التشريعات والقوانين لوضع ضوابط إدارية تنظم صلاحيات كل من الهيئات المدنية، العسكرية والتقنية في مجال الأمن السيبراني:

الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات العلام والاتصال ومكافحتها: التي أنشئت سنة 2009، ووضعت تحت السلطة المباشرة لوزير العدل، دخلت حيز التنفيذ بعد صدور المرسوم الرئاسي رقم 15-261 المؤرّخ في 08 أكتوبر 2015.

مصلحة الدفاع السيبراني ومراقبة أمن الأنظمة الشعبي: أستحدث بتاريخ 11جوان 2015، على مستوى دائرة الاستعمال والتحضير لركان الجيش الوطني، وأوكلت لها مهمة، حماية المنظومات والمنشآت الحيوية للبلاد ضد كل أنواع الجريمة السيبرانية.)بوازدية, 2019(

إنشاء أول مركز للأمن السيبراني تابع لاتصالات الجزائر: والذي يسمح للعديد من المؤسسات والهيئات الاستفادة من خدماته من أجل مواجهة الهجمات السيبرانية، ويعتمد تنظيم المركز العملياتي للأمن على ثلاثة جوانب محورية هي: الاستجابة والاستباقية وجودة الأمن(Belhimer, 2021).

– الجانب التقني والعملياتي: إن الوصول إلى التكنولوجيات الحديثة الخاصة بالحماية والرقابة في مجال الأمن السيبراني أصبح من الضروريات القصوى لاسيما بعد تسرب أخبار بأن دول معينة تراقب هواتف عدد معتبر من الجزائريين (شخصيات كانت أو أفراد)، وقد تكون العملية أكبر من ذلك، لذا وجب الاستثمار في هذا الجانب، سواء بالتعاقدات مع الشركات الرائدة في هذا الميدان لدول استراتيجيا تعتبر صديقة وحليفة للجزائر.

4.3 إطار حوكمة الأمن السيبراني المقترح :

تخفف حوكمة الأمن السيبراني من التعرض للمخاطر باستخدام مجموعة من المعايير والضوابط. اعتمدنا في هذه الدراسة على إطار حوكمة الأمن السيبراني الهرمي الذي يتناول الترابط بين: السياسات وأهداف الرقابة والمعايير والتوجيهات والضوابط والمخاطر والإجراءات والمقاييس(Hierarchical Cybersecurity Governance Framework, 2021)، والتي يمكن بلورتها فيما يلي:

– السياسات: ترسم السياسات من طرف أصحاب القرار ويتم تصميمها للتأثير على القرارات وتوجيه المنظمة لتحقيق النتائج المرجوة، ويتم فرضها من خلال المعايير وكذلك من خلال إجراءات لتحديد متطلبات قابلة للتنفيذ وخاضعة للمساءلة. تحدد التقنية كيفية تنفيذ هذه السياسات، وعادة ما توضع السياسات لتلبية مطالب خارجية (مثل القوانين واللوائح وحتى التعاقدات).

– **أهداف التحكم**: هي الأهداف أو الشروط المرغوب الوصول إليها، بمعنى أخر تصف ما يجب تحقيقه كنتيجة عند تطبيق المنظمة لعنصر التحكم، وهو ما يهدف المعيار إلى معالجته لاحقا. ترتبط أهداف التحكم ارتباطًا مباشرًا مع الممارسة الصحيحة لمواءمة الأمن السيبراني والخصوصية مع الممارسات المقبولة.

– **المعايير**: المعايير هي متطلبات إلزامية فيما يتعلق بالعمليات والإجراءات والإعدادات المصممة لتلبية أهداف التحكم. يُقصد بالمعايير أن تكون دقيقة وإلزامية لإنشاء الحد الأدنى من متطلبات الأمن (MSR: Minimum Security Requirements)، والتي تضمن تصميم وتشغيل الأنظمة والتطبيقات والعمليات لتشمل الأمن السيبراني وحماية الخصوصية.

