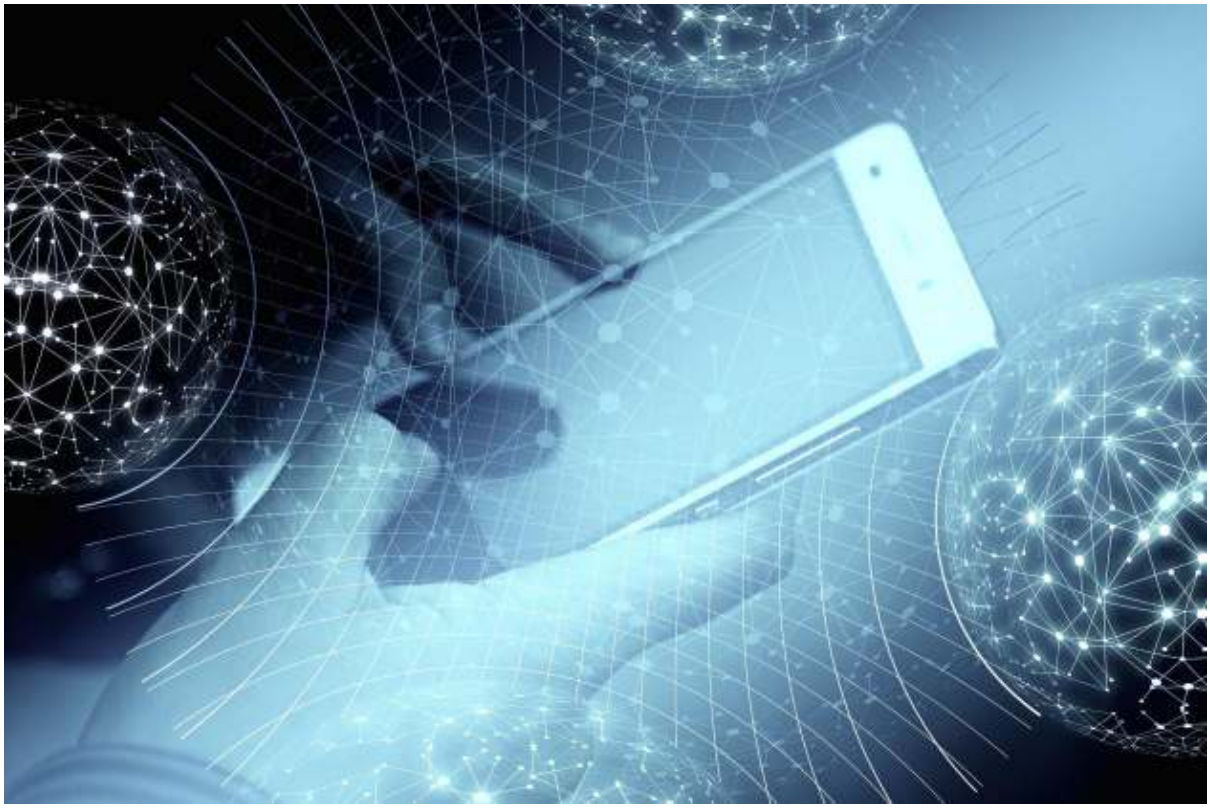

الإستراتيجية الوطنية اللبنانية للأمن السيبراني

نحو عام 2022

"يهدف لبنان لأن يكون لديه فضاء سيبراني أكثر امناً واستقراراً سواء في داخل الوطن أو في التبادلات الدولية"

الجمهورية اللبنانية
رئاسة مجلس الوزراء

2019

جدول المحتويات

تمهيد بقلم رئيس مجلس الوزراء

نحن اليوم، وفي خضم هذا العالم الذي يترابط مع بعضه البعض بشكل مضطرد، نشهد نمواً هائلاً في استخدام الأدوات الرقمية والتي بدورها باتت تولّد فرصًا لا تحصى ونمواً وازدهاراً في كافة المجالات، ولكنها بالمقابل، تختزن تهديداً محتملاً وداهماً لأمننا السيبراني. وفعلاً، تتزايد الهجمات االسيبرانية وتتطور كماً ونوعاً، مما يشكل تحدياً حقيقياً لبلدنا: اذ كيف بإمكاننا أن نكون مرنين بحيث نستطيع أن نواجه المخاطر المرتبطة بالفضاء السيبراني وفي نفس الوقت اتاحة حرية الاستخدام ضمن مساحة آمنة وجديرة بالثقة للمواطنين؟ والسؤال هنا تحديداً هو كيف نخلق لديهم هذه الثقة؟ الثقة التي تمكنهم من استخدام البيانات الشخصية والبيانات الحساسة بشكل خاص، أو الثقة في الأنظمة التي تنتجها أو تستضيفها أو توزعها. و في نهاية الأمر، كيف بإمكاننا أن نشجّع على الثقة بجميع الجهات الفاعلة والشركات والشركاء والموردين والخدمات العامة والدول التي يكون لوجودها الرقمي تأثير حقيقي على حياة مواطنينا.

نحن نعلم أنه لا يوجد تحويل رقمي بدون ثقة ولكن الأكيد أيضاً انه لا يمكن أن توجد ثقة بدون فضاء سيبراني آمن.

بناء على كل ذلك، يصبح أمر وضع استراتيجية وطنية للأمن السيبراني أولوية ملحة للبنان، خاصة وأننا من الدول الموقعة على "نداء باريس"[1] ومقتنعون تماماً بالحاجة إلى تأمين فضاءنا السيبراني في سياق التعاون الرقمي مع جميع شركائنا الدوليين.

