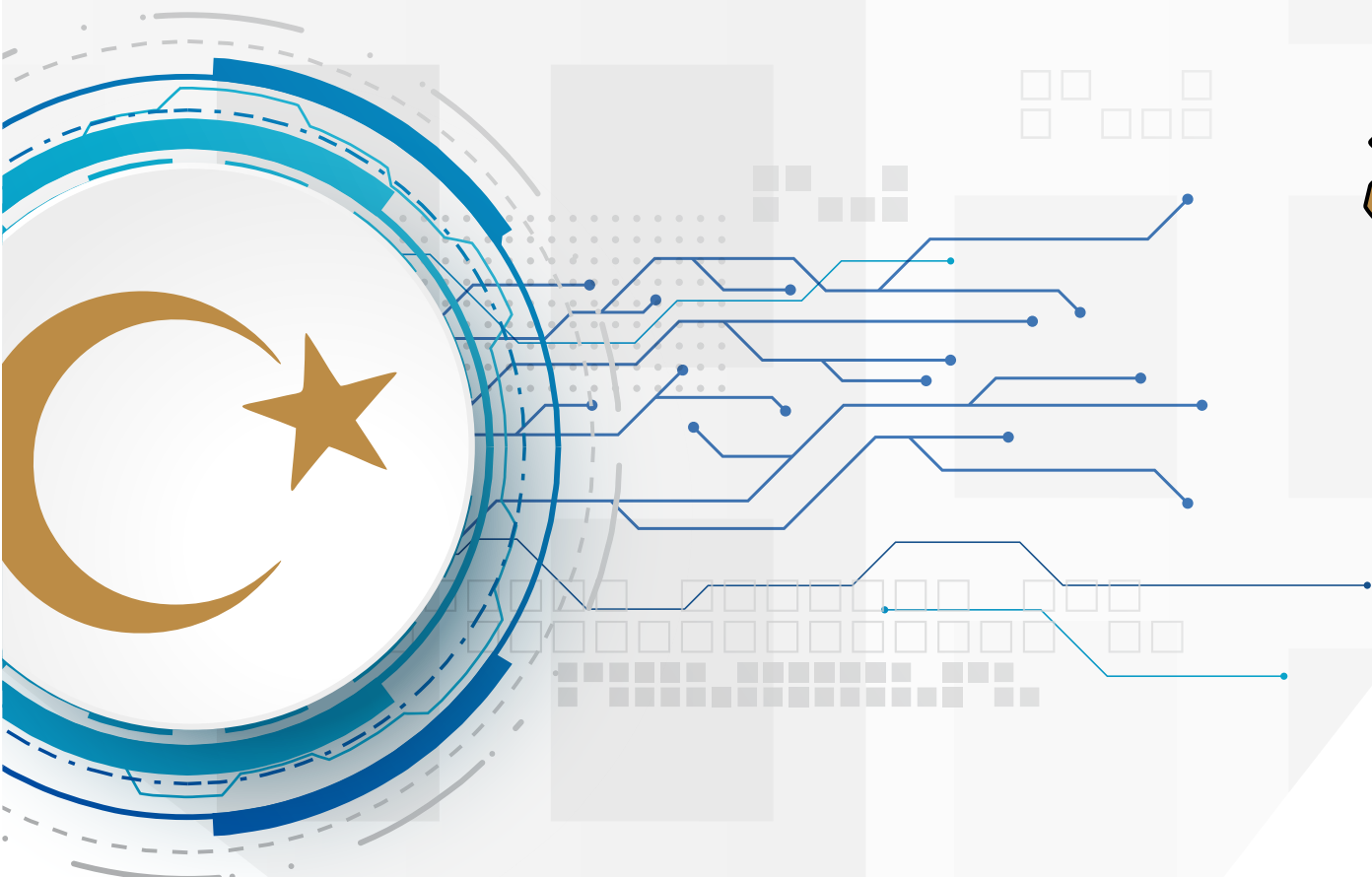




الهيئة الوطنية لأمن
وسلامة المعلومات



الاستراتيجية الوطنية للأمن السيبراني



لم يعد التحول الرقمي ترفاً تسعى لتحقيقه الدول ليسهل عليها أعمالها ومعاملاتها، بل أصبح أمراً محتوماً لا مفر منه تفرضه طبيعة الحياة العصرية واعتمادنا المتزايد بشكل متسارع على تقنيات الاتصالات والمعلوماتية. إذ لم يعد هناك قطاع أو صناعة يمكنها الاستغناء عما تُبَيِّره لها التقنية من إمكانيات والعمل في معزل عنها. ناهيك عما توفره التقنية من حلول للكثير من المشاكل التي تواجهه بلادنا كالمركزية والبيروقراطية وما يشكله اتساع الرقعة الجغرافية من تحديات.