– **التوجيهات**: المبادئ التوجيهية هي ممارسات موصى بها تستند إلى ممارسات آمنة معترف بها في كل المجالات. تساعد الإرشادات على زيادة المعايير عندما يكون التقدير مسموحًا به. على عكس المعايير، تسمح التوجيهات للمستخدمين بتطبيق حرية التصرف أو مجال واسع لتفسيرها أو تنفيذها أو استخدامها.

– **الضوابط**: الضوابط هي الرابط المستخدم لإدارة المخاطر من خلال منع أو اكتشاف أو تقليل تهديد معين على التأثير سلبًا على العمليات. تنطبق عناصر التحكم بشكل مباشر على المعايير، ويستخدم اختبار التحكم بشكل روتيني في اختبار ما قبل التطبيق للتحقق من أن أي نظام قد استوفى الحد الأدنى من مستوى الأمان قبل أن يسمح باستخدامه في البيئة الحقيقية. غالبًا ما يتم إجراء الاختبارات المتكررة على ضوابط معينة للتحقق من الامتثال للالتزامات القانونية والتنظيمية وحتى التعاقدية.

– **الإجراءات**: الإجراءات هي مجموعة موثقة من الخطوات اللازمة لأداء مهمة أو عملية محددة وفقًا لمعايير قابلة للتطبيق. وتساعد في معالجة مسألة كيفية قيام المنظمة بالفعل بتشغيل سياسة أو معيار أو عنصر تحكم. الإجراءات بشكل عام هي مسؤولية السلطات التنفيذية، ولكن تحت إشراف متخذي القرار لضمان معالجة متطلبات الامتثال المعمول بها. تهدف نتيجة الإجراء إلى تلبية عنصر تحكم محدد.

– **المخاطر**: من الناحية العملية، يرتبط الخطر بنقص التحكم (إذا فشلت عملية التحكم، فما هي المخاطر التي تتعرض لها المنظمة؟) غالبًا ما يتم حساب المخاطر من خلال الصيغة: **التهديد x الضعف x العواقب**، في محاولة لتحديد الحجم المحتمل لحالة الخطر التي تحدث. في حين أنه من غير الممكن أن تكون لديك بيئة خالية تمامًا من المخاطر، فقد يكون من الممكن إدارة المخاطر عن طريق تجنبها أو تقليلها أو نقلها أو قبولها.

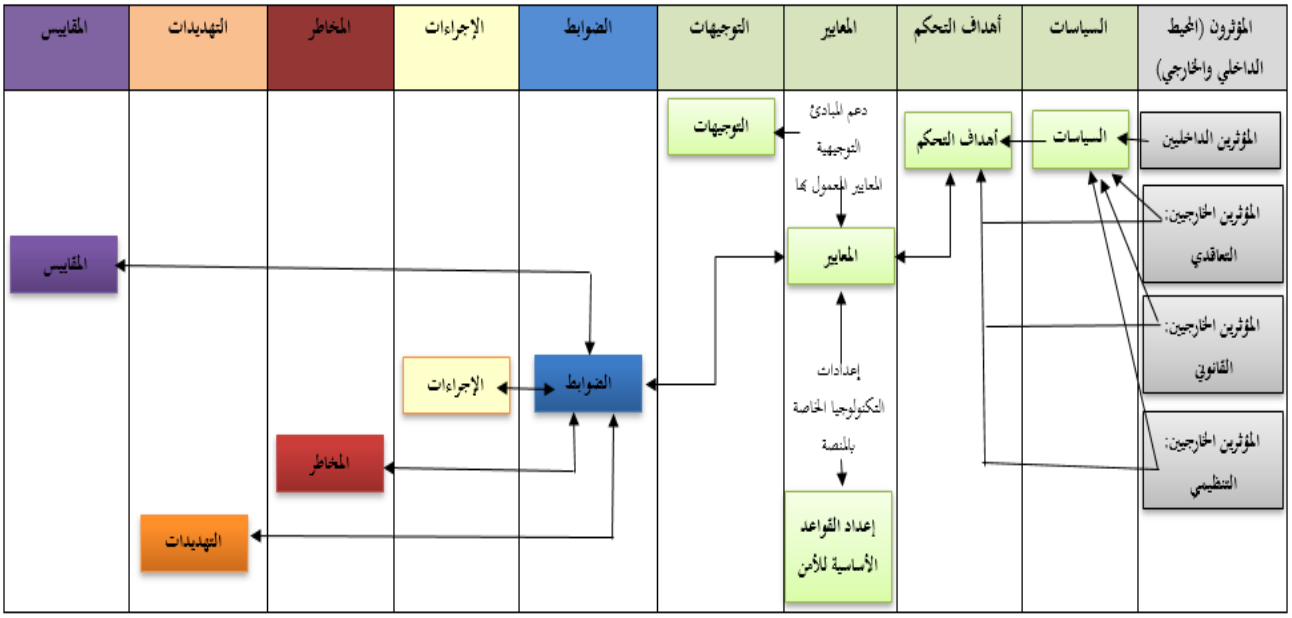
– **التهديدات**: يعد التهديد حدثًا طبيعيًا أو من صنع الإنسان والذي يؤثر على تنفيذ التحكم.