لذلك، وفي سياق الإعداد لهذه الاستراتيجية، فقد ركزنا بشكل خاص على اعتماد منهج المشاركة المفتوحة بين مختلف الإدارات والمؤسسات والمعنيين من اجل إشراك جميع أصحاب المصلحة، ومن مختلف القطاعات العامة بما فيها مختلف الأجهزة الأمنية والسلطات القضائية. وهكذا، فقد صدر أولاً القرار رقم 172 الذي مكّن من تعيين منسق وطني للأمن السيبراني ثم تلاه القرار رقم 173 الذي تمّ على اساسه إنشاء لجنة وطنية مهمتها اعداد هذه الاستراتيجية، تحت إشراف الأمانة العامة للمجلس الأعلى للدفاع والتي هي بدورها تتبع لرئاسة الحكومة. ومباشرة بعد انشائها، عملت اللجنة بكل جهد ومثابرة لوضع هذه الاستراتيجية، حيث شاركت بنشاط وكثافة في ورش عمل ومؤتمرات كما وقامت بزيارات استكشافية نظمتها لها بعثة الاتحاد الأوروبي في لبنان، وشارك فيها عدد من الخبراء الأوروبيين الكبار المختصين بهذا المجال. وفي نفس الوقت كانت اللجنة تقيم ايضاً تعاونًا أكاديميًا مع كل من الجامعة اللبنانية وجامعة القديس يوسف وهذا ما يظهر الحرص على وجود اكبر عدد ممكن من اصحاب المصلحة ومن كافة الاطراف من اجل وضع تصور مشترك لهذه الاستراتيجية. وهنا أستغل الفرصة لأعرب عن امتناني لكل من ساهم في هذا العمل الذي اصفه بالإنجاز الوطني الكبير.

[1] في 12 نوفمبر 2018، وبمناسبة اجتماع منتدى إدارة الإنترنت (IGF) في اليونسكو، أطلق رئيس الجمهورية الفرنسي إيمانويل ماكرون نداء باريس للثقة والأمن في الفضاء السيبراني. هذا الإعلان الرفيع المستوى لتطوير مبادئ مشتركة لتأمين الفضاء السيبراني قد تم دعمه بالفعل من قبل 552 مؤيدًا، بما في ذلك 66 دولة و 347 كيان من القطاع الخاص و 139 منظمة دولية والمجتمع المدني.

ان هذه الجهود قد أوصلتنا الى نتيجة يقينية وأظهرت لنا الطريق الذي سنسلكه في اطار أمننا السيبراني: الا وهو ان العمل على إنشاء وتأسيس وكالة على مستوى الوطن، تحت سلطة رئاسة مجلس الوزراء بحيث تكون ملحقة بالمجلس الأعلى للدفاع، يبدو أمراً ملحاً لا غنى عنه. وهذه الوكالة ستكون هي السلطة المسؤولة عن أمن أنظمة المعلومات والمساعدة في مكافحة الجريمة السيبرانية. ان هذه الوكالة ستضمن امر حمايتنا من الهجمات السيبرانية من خلال تنفيذ استراتيجيتنا الوطنية هذه على كامل ارجاء الوطن، وبالتالي ستساهم في صون سيادتنا الرقمية والحفاظ عليها.

لكن يجب أن اشير هنا الى أن عمل هذه الوكالة سيكون عديم الجدوى إذا لم نبذل في نفس الوقت جهداً كبيراً لرفع مستوى الإدراك لدى مواطنينا وتوعيتهم على المخاطر اليومية لاستخدام الأدوات الرقمية وإذا لم نشجع على التدريب المهني لرفع مستوى كافة الجهات الأساسية التي ستكون مشاركة في مسؤولية حماية الوطن في الفضاء السيبراني.

ان مشروعي له طموح: ضمان الحد الادنى من الأمن لمواطنينا ولحسن سير عمل نظامنا الديموقراطي، وأن تكون هذه الاستراتيجية متبناة من جميع الأطراف المعنية في لبنان في اطار جهد جامع على المستويين المحلي والدولي.

وحيث انه من الضروري أيضاً في هذا المجال أن نعمل على تطوير اطار واسع للتعاون بين السلطات العامة، القطاع الخاص، والمجتمع المدني، فإنني أدعو جميع الأطراف المعنية في الوطن أن تشارك في هذا الجهد الجماعي لكي يكون تنفيذ هذه الاستراتيجية فعالاً ومفيداً لمصالح بلدنا.

سعد الحريري

رئيس الوزراء

مقدمة

منذ اللحظة الأولى لإنشائها، كانت شبكة الإنترنت تطمح الى وضع أداة جديدة في خدمة الإنسانية تعمل من خلال منصة عالمية يمكن الوصول إليها بحرية من اجل مشاركة المعلومات والمعرفة ضمن فضاء افتراضي جامع يتجاوز كل الحدود الجغرافية التقليدية. وإذ تم تحقيق هذا الهدف، فيجب الإدراك أن التطور المضطرد في التقنيات الرقمية قد زاد أيضًا من المخاطر المرتبطة بهذا الفضاء. وبالفعل فان الفضاء السيبراني هو في واقع الأمر فضاءٌ افتراضيٌّ يُستخدم للتعبير عن السلطة والقوة المتعلقة بالتوترات الثقافية والسياسية والعسكرية والاقتصادية. على هذا النحو، فإنه يتطور باستمرار في بناء العلاقات الدولية المعاصرة.

واليوم باتت حياتنا اليومية وتفاعلاتنا الاجتماعية واقتصاداتنا تعتمد على الموثوقية والشفافية والأمن في تكنولوجيا المعلومات والاتصالات. في هذا الاطار، من الواضح أن لبنان، مثله مثل جميع الدول الأخرى، يواجه العديد من التهديدات في فضائه السيبراني (الجريمة السيبرانية، التجسس، التخريب، الابتزاز، الاستخدام الاحتيالي أو المفرط للبيانات الشخصية وغيرها...)، مما يقوض درجة الثقة والأمن بفضائه السيبراني.

في هذا السياق، فإن المسؤولية الأساسية للدولة اللبنانية تكمن في توفير حلول الأمن السيبراني لكافة التحديات الحالية والمستقبلية، وفي اتاحة فضاء سيبراني مفتوح وحر، ضمن مبادئ احترام الديمقراطية وضمان حمايتها، وكل ذلك من اجل تحقيق درجة عالية من الأمن والثقة للقطاع العام والقطاع الخاص والمواطنين على حد سواء. من هنا، أتت ضرورة إنشاء لجنة وطنية في عام 2018، مهمتها وضع استراتيجية وطنية لبنانية للأمن السيبراني. وبالتالي فإن الإستراتيجية التي نقدمها هنا هي نتيجة لهذا العمل الجماعي المكثف الذي قامت به اللجنة، وهي تشكل حجر زاوية في عملية تأمين الأمن القومي لمجتمعنا الذي يتطور ليصبح حتماً، مجتمعاً رقمياً أكثر من أي وقت مضى، وبالتالي فان هذه الاستراتيجية تهدف لخدمة الصالح العام لجميع الأطراف الفاعلة في المجتمع اللبناني.