إلا أن عملية التحول الرقمي، وبطبيعة الحال، تنطوي على عدد من التحديات والمخاطر التي يجب أن يُسعى لمعالجتها والاستعداد للتعامل مع تبعاتها والحد من آثارها السلبية. وهو الأمر الذي نسعى إلى تحقيقه عبر تَبَيُّ تقنيات وآليات الأمن السيبراني. كما أنه ومن خلال تنسيق وتوحيد جهود مؤسسات الدولة المختلفة في كل القطاعات عبر استراتيجية وطنية للأمن السيبراني يمكننا النجاح في تأمين وحماية هذا المجال الحيوي والحساس، وكذلك الحد من أي تهديدات أو مخاطر قد تُعرقل قدرتنا على تسخير التقنية لخدمة بلادنا.

1. توطئة

1.1.1. الأمن الوطني

كما هو متوقع، ومثله مثل كل تقنية جديدة يبتكرها الإنسان، يتم استغلال الفضاء السيبراني من قبل الحكومات المختلفة كسلاح ضد خصومها ومجال لفرض سيطرتها وتحقيق مصالحها. إذ أمسى الفضاء السيبراني ثغراً جديداً يحتاج من يربط عنده ويذود عنه. فهناك العديد من البنى الحيوية الحساسة التي تعتمد في عملها على تقنيات المعلوماتية والاتصالات مثل معامل ومركبات إنتاج النفط والغاز ومحطات الطاقة الكهربائية ومنظومات إمداد المياه. وكذلك ما تشكله شبكات الاتصالات الوطنية بمختلف أنواعها بحد ذاتها من بنية تحتية حيوية وحساسة لا غنى عنها للعديد من الأنشطة الاقتصادية للمجتمع مثل ربط المصارف وفروعها والمؤسسات الحكومية ومكاتبها في كل المدن. كما أن الكثير من الدول أحالت الفضاء السيبراني إلى مسرح جديد لبسط نفوذها بوسائل القوة الناعمة، وتستغل إمكانات وسائط التواصل الاجتماعي للتأثير في المجتمعات بما يخدم أهدافها.

1.1. التحديات

2.1.1. صعوبات التنظيم

تشكل طبيعة الفضاء السيبراني الخاصة تحدياً عند محاولة الاعتماد على التشريعات التقليدية في تنظيمه، فبالرغم من أن التعاملات في الفضاء السيبراني قد تشبه شكلياً مثيلاتها في الحياة الواقعية، إلا أنها تختلف اختلافاً جوهرياً في تفاصيلها من الناحية العملية. فمثلاً، وكما نعلم جميعاً، قد يتشارك البريد الإلكتروني ومثيله العادي في الاسم والغرض، المتمثل في تيسير التواصل بين أكثر من طرف، إلا أن هذا التشابه يقف عند هذا الحد ليس أكثر، فالبريد الإلكتروني يختلف اختلافاً تاماً عن نظيره العادي من كل النواحي الأخرى، مثل طريقة العمل والحفظ والنقل والتخزين. وبالتالي فإننا سنحتاج تنظيمياً وحوكمة مختلفة اختلافاً كلياً لكل منهما، والأمر سيان في كل ما يتعلق بتنظيم شؤون الفضاء السيبراني الأخرى. كما تضيف حقيقة تشارك دول العالم جميعاً لهذا الفضاء فيما بينها، ودون وجود حدود واضحة لمجال سلطة كل منها، المزيد من التعقيدات والعقبات لمساعي تنظيم وضبط الجرائم السيبرانية.