– **المقاييس**: توفر المقاييس وجهة نظر "نقطة زمنية Point In Time" لقياسات محددة منفصلة، على عكس الاتجاهات والتحليلات المستمدة من مقارنة خط الأساس لقياسين أو أكثر تم إجراؤها خلال فترة زمنية. يتم إنشاء التحليلات من تحليل المقاييس. تم تصميم التحليلات لتسهيل اتخاذ القرار وتقييم الأداء وتحسين المساءلة من خلال جمع وتحليل وإعداد التقارير المتعلقة بالبيانات ذات الصلة بالأداء. المقاييس الجيدة هي تلك التي تكون ذكية (محددة وقابلة للقياس ويمكن تحقيقها وقابلة للتكرار وتعتمد على الوقت) (Hierarchical Cybersecurity Governance Framework, 2021) .

الشكل رقم (02) يمثل إطار لحوكمة الأمن السيبراني الهرمي الذي يمكن اعتماده كإطار عام لبرنامج لحوكمة الأمن السيبراني، مع إجراء التعديلات الضرورية لتكييفه مع الواقع السياسي، الاجتماعي، الاقتصادي و الأمني للجزائر، فلا يمكن تصور نجاح الأمن السيبراني بدون ضوابط أساسية، والحوكمة جزء من هذه الضوابط التي تضم المكونات التالية: **– استراتيجية الأمن السيبراني – إدارة الأمن السيبراني – سياسات وإجراءات الأمن السيبراني – أدوار ومسؤوليات الأمن السيبراني – إدارة مخاطر الأمن السيبراني – الأمن السيبراني ضمن إدارة المشاريع المعلوماتية والتقنية – الالتزام بتشريعات وتنظيمات ومعايير الأمن السيبراني – المراجعة والتدقيق الدوري للأمن**

السيبراني (Essential Cyber security Controls, 2018, p. 12). هاته المكونات المتنوعة تتطلب كل على حدى دراسة منهجية ودقيقة، يمكن عند الانتهاء من إعدادها أن تكتمل الصورة وتتضح معالم حوكمة الأمن السيبراني. حينها يمكننا الحديث عن مكانة الأمن السيبراني في الجزائر ضمن المنظومة الأمنية ككل ومساهماتها في حماية الأمن القومي من كل أشكال التهديدات والمخاطر.

الشكل رقم (02): إطار لحوكمة الأمن السيبراني الهرمي(HCGF)



المصدر: (Hierarchical Cybersecurity Governance Framework, 2021)

من الأفضل عند اعتماد إطار لحوكمة الأمن السيبراني اتباع إطار عمل معترف به دوليًا، لأن هناك العديد من المعايير التي يمكن استخدامها كدليل لحوكمة الأمن السيبراني، على سبيل المثال يمكن أن نذكر: (COBIT) وهو إطار قياسي مكون من عدة أدوات تساعد متخذي القرار على تقليل الفجوة وتقليل المخاطر بين نظم المعلومات والاحتياجات الفنية واحتياجات الأعمال الأساسية للمؤسسة، والمعهد الوطني للمعايير والتكنولوجيا (NIST)، المنظمة الدولية للتوحيد القياسي (ISO)، اللجنة الفنية الكهربائية الدولية (IEC) وأخصائي أمن نظم المعلومات المعتمد (CISSP)، كذلك تتناول ISO/IEC 27032 الأمن السيبراني أو أمن الفضاء السيبراني ، والمعروف باسم "الحفاظ على سرية وسلامة وتوافر المعلومات في الفضاء السيبراني" (Maleh et al., 2021, p. 6).