ان هذه الخطوة، ولا شك، تمثل نهجاً جريئاً وطموحاً قام لبنان بوضعه لنفسه من اجل تنظيم فضائه السيبراني. ان الأهداف المبتغاة من هذا النهج هي تنظيم فضاء لبنان السيبراني، وضع العنصر البشري في مركز مسؤولياته امام التحديات السيبرانية، بناء الوعي للجهد الجماعي الوطني على المستوى الداخلي، والوصول الى أسس لتعاون أقوى على المستوى الدولي.

الجزء الأول –
الاستراتيجية الوطنية اللبنانية للأمن السيبراني

الفصل الأول: السياق الإستراتيجي للبنان

يجد لبنان نفسه اليوم في خضم موجة التقدّم التكنولوجي الذي تكتسح العالم حاليًا. الا انه، ومن خلال اعتماده على خدمات رقمية متواضعة وبيئة سيبرانية غير آمنة، بات عرضة إلى مخاطر متعددة قد تستهدف أمنه وبناه التحتية فضلا عن سلامة وخصوصية مواطنيه.

أضف الى ذلك أن غياب استراتيجية وطنية واضحة وموحدة للأمن السيبراني عبر مختلف هيئات القطاع العام، ومعها مؤسسات القطاع الخاص، يجعل من عملية الدفاع ومنع هذه الهجمات عملية صعبة وشبه مستحيلة. **واذا ما نظرنا إلى نقاط الضعف، وخروقات البيانات، ومختلف انواع الهجمات التي عانت منها بعض الجهات اللبنانية، خصوصا خلال العام 2018، واذا ما أدركنا مدى السهولة التي تمكن بها المهاجمون من الوصول إلى شبكات جهات مختلفة في القطاعين العام والخاص**، تصبح الحاجة إلى الأمن السيبراني في لبنان ومكافحة السلوك السيبراني المؤذي والحفاظ على مستوى جيد من أمن البيانات وسلامة النظم المعلوماتية ضرورة ملحة وداهمة.

ويمكننا القول أنه، رغم بعض المحاولات المنفردة والخجولة التي تبذلها بعض المؤسسات والجهات في سبيل حماية بياناتها وأنظمتها، فان المبادرات والجهود التي نفذت وتنفذ على مستوى البلد ككل هي غير كافية إلى حد كبير في تحقيق الهدف المنشود. بناء على كل ذلك، باتت الحاجة ماسّة الى دمج كافة الجهود في اطار نهج تعاوني عبر اتباع إستراتيجية وطنية شاملة ومحددة الأطر بشكل جيّد في سبيل تأمين الدفاع الفعّال ضد الهجمات والجرائم السيبرانية. اذاً لم يعد هناك أدنى شك لدى أي كان من ان الجهود غير المنظّمة والمنسقة بين الجهات المعنيّة والتي بذلت في السابق وحتى يومنا هذا في مجال الأمن السيبراني في لبنان لا يمكن أن تحقق ابداً النتائج المرجوة. وفيما يلي نذكر بعض الأسباب التي توضح الوضع الحالي في هذا المجال:

- **غياب استراتيجية وطنية موحدة في مجال الأمن السيبراني**: ان كل مؤسسة من مؤسسات القطاعين العام والخاص لديها رؤيتها وكذلك الإجراءات الأمنية الخاصّة بها، والتي وان كانت فعّالة في السيّاق الخاصّ، الا أنه من الصعب دمجها في اطار تعاوني اشمل من دون وجود معايير واضحة المعالم، ومؤشرات أداء رئيسية واضحة. والأهم من ذلك كلّه عدم امكانية تبادل المعلومات والتعاون في أطر مشتركة مع الآخرين.

- **غياب القوانين والأنظمة التي تحكم الجرائم السيبرانية**: يفتقر لبنان إلى القوانين والتشريعات والأنظمة اللازمة لحماية الحقوق السيبرانية للمؤسسات الحكومية والشركات الخاصة والأفراد على حد سواء. كما يسجل غياب الجهود لوضع التعريفات الواضحة للأعمال الإجرامية السيبرانية وانواعها المختلفة كما وأن قانون العقوبات الحالي لا يلحظ هذا النوع من الجرائم. أضف إلى ذلك، أن العواقب والآثار التي تترتب على مثل هذه الأعمال الإجرامية ليست محددة بدورها بشكل واضح.

- **غياب الوكالة الوطنية للأمن السيبراني**: لا يوجد في لبنان حالياً أية جهة وطنية أو وكالة حكومية مختصة مهمتها: 1- حماية وحفظ الأمن السيبراني؛ 2- اقتراح ومتابعة تنفيذ وتطبيق القوانين المتعلقة بذلك؛ 3- التوظيف / الاستعانة بالأشخاص ذوي الخبرة اللازمة التي تحتاج اليها مختلف الجهات والمؤسسات في سبيل وضع أطرها الأمنية السيبرانية المناسبة؛ 4- تقديم عروض و ورش تدريبية

مختصّة؛ 5- دعم وتشجيع البحث العلمي والتطوير؛ 6- ضمان استمرارية وشمولية برامج التوعية بالأمن السيبراني على مستوى الوطن.

- **مكافحة الفساد في الاقتصاد الرقمي**: كما كانت الحال عليه في الاعوام السابقة، بقي تصنيف لبنان في العام 2018 ضمن فئة الدول التي سجّلت مستويات فساد عالية، وهذه حالة ثابتة تقريباً للبلد في هذا التصنيف منذ تسعينات القرن الماضي. ويمكن أن تُعزى هذه الحالة إلى عواقب الحرب الأهلية التي عصفت به آنذاك، حيث نشأ عنها جيل كامل من المواطنين الذين عاشوا في ظل مجتمع يفتقر إلى هيكل الدولة والنظام العام. وبدلاً من أن يستعيد هذا الجيل مفاهيم الثقافة اللبنانية التقليدية التي كانت سائدة قبل الحرب والمبنية على النزاهة والاحترام والكفاءة، اذ به يخرج من هذه الحرب ولا يرى سوى حاجته إلى إشباع رغباته بشتى الوسائل كتعويض عن سنوات الحرمان.