2.1.1. نقص القدرات

لا يمكن أن تلقى مسؤولية الأمن السيبراني، مثله مثل أي نوع آخر من الأمن، على عاتق طرف غريب أو أجنبي، إذ حتى المؤسسات لا يمكنها أن تثق ثقة تامة في أن يقوم طرف آخر غير موظفيها بالقيام بهذه المهمة. ومع حداثة العهد بهذا المجال، تعاني صناعة الأمن السيبراني من شح حاد في الكوادر المتخصصة والخبيرة، والأمر لا يقتصر على بلادنا فحسب، بل هو نقص تعاني منه كل دول العالم. كما أن تسارع وتيرة تطور وتعقيد التهديدات والمخاطر السيبرانية يجعل من الضروري تبني مقاربات مختلفة وجديدة كلياً لأساليب وإجراءات الحماية والتأمين للأصول والبنى التحتية.

2.1.1. موثوقية المعاملات

بسبب اختلاف المعاملات الإلكترونية عن مثيلاتها في الحياة الواقعية في طريقة عملها اختلافاً جوهرياً، فبالتالي ستشكل طرق التحقق من سلامة وأمان هذه المعاملات تحدياً في حد ذاتها، كما ستتغير طرق المصادقة على صحة المعاملات والتحقق من هوية أطرافها وامتلاكهم صلاحية إجراءها تغييراً كلياً، الأمر الذي يحتم ضرورة تغيير وتحديث التشريعات المنظمة لها.

2.1.1. ثقافة الأمن السيبراني

لا جرم أن سهولة التواصل وتلاشي الحدود بين الدول والمجتمعات له الكثير من المزايا والفوائد، إلا أنه وفي نفس الوقت سيُسَهِّل على من يريد أن يصل بضرره إلى أي طرف أو شريحة ما في المجتمع أن يفعل ذلك وببسر لم يكن وبالغ لولا هذا المجال المفتوح المتمثل في الفضاء السيبراني. وهو الأمر الذي لم يَخْفَى عن المجرمين والمخربين والمتطرفين، مما حدا بهم إلى نقل أنشطتهم إلى هذا الفضاء الرحب. ولم يقتصر الأمر على الأفراد بل أن كل الحكومات حول العالم تعمل على تطوير قدراتها السيبرانية في المجالات الدفاعية والأمنية والاستخباراتية، فيما يعرف بالحرب السيبرانية. كما اتجهت بعض الدول المتقدمة إلى تطوير أساليب وآليات تمكنها من استغلال وسائل التواصل الاجتماعي للتأثير والتغيير في المجتمعات بُغية تحقيق أهدافها وتلبية مصالحها على حساب الدول التي تكون ضحية مثل هذه الممارسات.

2. الرؤية


توفير بيئة آمنة للتحول الرقمي وبناء القدرات اللازمة لمواجهة المخاطر المصاحبة له، وتمكين الأفراد والمؤسسات من النجاح في الاستفادة من الفضاء السيبراني بأمان.



3. نطاق الاستراتيجية

تشمل هذه الإستراتيجية كل ما يتعلق بحماية وتأمين مصالح وحقوق الوطن والإنسان في الفضاء السيبراني.

4. أهداف الإستراتيجية

- 
- 1.4 تعزيز وتطوير الإطار القانوني والتشريعي وضمان ترسيخ الحوكمة الرشيدة للفضاء السيبراني.
 - 2.4 بناء ورفع القدرات البشرية والمادية الضرورية لحماية وتأمين الفضاء السيبراني والتحول الرقمي.
 - 3.4 تعزيز موثوقية وأمان واعتمادية المعاملات الإلكترونية.
 - 4.4 تشجيع التعاون مع الداخل والخارج، أفراداً ومؤسسات، سعياً لتوطين صناعة الأمن السيبراني.
 - 5.4 دعم التوجه نحو التحول الرقمي عبر نشر ثقافة الأمن السيبراني في المجتمع.

5. مجالات تنفيذ الإستراتيجية



1.5. برنامج لتهيئة الأطر العامة والبيئة القانونية والتشريعية للفضاء السيبراني.

يتم خلاله العمل على سد الفراغ التشريعي في كل ما يتعلق بتأمين الفضاء السيبراني ومكافحة الجرائم السيبرانية وحماية الخصوصية وتأمين الهوية الرقمية والمعاملات الإلكترونية وحقوق الإنسان. بحيث يتم التواصل بين كل المؤسسات الوطنية الحكومية والأهلية ذات العلاقة للتشاور والعمل على إصدار القوانين المنظمة لشؤون الفضاء السيبراني واللوائح التنفيذية الخاصة بها، وخاصة التشريعات المنظمة للمعاملات الإلكترونية والجرائم السيبرانية ومكافحة الإرهاب.