4. الخلاصة:

إن التطور الرهيب للتكنولوجيا في جميع المجالات وخاصة في مجال تكنولوجيا المعلومات والاتصالات وما رافقه من انفجار العالم الافتراضي من خلال تنوع المحتوى والخدمات الذي تقدمه الإنترنت للبشرية جمعاء من ذكاء اصطناعي، وانترنت الأشياء، والواقع الافتراضي والواقع المعزز والحوسبة السحابية كل هاته الخدمات المذهلة والإيجابية صاحبتها في نفس الوقت أخرى سلبية ومدمرة متمثلة في التهديدات والمخاطر السيبرانية المختلفة من فيروسات ضارة إلى اختراقات وسرقات وتدمير للبيانات وتجسس. ويمكن أن تمتد إلى حروب سيبرانية تمس الأمن القومي، كل هاته التحديات تفرض على الجزائر الأخذ بأسباب المواجهة والتصدي لمختلف هاته التهديدات والمخاطر، وهذا بتبني

برامج متكاملة في ميدان الأمن السيبراني، وخاصة مع توجه الجزائر نحو الحكومة الإلكترونية من خلال التحول الرقمي لكل المرافق ومنها الخدمة العمومية.

وفي الختام إيجاز ما توصلنا إليه من نتائج فيما يلي:

– الأمن السيبراني من التحديات الصعبة التي تواجهها الجزائر في ظل تنامي كل أشكال التهديدات والمخاطر (المنظمة والإجرامية).

– الإحصائيات والمعلومات للهيئات والمنظمات الدولية كلها تشير إلى مدى هشاشة تشير الأمن السيبراني مع الأسف في الجزائر.

– نقائص واختلالات ملحوظة في مجال الإجراءات التنظيمية والجوانب التقنية مقارنة مع المعايير الدولية، رغم المجهودات المبذولة في هذا الميدان.

– غياب لمفهوم الحوكمة الأمن السيبراني في أروقة المؤسسات والإدارات ذات الصلة.

أما فيما يخص التوصيات فيمنك تلخيصها فيما يلي:

– لكسب رهان الأمن السيبراني، لابد من تقييم ما أنجز (تعديلات، إضافات، إعادة النظر...)، ليواكب التحول الرقمي للخدمة العمومية ويلائم التحديات السيبرانية التي تواجها الجزائر.

– على متخذي القرار في الجزائر نشر ثقافة (**المواطنة الرقمية** Digital Citizenship[3] و**النظافة الرقمية**[4] Cyber Hygiene) لخلق بيئة مناسبة للتحول الرقمي للخدمة العمومية.

– تحديد سياسة استباقية، تتفاعل مع هو حاصل أو محتمل في ميدان الأمن السيبراني، في الزمان والمكان المناسبين.

– التمكين لبرنامج لحوكمة الأمن السيبراني، اعتمادا على نماذج دولية ومعايير عالمية يمكن الاستفادة منها في بلورة هذه الفكرة ميدانيا.

– الاستفادة من تجارب الدول الرائدة في مجال الأمن السيبراني إقليميا ودوليا، سواء عن طريق الاتفاقيات الثنائية لتبادل الخبرات أو بالانضمام للمنظمات في مجال حماية أنظمة المعلومات والأمن السيبراني.

- تعزيز القدرات الوطنية وخاصة تلك الخاصة بالمؤهلات البشرية العاملة في أمن المعلومات وما إنشاء المدرسة العليا للرياضيات والذكاء الصناعي في الجزائر إلا دليلا على ذلك.

– ويبقى العنصر البشري في رأي المحرك الأساسي لرفع التحديات ومواجهة الصعاب، فالتكوين المستمر والنوعي، عامل لرفع مستوى الكفاءات والمهارات المطلوبة (التقنية، التنظيمية، الاستشرافية والقيادية...).