إن الفساد والاقتصاد الرقمي يتناقضان بشكل كامل، فالفساد هو من العوائق الرئيسية ضد تطبيق سياسات الأمن السيبراني في بلدان العالم، لأن اعتماد المكننة وتطوير الاقتصاد الرقمي يستطيع أن يحدّ، وفي أحسن الأحوال أن يلغي، الكثير من أنماط الفساد.

كما انه من المعروف أيضاً أن الجهات الفاسدة وفي كثير من الأحيان تتورط في هجمات إلكترونية نشطة أو ساكنة، مباشرة أو غير مباشرة، داخلية أو خارجية، بهدف تعطيل الخدمات التي توفرها البنية التحتية الرقمية للاقتصاد الرقمي الوطني، حيث يهدف هؤلاء الى اثبات ادعاءاتهم بعدم كفاءة الخدمات الرقمية من أجل اقناع اصحاب القرار بالعدول عن مشاريع المكننة والعودة الى العمليات اليدوية السابقة، حيث يصعب على الجهات المختصة ملاحظة أو تتبع مكامن الفساد.

- **السياق الاجتماعي والديموغرافي اللبناني المتعدد الأوجه**: يرتكز الدستور اللبناني على الأسس الديمقراطية التي تحافظ على المساواة في الحقوق بين المجتمعات الدينية المتعددة فيه. واذ تعدّ التعددية مكونًا فريدًا ومميّزًا وغنيً للأمة الا انها يُمكن اساءة استغلالها لزعزعة الاستقرار في كل مجال من مجالات الحياة العامة والمدنية في البلد، مما يتسبب في عرقلة كل مجالات التعاون والتبادل والاستخدام المناسب للمؤهلات، وخاصة عندما تصل الحال بالجهات والمؤسسات المتعددة التي تشكل المجتمع اللبناني الى الجنوح نحو الانعزالية والفردية مما يؤدي الى استنزاف الدولة من المهارات الضرورية والمطلوبة لحسن سير عمل مؤسساتها وقطاعاتها كما ويؤثر على المرونة الخدماتية الشاملة المبنية على التعاون بين مختلف الجهات والمؤسسات فيها.

إن انجع السبل لتفادي هذا الوضع هو في الاعتماد اولاً، وقبل كل شيء، على مبدأ الكفاءة، بحيث يجب أن يمتلك الأفراد المعيّنون في مختلف المناصب والمراتب، الخبرة اللازمة في مجالهم أو أن يطلب منهم مثلاً امتلاك شهادة تثبت تخصصهم في مجال وثيق الصلة بأعمالهم التي سيقومون بها. يعكس هذا التوجّه أيضاً المتطلبات الإلزامية للعمل في مجال الأمن السيبراني.

يمكن تشبيه الهجمات السيبرانية بالفيروس الذي يصيب أعضاءً في أي جسم حي. فان هي تُركت من دون علاج أو عولجت بشكل غير كافٍ، فستعرض كامل الجسم للخطر. وحتى أن هذا الخطر يمكن أن ينتشر إلى أفراد آخرين، مهدداً بتلويث المجتمع بأكمله وصولاً ربما الى هلاكه.

ولاستئصال أي امكانية لانتشار مثل هذا التهديد المحتمل على مستوى الوطن بأكمله، ينبغي أن يكون العمل منسقاً وشاملاً، بحيث يشارك فيه جميع أصحاب المصلحة المعنيين، وباستخدام مجموعة واسعة من أدوات التطبيق كما واعتماد الخبرات الموثوقة.

باختصار اذاً، يجب على الدولة التأكد من أن الأشخاص المعينين لتنفيذ الاستراتيجية الوطنية للأمن السيبراني هم اناس أكفاء، موثوقون، من ذوي الخبرة العالية، ويتحلون أيضاً بالمسؤولية في الحفاظ على المصلحة المشتركة وتعزيز الصالح العام، ويكون حافزهم للعمل هو الحسّ الوطني القوي.

- **النقص في التعاون بين مختلف الإدارات على المستوى الوطني**: ان كل مؤسسة تعمل حالياً على تأمين أمنها السيبراني بشكل منفصل، من دون وجود إطار واضح يسمح لها بالتعاون مع المؤسسات الأخرى. وهذا ما يفقد المؤسسات ميزة الاستفادة الاكيدة من مبدأ التنسيق وتقاسم وتبادل المعلومات والبيانات والخبرات. أضف إلى ذلك، أن النقص في التعاون قد يحصل حتى بين مختلف الإدارات ضمن المؤسسة الواحدة، وخاصة في المجال الأمني، بحيث يعمل كل قسم أو وحدة بشكل مستقل بدلا من التعاون معاً في سبيل تأمين امن الادارة / المؤسسة العامة.

- **عدم وجود مشاركة فعالة من جانب القطاع الخاص في سبيل النهوض بواقع القطاع العام**: يفتقر القطاع العام إلى وجود اطار تنظيمي والى غياب نظام توعوي لديه يسمح له بالاعتماد على القطاع الخاص عند الحاجة، من اجل التشارك معه في تغطية النقص الذي لديه في الخبرات وتنمية وتفعيل أقسام تكنولوجيا المعلومات الموجودة لديه والوظائف التابعة لها. وقد أدى ذلك إلى اعتماد القطاع العام، في كثير من الاحيان، اعتماداً كلياً على الشركات الخاصة من اجل تأمين وتوفير خدمات تكنولوجيا المعلومات والأمن السيبراني له. وان كان من المهم للقطاع العام أن يستعين بمصادر خارجية لمثل هذه الخدمات، الا ان النموذج المعتمد في هذا الاطار أضعف التعاون مع القطاع الخاص. وتؤكد السجلات إلى أن القطاع الخاص، وفي أغلب الأحيان، لم ينجح في تسليم مشاريع تكنولوجيا المعلومات المطلوبة إلى القطاع العام بشكل كامل أو حتى بشكل كاف، وأن القطاع العام لم يستفد كما كان ينبغي له أن يستفيد من تنفيذ هذه المشاريع. من هنا تنبغي معالجة هذه الثغرات في المستقبل عند أي شراكة تحصل مع القطاع الخاص و / أو عند قيام تعاون دولي من أجل ضمان نتائج بناءة في هذا المضمار.