2.5. برنامج لإنشاء وتطوير آليات متكاملة لحماية أمن الفضاء السيبراني وتأمين البنى التحتية الحيوية للاتصالات وتقنية المعلومات.

يعمل من خلال هذا البرنامج على توجيه المؤسسات الوطنية لإنشاء أجسام تُعنى بمسائل الأمن السيبراني وبالأخص المؤسسات المسؤولة عن البنى الحيوية التي يجب أن تكون أيضاً فرقة خاصة للاستجابة لحوادث الأمن السيبراني (CSIRT)، وتكون مهمة الفريق الوطني (LibyaCERT) أن ينسق بين جهود كل هذه الفرق وأن يُشكّل نقطة التواصل الرئيسية بينها ومع مثيلاتها حول العالم. ونظراً لأنه لا يمكن حماية ما لا يمكن رؤيته، فإن هذا البرنامج يستهدف إقامة مراكز عمليات أمن سيبراني تُعنى بمراقبة الأنظمة والشبكات (cSOC) بشكل مستمر للكشف عن أي مخاطر قد تُهدد هذه البنى الحيوية وكذلك تبني كل الآليات الكفيلة بتوقع ومنع أي تهديدات مستقبلية محتملة الحدوث. ولتكوين صورة شاملة وموحدة لوضع الفضاء السيبراني، يتم العمل على إنشاء غرفة مركزية لعمليات الأمن السيبراني على مستوى الوطن ككل.

3.5. برنامج تجهيز البيئة الوطنية لتقنيات التشفير والتوقيع الرقمي والمصادقة على المعاملات الإلكترونية.

التحول الرقمي يعني أن تُصبح المعاملات كلها رقمية وهو الأمر الذي لن يتحقق دون أن تكون مُؤمنة عبر آلية تضمن سرية وسلامة هذه المعاملات وكذلك هوية من يقوم بها، ول يتم ذلك يجب العمل على إنشاء معمارية المفتاح العام والتي تُشكل حجر الأساس الذي لا غنى عنه لرقمنة المعاملات. كما يتم أيضاً العمل على ترسيخ مفهوم الهوية الرقمية التي من شأنها تيسير وتأمين المعاملات الإلكترونية.

4.5. برنامج بناء القدرات البشرية والخبرات الوطنية في مجال الأمن السيبراني بمختلف القطاعات.

إن مسؤولية أمن الوطن مهمة منوطة بأهله دون غيرهم، والأمن السيبراني ليس استثناءً. لذا يهدف هذا البرنامج إلى بناء كوادرات تقنية وطنية متخصصة بهذا النوع المهم من الأمن. وكذلك العمل على تطوير خبرات محلية متقدمة على كل الأصعدة العلمية والعملية وفي كل القطاعات يمكنها سد العجز الحالي والمستقبلي في كوادرات الأمن السيبراني. كما يجب العمل على توفير التدريب والتطوير المستمر لمواكبة الطبيعة المتغيرة والمتطورة بشكل سريع لتهديدات ومخاطر الفضاء السيبراني. وهو ما يوجب الاستفادة من خبرات من سبقنا في هذا المجال عبر التواصل والتعاون معهم والاستفادة من تجاربهم بالمشاركة في المناشط الدولية المختلفة ذات العلاقة.

5.5. برنامج لدعم البحث العلمي وتعزيز روح المبادرة والابتكار وتوطين صناعة الأمن السيبراني

التحديات والمخاطر السيبرانية دائمة التغير والتطور وبشكل متسارع، لذا يهدف هذا البرنامج إلى توفير الدعم والتشجيع لأنشطة البحث العلمي في المؤسسات الوطنية. كما يتم من خلاله العمل على تأطير المبادرات البحثية الفردية وتشجيعها وتقديم الدعم لها لما عرف عنها من قدرة متميزة غير تقليدية في كشف الكثير من التهديدات السيبرانية التي لم تتمكن المؤسسات البحثية الاعتيادية من اكتشافها. ويسعى البرنامج إلى دعم القطاع الخاص الوطني وتحفيزه لتطوير صناعة أمن سيبراني محلية تشكل رافداً وداعماً للقطاع الأهلي والحكومي.