5. الإحالات والمراجع:

Abi tyas, tunggle. (2021). What is Cyber Hygiene and Why is it Important? *Technical Writer and Editor - TechTarget*. https://www.upguard.com/blog/cyber-hygiene

Africa : Internet penetration, by country 2020. (2021). Statista. https://www.statista.com/statistics/1124283/internet-penetration-in-africa-by-country/

Beaufre, A. (1964). *Dissuasion et stratégie*. imp. moderne de l'Est.

[3] المواطنة الرقمية هي مجموعة من الضوابط والإجراءات والقيم التي يحتاجها المواطن لتوجيه سلوكياته أثناء استخداماته اليومية للتكنولوجيا في الحياة اليومية، فيكون لها جوانب إيجابية تساهم في تعزيز الحماية مع توجيهه إلى السلوكيات الصحيحة للمنفعة (الجوانب الأخلاقية والمسؤولية).

[4] أما النظافة الرقمية تشير النظافة السيبرانية إلى الخطوات التي يمكن لمستخدمي أجهزة الكمبيوتر والأجهزة الأخرى اتخاذها لتحسين أمنهم عبر الإنترنت، كذلك تعني اعتماد عقلية وعادات تتمحور حول الأمن تساعد الأفراد والمؤسسات على التخفيف من الانتهاكات المحتملة عبر الإنترنت.

Belhimer, A. (2021, août 3). *Cyber security center*. المصدر. https://almasdar-dz.com/134564--الجزائر-تنشئ-أول-مركز-للأمن-السيبراني

Beuve, J., Cristofini, O., Gimenez, J., & Porcher, S. (2021, janvier). La transformation digitale du secteur public Atteindre les promesses et éviter les désillusions. *Les Policy Papers de la Chaire EPPP*, *6*. www.chaire-eppp.org/policy-papers

Cirlig, C. C. (2014). *Cyber defence in the EU Preparing for cyber warfare?* 10. http://www.europarl.europa.eu/thinktank

Daniel T. Kuehl. (2009). From Cyberspace to Cyberpower : Defining the Problem. *Cyberpower and National Security, National Defense University Press, Washington*.

De Waal, B., Outvorst, F., & Ravesteyn, P. (2016). *Digital Leadership: The Objective-Subjective Dichotomy of Technology Revisited*.

Definition of Digital Transformation—Gartner Information Technology Glossary. (2021). Gartner. https://www.gartner.com/en/information-technology/glossary/digital-transformation

DeNardis, L., & Raymond, M. (2013). Thinking Clearly About Multistakeholder Internet Governance. *SSRN Electronic Journal*, *7*(3). https://doi.org/10.2139/ssrn.2809780

Essential Cyber security Controls. (2018). National Cybersecurity Authority. https://ega.ee/wp-content/uploads/2019/03/Essential-Cybersecurity-Controls.pdf

Gouvernance & Conformité | Sécurité de l'information | Okiok. (2018). *OKIOK - Securité dans un monde en changement*. https://www.okiok.com/fr/services/gouvernance-conformite/

Guerra, F. (2019, août 28). *Cyber Security*. Political Encyclopedia. https://political-encyclopedia.org/dictionary/الأمن السيبراني

H. Dutton, W., & Peltu, M. (2005). The emerging Internet governance mosaic : Connecting the pieces. *Oxford Internet Institute*, *5*.

Hierarchical Cybersecurity Governance Framework. (2021). Hierarchical Cybersecurity Governance Framework. https://www.complianceforge.com/reasons/hierarchical-cybersecurity-governance-framework/

Hoorweg, E., & de Graaf, P. (2012). *No digital transformation without cybersecurity*. Capgemini Group.

Iasiello, E. (2018). La cyber-dissuasion est-elle une stratégie illusoire ? *ASPJ Afrique & Francophonie*, *7*(1). http://dx.doi.org/10.5038/1944-0472.7.1.5

ITU-Global Cybersecurity Index 2020 Measuring commitment to cybersecurity (Nº 4). (2021). Global Cybersecurity Index cover page. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf

Joseph S. Nye, Jr. (2010). Cyber Power. *Belfer Center for Science and International Affairs Harvard Kennedy School*, 30.

kohnke, anne, shoemaker, dan, & sigler, ken. (2016). *The complete guide to cybersecurity risks and controls*. CRC Press Taylor & Francis Group.