- **عدم وجود مبادرة على أعلى المستويات في سبيل وضع نظام وطني للمعلومات واستراتيجية للتحول الرقمي**: على الرغم من كل الجهود التي بذلت بشكل مستقل أو من خلال مكتب وزير الدولة لشؤون التنمية الادارية ضمن مشاريع الحكومة الإلكترونية أو مشاريع الأتمتة التي حصلت منذ عام 1995 في مختلف الوزارات، يبقى لبنان يفتقر الى تطوير رؤية شاملة على مستوى الدولة تضمن نهج تعاوني مشترك بين كافة المؤسسات. وهناك خلل واضح وجدي بين المؤسسات في موضوع التنسيق في مجال تكنولوجيا المعلومات والاتصالات والذي لا يسنده أي اطار مؤسسي على مستوى عالي، مما يجعل من الصعب جداً اكتشاف وتحديد وإدارة الحوادث المتعلقة بالأمن السيبراني. في مثل هكذا بيئة، يصبح الاستخدام الفعال للأمن السيبراني والدفاع السيبراني لحماية المواطنين، والمؤسسات العامة أو الخاصة المستهدفين من قبل الهجمات السيبرانية مهدد جدياً بالخطر.

- **النقص في عدد خبراء الأمن السيبراني وصعوبة التكيف مع التغيرات السريعة**: ان الهيئات الإدارية والشركات والجامعات في لبنان هي في حاجة ماسة إلى تطوير الوعي حول قضايا الامن السيبراني وصولاً الى خلق جو من الأمن السيبراني جيد التنظيم ومتوازن وذلك من خلال تطوير البرامج التعليمية والتدريبية على جميع المستويات (المدارس والجامعات، الوظائف، المؤتمرات، إلخ...)، لتكون جميعها جاهزة للتعامل مع التطور السريع في طبيعة الجرائم السيبرانية والأساليب المستخدمة فيها. لكن لسوء الحظ، تقتصر تدريبات الامن السيبراني حالياً على بعض المنظمات التعليمية أو الجمعيات في بعض المناطق أو بعض الجامعات أو البرامج التعليمية الأخرى. ويميل الطلاب حالياً إلى الاعتماد على التعليم الذاتي في هذا المجال بدلاً من الحصول على برامج تعليمية وتدريبية رسمية توفر

لهم الأدوات اللازمة والموثوقة لتلبية حاجة السوق الى مثل هذه المواهب في القطاعات والصناعات المكشوفة للمخاطر في لبنان.

مما سبق، نستنتج ان لبنان ومؤسساته، كان ولا يزال، عرضة للتهديدات والجرائم السيبرانية مثله مثل أي بلد آخر في العالم. وأن أمر تنظيم الامن السيبراني في لبنان لم تتم حتى الآن مقاربته على المستوى الوطني بالشكل الصحيح، كما ويفتقر هذا الأمر إلى التعاون والتنسيق اللازمين بين كافة الجهات في القطاعين العام والخاص وعلى المستوى الدولي لضمان الاحتياجات الأساسية في مجال السلامة والخصوصية المعلوماتية لمواطنيه.

ان العديد من المؤسسات والشركات اللبنانية تقدم اليوم خدمات عبر الإنترنت للكثير من المواطنين والعملاء الذين أصبحوا اكثر واكثر ممن يعتمدون على الإنترنت في تأمين الحاجيات والخدمات. ولكن، ان استخدامهم الإنترنت غير الآمن سوف يجعلهم عرضة دائمة للهجمات السيبرانية. لكن، وبالرغم من أنه لا يمكن القضاء بصورة كاملة على هذا الخطر، من الممكن تقليله بشكل كبير وفعال عن طريق تقييد مساحات الهجوم وتخفيف انتشار الهجمات إلى مستوى يسمح للمجتمع بالاستمرار في الازدهار والاستفادة من الفرص الهائلة التي توفرها له التكنولوجيا الرقمية.

1.1 ما الذي تم انجازه

فيما يلي، نذكر باختصار أهم الجهود التي قامت بها جهات مختلفة في مجال الأمن السيبراني. نبدأ في العام 2006، حيث قامت الشرطة القضائية في قوى الأمن الداخلي بتأسيس مكتب مختص بمكافحة جرائم الملكية الفكرية وجرائم المعلوماتية، وتم تكليفه بالتحقيق في الشكاوى وخروقات الأمن السيبراني والجرائم المتعلقة بتكنولوجيا المعلومات تحت إشراف السلطات القضائية، كما وتم اعطاؤه دور في القيام بحملات توعية للمؤسسات العامة والمؤسسات التعليمية حول أحدث التهديدات والهجمات السيبرانية والجرائم عبر الإنترنت.

أيضاً، عملت الأجهزة الأمنية والاستخباراتية الأخرى، كل من جهتها وعلى أوسع نطاق ممكن، من اجل تعزيز قدراتها في التحري والتحقيق في مكافحة مختلف التهديدات التي يتعرض لها الأمن القومي، بما فيها الهجمات السيبرانية، التجسس والارهاب السيبراني.

أما في العام 2010، فقد قام رئيس الوزراء اللبناني بإنشاء لجنة وطنية، تضم ممثلين عن الجهات الحكومية الأساسية وعن الأجهزة الأمنية وحددت مهمتها الرئيسية في وضع تصور وطني حول الأمن السيبراني ومكافحة الجريمة السيبرانية. ولكن، وبعد مرور تسعة سنوات على هذا القرار، يتبيّن أن النمو السريع والتطوّر المستمر في صناعة التكنولوجيا ومنهجية وأفضل ممارسات الأمن السيبراني وكذلك تطور وانتشار تقنيات الهجوم والدفاع السيبراني جعلا سبل معالجة هذا الموضوع الخاص والفريد أمراً شديد الحساسية واكثر تعقيدا مما كان عليه الوضع في السابق.