6.5. البرنامج الوطني لتعزيز ثقافة الأمن السيبراني للمجتمع لتحقيق الاستفادة الأفضل من التقنية.

يتم عبر هذا البرنامج بذل كل الجهود الرامية لرفع مستوى وعي المجتمع بالمخاطر والتهديدات في الفضاء السيبراني وكيف يمكن للجميع أن يستفيد مما تقدمه التقنية من فوائد دون أن يتعرضوا لما ينطوي عليه ذلك من أخطار. كما يشمل هذا البرنامج إطلاق حملات تستهدف كل شرائح المجتمع وكل الفئات العمرية وخاصة الأطفال بشكل مباشر أو عبر توعية من يحيط بهم كأولياء الأمور والمعلمين. ويجب أن تنشر ثقافة الأمن السيبراني عبر كل وسائل إيصال المعرفة المختلفة كالمناهج الدراسية والدورات المتخصصة والتلفزيون والإذاعة ومواقع التواصل الاجتماعي والمطبوعات المختلفة على سبيل المثال لا الحصر. كما يجب العمل على حماية المجتمع من مخاطر استغلال الفضاء السيبراني في نشر التطرف والترويج للأنشطة الغير قانونية.

7.5. برنامج لتأهيل وضمان التزام المؤسسات الوطنية بمعايير وضوابط وسياسات الأمن السيبراني المحلية والدولية.

يستهدف هذا البرنامج أن تلتزم المؤسسات الوطنية منذ لحظة تأسيسها وأثناء عملها بأن تجعل متطلبات الأمن السيبراني أساساً لأي من أنشطتها الحالية والمستقبلية وجزءاً محورياً لمنظومة الحوكمة لديها. يتم بناء آليات تنظيمية واضحة تضمن قيام المؤسسات العاملة في البلاد بالالتزام بما يصدر عن الجهات المنظمة لقطاع الأمن السيبراني من ضوابط وسياسات. كما يتم دعم وتشجيع المؤسسات الوطنية للعمل نحو الالتزام بالمعايير الدولية ذات العلاقة.

8.5. برنامج لتعزيز الشراكات والتعاون الدولي والإقليمي والمحلي لتأمين الفضاء السيبراني.

تضطرنا حقيقة أن الفضاء السيبراني هو مجال تشترك فيه كل دول العالم وليس مقيداً بالحدود الجغرافية التقليدية، أن نولي أهمية كبرى للتعاون والتواصل مع محيطنا الإقليمي والعالمي لكي تتمكن من تأمين هذا المجال الحيوي بالشكل الصحيح. فعادة ما يكون مصدر العديد من التهديدات والمخاطر يقع في أماكن خارج نطاق سلطة الدولة المتأثرة بنتائج تلك التهديدات. كما يتوجب أن يتم تعزيز الشراكات بين المؤسسات الوطنية المختلفة وفي كل القطاعات لكي يمكنها تبادل المعلومات والخبرات، وتوضع آلية خاصة لتبادل المعلومات حول الحوادث السيبرانية تستهدف الحد من خطر انتشار الاختراقات التي تكون قد تعرضت له إحدى المؤسسات من أن يصل ضرره لمؤسسة أخرى.

9.5. برنامج رفع جاهزية البنى التحتية لتقنية المعلومات والاتصالات للمؤسسات الوطنية لمواجهة الطوارئ والتعافي منها وضمان استمرارية الأعمال.

من أهم مميزات التحول الرقمي هو ما يقدمه من تيسير وتسهيل لأعمال وإجراءات المؤسسات والأفراد، إلا أنه في حالة لم يتم تأهيل البنى التحتية الحيوية لتقنيات الاتصالات والمعلوماتية بحيث يكون لها القدرة على التعامل مع أي تغير في الأعباء التشغيلية وأن تكون لها المرونة الكافية للتعافي بسلاسة من أي طوارئ قد تواجهها، فقد يصبح التحول الرقمي عائقاً يعرقل عمل الدولة ونقمة بدل أن يكون نعمة تُيسر وتسهل على المواطنين إجراءاتهم ومعاملاتهم. عليه يتوجب إلزام المؤسسات الوطنية ضمن سعيها نحو التحول الرقمي بضرورة تلبية متطلبات رفع جاهزية بُناها التحتية لمواجهة الطوارئ والتعافي منها، وكذلك تزويدها بما تتطلبه معايير استمرارية الأعمال من موارد.