Krepon, M. (2013, septembre 16). *Space and nuclear deterrence*. https://www.thespacereview.com/article/2367/1

Kurbalija, J. (2014). Switzerland and Internet governance: Issues, actors, and challenges. *Politorbis -Revue de politique étrangère*, *57*(2). www.eda.admin.ch/politorbis

Leigh Keast, R., P. Mandell, M., & Brown, K. (2006). Mixing State, Market and Network Governance Modes: The Role of Government in 'Crowded' Policy Domains. *International Journal of Organization Theory and Behavior*, *9*(1), 25-50.

Maleh, Y., Sahid, A., & Belaissaoui, M. (2021). A Maturity Framework for Cybersecurity Governance in Organizations. *EDPACS The EDP Audit, Control, and Security Newsletter*, *63*(6). https://doi.org/0.1080/07366981.2020.1815354

Managing Cybersecurity Risk. (2020). https://www.isaca.org/resources/infographics/managing-cybersecurity-risk

Meuleman, L. (2008). *Public Management and the Metagovernance of Hierarchies, Networks and Markets, Contributions to Management Science*. Heidelberg: Physica-Verlag HD.

OECD. (2018). *GOING DIGITAL IN A MULTILATERAL WORLD*.

P. Osborne, S. (2010). *The New Public Governance? Emerging Perspectives on the Theory and Practice of Public Governance*. Routledge Taylor & Francis group.

Pam Nigro. (2020). *Cybersecurity governance: A path to cyber maturity*. https://searchsecurity.techtarget.com/post/Cybersecurity-governance-A-path-to-cyber-maturity

Pancholi, S., & Strobl, G. (2018). *Digital transformation and its impact on cybersecurity.* THE POWER OF BEING UNDERSTOOD-RSM.

R Tanniru, M. (2018). Digital Leadership. *intechopen*. https://doi.org/10.5772/intechopen.76045

Ryan Ellis, & Vivek Mohan. (2019). *Rewired Cybersecurity Governance*. John Wiley & Sons, Inc.

Swinton, S., & Hedges, S. (2019, juillet 25). *Cybersecurity Governance, Part 1: 5 Fundamental Challenges*. SEI Blog. https://insights.sei.cmu.edu/blog/cybersecurity-governance-part-1-5-fundamental-challenges/

Talel. (2019, juin 14). La cybersécurité, oxygène de la transformation digitale. *Webmanagercenter*. https://www.webmanagercenter.com/2019/06/14/435908/la-cybersecurite-oxygene-de-la-transformation-digitale/

techopedia—What is cyberpower? (2021). Icy Science. https://ar.theastrologypage.com/cyber-defense

Towers Clark, C. (2020). *Trust is a keystone of digital transformation*. Chairman at Pod Group. https://digileaders.com/trust-is-a-keystone-of-digital-transformation/?utm_source=siacial&utm_medium=social&utm_campaign=blog_promo&utm_content=Charles%20Towers-Clark

Verina, N., & Titko, J. (2019). Digital transformation: Conceptual framework. *Proc. of the Int. Scientific Conference "Contemporary Issues in Business, Management and Economics Engineering'2019", Vilnius, Lithuania*, 9-10.

V.Puyvelde, D., & F.Brantly, A. (2019). *Cyber security Politics, governance and conflicts in cyberspace*. Polity Press. politybooks.com

بوازدية، ج. (2019). الاستراتيجية الجزائرية في مواجهة الجرائم السيبرانية التحديات والافاق المستقبلي. *مجلة العلوم القانونية والسياسية*, *10*(1)، 1280-1283.

شماخ، و. (2018). *الإطار القانوني والتنظيمي المتعلق بالأمن السيبراني في الجزائر*. الحوار العربي الإقليمي واجتماع الخبراء حول ترابط حوكمة الأنترنت والأمن السيبراني، بيروت.

عامر، د. ع. (2018). اهمية التحول الرقمي للجهاز الاداري للدولة. *الصدى.نت*. http://elsada.net/86221/ .