لذا اصبح من الضروري التعاطي مع الاستراتيجية الوطنية للأمن السيبراني بمقاربة أكثر جدية وفعالية من السابق في سبيل التمكن من رسم وتحديد الإجراءات الفعالة التي يجب اتخاذها من قبل اللجنة الوطنية المكلفة هذا الموضوع.

اذاً، ومن الناحية العملية والتشغيلية، ومقارنةً بنهج 2010، نستطيع القول أن الاستراتيجية أصبحت تحتاج لأن تركّز على: 1- جعل الأمن السيبراني بحد ذاته هدفًا إلزاميًا، وملزمًا قانونًا وقابلاً للتنفيذ في كافة البنى التحتية لنظام المعلومات في لبنان بوجه عام؛ 2- تعزيز القدرات الوطنية في مجال الدفاع السيبراني وخاصة

ضد السلوكيات السيبرانية الخبيثة وفي مكافحة الجرائم والهجمات السيبرانية 3- تحديد هيكلية الجسم المركزي الذي يقع تحت سلطة رئاسة مجلس الوزراء ويكون مسؤولاً عن متابعة وتنفيذ مكونات هذه الاستراتيجية.

وصولاً الى العام 2018، حيث صادق مجلس النواب اللبناني على القانون رقم 81 والذي بات يعرف بـ "قانون المعاملات الإلكترونية"، والذي تضمن فصلًا عن كيفية التعاطي مع الأدلة الرقمية ووجوب المحافظة عليها.

من جهتها، قامت بعض الجامعات في لبنان بإعادة هيكلة مناهجها وفتحت برامج جديدة في درجة الماجستير حول الأمن السيبراني والعلوم الجنائية الرقمية.

والجدير بالذكر أيضاً أن لبنان يتعاون أيضا مع الدول المتقدمة في تكنولوجيا المعلومات والاتصالات والمنظمات الدولية في مجال الأمن السيبراني.

كما ويجري تطوير استراتيجية للتحول الرقمي على مستوى الدولة تحت إشراف مكتب وزير الدولة لشؤون التنمية الادارية.

في نفس الاطار، وبين عامي 2018 و2019، وفي إطار مشروع " CyberSouth " الذي ينظمه مجلس أوروبا، قامت وزارة العدل بتدريب حوالي 20 قاضيا على طرق مواجهة جرائم الإنترنت. وبالرغم من أن هذه خطوة كبيرة في الاتجاه الصحيح، الا أنها غير كافية و لا تزال وزارة العدل تحتاج إلى القيام باستكمال ومتابعة الجهود في هذا الموضوع وعلى أعلى المستويات.

من جهتها، تلعب وزارة الاتصالات دوراً رئيسياً في نشر بنية تحتية جيدة وبتعاون مكثف مع مشغلي قطاع الخلوي وهيئة أوجيرو. هذا وتتناول الوزارة بانتظام قضايا تتعلق بالأمن السيبراني للشبكات والبنى التحتية للاتصالات والمعلومات مع جميع أصحاب المصلحة الوطنيين المعنيين بالموضوع. وقد بذلت الوزارة أيضاً ولا تزال جهود تنسيقية مع الاتحاد الدولي للاتصالات لتحسين مؤشر الأمن السيبراني الخاص بلبنان.

أما مصرف لبنان، فقد طوّر ونفذّ من جانبه، وضمن نهج التحسين المستمر لديه، برنامجه الناضج والمتقدّم والمبتكر للأمن السيبراني والذي يعتمد على المعايير الدولية بما سمح للمصرف حتى اليوم من استباق واحباط الهجمات السيبرانية. يتكون هذا البرنامج من دعامتين أساسيتين، ويتطور باستمرار وذلك تماشياً مع أفضل الممارسات والمعايير المعتمدة في أمن تكنولوجيا المعلومات على المستوى العالمي:

- الجزء الخاص بالحوكمة والامتثال لتعليمات الأمن: يحتوي الركن الأول على تعريف وتحديث خارطة طريق وضعها مصرف لبنان حول أمن تكنولوجيا المعلومات، وإعداد ومتابعة سياسات أمن تكنولوجيا المعلومات، والتقييم والإدارة الاستباقية للمخاطر، وإطلاق وتقييم برنامج التوعية الأمنية.
- منهج الأمن المبني على الدفاع في العمق: أما الركن الثاني فيتكون من حلول أمنية متعددة الطبقات، متعددة التقنيات، تغطي البنية التحتية لأمن الشبكة والنقاط الانتهائية التابعة لها، ومباحث أمن التطبيقات، وعمليات أمن المعلومات المتقدمة والذكية.

أخيراً، ننوه الى أن العديد من المنظمات اللبنانية، في القطاعين العام والخاص، واجهت وما زالت تواجه وبمعدل متزايد بشكل ينذر بالخطر، الهجمات السيبرانية التي تستهدف بشكل رئيسي مواقعها على شبكة الإنترنت، مما يضعها خارج الخدمة. أما بعضها الآخر، فقد شهد هجمات من نوع آخر أدت إلى الكشف عن بعض السجلات الشخصية للمواطنين اللبنانيين ونشرها للعلن.

1.2 التهديدات

صممت الأنشطة الخبيثة التي تستهدف الفضاء السيبراني لتقويض السرية والسلامة وتوافر الخدمات في شبكات وأنظمة تكنولوجيا المعلومات العاملة في هذا الفضاء ولكي تستهدف ايضاً المعلومات التي تحويها.

ان هذه الأنشطة الخبيثة لديها بعض من الخصائص المشتركة: هي لا تعترف بالحدود بين الدول؛ هي من النوع التي لا يمكن أن ننسبها بسهولة الى جهة معينة؛ أنها لا تتطلب بالضرورة ميزانيات ضخمة و / أو مهارات تقنية عالية. علاوة على ذلك، من الممكن لجهات متعددة أن تساهم في هذه الأنشطة وأن تضع هذه التهديدات موضع التنفيذ، بمعرفة منها أو عن عدم معرفة، مما يوسع نطاق عملها ويجعل امكانية كشفها وتحديدها وادارة التعامل معها أمراً أكثر صعوبة وتعقيداً.

يمكن تصنيف أبرز التهديدات الرئيسية، استناداً الى مصدرها وطرق تنفيذها، على النحو التالي:

- **الجرائم المعتمدة على الوسائل السيبرانية**: في هذه الحالة، تكون أجهزة تكنولوجيا المعلومات والاتصالات هي الأداة الرئيسية لارتكاب الجريمة وايضاً الهدف الرئيسي للجريمة نفسها. نذكر بعض الأمثلة الأكثر صلة بها: كتطوير ونشر البرامج الخبيثة لتحقيق مكاسب مالية؛ القرصنة لسرقة البيانات الحساسة؛ هجمات حجب الخدمة، الفدية والابتزاز؛ وتغيير أو تدمير أو الاضرار بالبيانات. الحصول على الأموال يكون عادة هو الهدف الرئيسي لمثل هذه التهديدات.

- **الجرائم التي يتم تمكينها باستخدام الوسائل السيبرانية**: ويتم تصنيف هذا النوع حين تُستخدم أجهزة الحاسوب لارتكاب جرائم هي في العادة ذات طبيعة تقليدية. الأنشطة الرئيسية في هذا النوع من الجرائم تشمل الاحتيال عبر الإنترنت أو سرقة البيانات أو التجسس أو السرقة أو الابتزاز أو نشر الاشاعات أو التدمير. يمكن لهذه الجرائم أن يكون مصدرها بلدان ومناطق أخرى ولكن أيضًا قد تتم من داخل البلد نفسه حيث السعي عمومًا إلى الحصول على أموال أو بيانات لاستخدامها في أعمال ضارة أخرى.

- **التهديدات والهجمات التي تقوم بها أو ترعاها الدول**: وتحصل عندما تحاول الدول الأجنبية، أو جهات أو مؤسسات أو أطراف ترعاها دول أجنبية، اختراق الفضاء السيبراني لدول أخرى أو اختراق شبكاتها العامة أو الخاصة، أو الحصول على الملفات الحساسة الموجودة على الشبكات السحابية. وعادة ما يكون الغرض منها هو اما تحصيل مكاسب سياسية أو دبلوماسية أو عسكرية أو تكنولوجية أو تجارية أو مالية، واما اكتساب ميزة وتفوق استراتيجي. وعادة ما تستهدف هذه الأنشطة البنى التحتية الوطنية الهامة في بلد ما في المجالات التالية: الدفاع، المالية، الطاقة، الصحة، المرافق، والاتصالات.

وتشمل الأنشطة الرئيسية للدول في هذا المجال أيضاً عمليات تطوير قدرات خاصة للتجسس السيبراني وعمليات تدمير القدرات بدلا من استخدام التقنيات الجاهزة والمتداولة.

- **التهديدات الارهابية:** حيث تقوم المنظمات الارهابية باستخدام الانترنت من أجل القيام بـ :

  - الدعاية / الإعلان وبث الاشاعات؛
  - التجنيد والتعبئة؛
  - جمع التبرعات؛
  - الشبكات الآمنة؛ تبادل المعلومات المشفرة / المجهولة المصدر؛
  - التدريب عن بعد؛
  - التخطيط والتنسيق؛

- اعلان المسؤولية عن الهجمات، وبالتالي ابراز قدراتها كتقنية للترهيب؛
- استخدام الإنترنت مع تحسين مستمر للمهارات، من خلال عملية إغراق الأهداف.

هذا وتتطلع الجماعات الإرهابية بشكل متواصل إلى قيام بأنشطة سيبرانية مؤذية اتجاه لبنان.

- **تهديدات من قبل "النشطاء السيبرانيين"**: وتتم الأنشطة من هذا النوع، بصفة رئيسية، لأغراض تخريبية وإجرامية اتجاه الضحايا، حيث يستخدم ما يسمى "بالنشطاء" اساليب وادوات القرصنة الرقمية لنفس غايات المنظمات الإرهابية.

- **التهديدات الداخلية**: وهي تشكل خطرا مستمرا يقوم بها أفراد من الداخل، يكونون من العاملين "الموثوقين" ضمنياً في المؤسسة / الجهة التي تتعرض للهجوم، ويكون لديهم في العادة حق الوصول الى الأنظمة الحيوية والاطلاع على البيانات التي تحويها. ان هذه التهديدات تسبب أضرارا مالية لا يستهان بها كما وتهدد سمعة الشركة أو المؤسسة أو الجهة التي يعملون بها من خلال سرقة البيانات الحساسة وحقوق الملكية الفكرية فيها. كما ويمكنهم أن يشكلوا تهديدًا مدمرًا للمؤسسة في حال استخدموا المعرفة المميزة أو حق الوصول من اجل تسهيل أو شن هجوم يهدف الى تعطيل كامل للخدمات الحيوية على شبكة مؤسستهم أو لحذف البيانات من الشبكة.

أخيراً، نذكر أن البعض من الذين يتسببون بالأضرار من الداخل قد يكونون ضحية لحالات الهندسة الاجتماعية، وبالتالي يكون تسببهم للضرر غير مقصود لغرض أو هدف معين.

- **التهديدات من قبل المبتدئين في برامج القرصنة**: وذلك حين يقوم اشخاص ليست لديهم الخبرة باستخدام البرامج الخبيثة أو الأدوات التي تم تطويرها من قبل الآخرين – و / أو تنزيلها من الانترنت – لإجراء هجمات سيبرانية. هؤلاء تكون لديهم عمومًا إمكانية الوصول إلى أدوات القرصنة وشرح لاستعمالاتها والى الموارد والأدوات المتوفرة على الإنترنت والقابلة للتنزيل من مصادر عامة مفتوحة.

- **الهجمات على شبكات المعلوماتية**: حيث تقوم الجهات المهاجمة باستخدام البرمجيات الخبيثة بهدف تعطيل البنى التحتية السيبرانية واتلافها. يمكن أن يتراوح هذا التهديد من السيطرة والتحكم على المواقع الالكترونية والتلاعب بأنظمة القيادة والتحكم الخاصة بالعمليات الصناعية.

1.3 الاتجاهات التي تتبعها التهديدات السيبرانية

يؤثر كل من التطوّر المستمر والسريع في تكنولوجيا المعلومات والاتصالات وكذلك انتشار العولمة، والزيادة الهائلة في حجم البيانات، والعدد المتزايد من مختلف الأجهزة والمعدات المتصلة بشبكات البيانات، كل ذلك يؤثر تأثيراً كبيراً على الحياة اليومية، على الاقتصاد، وعلى سير العمل في الدولة ككل. إضافة إلى ذلك، فقد توسع انتشار الانترنت وتزايدت نسبة استخدامه بشكل غير مسبوق، بحيث نشهد نمواً كبيراً في عدد المستخدمين كما وانتشار خدمات وحلول تكنولوجية جديدة عبره، مثل انترنت الأشياء، وانترنت الأشياء الصناعية، والحوسبة السحابية، بشكل مضطرد. ان كل ما سبق ذكره يؤدي إلى توسع مشهد التهديدات السيبرانية والنمو في الهجمات التي تزداد كل يوم تعقيداً وشدة وتطوراً، مما يؤدي حتماً الى فداحة أكبر في الأضرار عند نجاح هذه الهجمات.

كما لا يجب إهمال موضوع تزايد عدد الجهات الحكومية المشاركة في أنشطة التجسس السيبراني والتي تستهدف أجهزة الحاسوب المتصلة بالإنترنت أو الشبكات المغلقة على حد سواء. ويعود ذلك إلى حقيقة أن عملية جمع المعلومات التي تقوم بها الدول والمتعلقة بالأمن القومي وبالأصول الاقتصادية لبلدان أخرى، تمثل موردا هاماً لهذه الدول في الساحتين الإقليمية والدولية. لهذا فان عدد الجهات والمؤسسات التي ترعاها الدول، والقادرة

على تنفيذ الهجمات السيبرانية، يزداد بشكل كبير كماً ونوعاً، مما يشكل مصدراً جديداً للتهديدات والمخاطر غير المعلومة ماهيتها ونتائجها على لبنان.

بالإضافة إلى نشاط الجهات الحكومية، بات الأفراد والجماعات الذين يملكون دوافع سياسية ولديهم موارد مالية محدودة يتمتعون بقدرة متزايدة على تنظيم وتنسيق أنشطتهم باستخدام الشبكات الاجتماعية بهدف القيام بهجمات حجب الخدمة وأنواع أخرى من النشاطات المؤذية.

علاوة على ذلك، فإن انتشار اعتماد وتطبيق معايير التشفير الحديثة والمتنامية بشكل سريع، من قبل المؤسسات الحكومية والشركات الخاصة - مثل SSL أو بروتوكولات SSH على سبيل المثال لا الحصر- قد كشف عن آثار جانبية غير متوقعة: اذ تسبب في جعل عمليات كشف الحدث الأمني السيبراني في وقته الحقيقي، والتحليل ما بعد الحدث، والدفاع، والتحقيق مسألة أكثر تعقيدًا. فقد أثبتت الوقائع أنه في ظل بعض الظروف المحددة وضمن بنى تحتية معلوماتية معينة، أصبح من شبه المستحيل على مؤسسات ضخمة مثل مراكز البيانات الكبيرة القيام باكتشاف الاختراق في الوقت الفعلي لحدوثه.

في الوقت الحاضر، باتت مثل هذه السيناريوهات تسمح لكثير من الاطراف بالتسلل وعلى نطاق واسع إلى المعلومات الحساسة والحيوية باستخدام نفس بروتوكولات التشفير التي يستخدمها عادةً الضحايا لتعزيز أمنهم السيبراني.

وهذا ما يؤدي في اغلب الأحيان إلى فشل الحلول التقليدية المستخدمة سابقاً مثل تقنية منع تسرب البيانات (DLP)، كما ويؤدي الى توسيع نطاق ما يسمى بـ "نافذة الهجوم" بشكل كبير وإلى مزيد من الخروقات الطويلة الأمد للبيانات عوضاً عن الخروقات القصيرة الأمد التي كانت تحصل في السابق التي لم يكن من الممكن كشفها ابداً. وأخيراً نذكر في هذا المجال، أن التطور السريع في قدرات المهاجمين وتطور مهاراتهم يجعل عملية تعقب ونسب الهجوم الى جهة معينة امراً أكثر تعقيدًا بشكل كبير.

1.4 التحديات

تنشأ مخاطر الأمن السيبراني الرئيسية من واقع اعتماد كافة قطاعات الدولة والاقتصاد والسكان المضطرد والمتزايد على البنى التحتية لتكنولوجيا المعلومات والاتصالات والخدمات الإلكترونية في نشاطهم اليومي.

لا شك في ان الجرائم السيبرانية تقوّض أسس عمل النظام الاقتصادي للدولة وتقلل من الثقة العامة في الخدمات الرقمية. لذلك، هناك حاجة ماسة إلى استخدام موظفين أكفاء واعتماد أدوات وتقنيات حديثة لضمان منع واكتشاف الجرائم السيبرانية وملاحقة مرتكبيها. وعلى الدول أن تعمل في هذا المضمار على تعزيز عملية تبادل المعلومات فيما بينها بهدف التمكن من مكافحة الجريمة السيبرانية.

ومن الضروري أيضاً من أجل منع وردع التهديدات الأمنية المستقبلية، الاستمرار في تطوير المعرفة المتعلقة بالأمن السيبراني والاستثمار في تطوير البنى التحتية والحلول التكنولوجية.

ان أحد التحديات الرئيسية **يتمثل في تطوير إطار قانوني عصري وفي تعزيز وسائل عمل أجهزة تطبيق القانون من جيش وقوى أمن داخلي وقوى أمن عام وأمن الدولة**، من أجل أن يتوفر لهم منهاج قانوني وتقني عصري ومتكامل بهدف إتاحة تحديد المسؤوليات الجنائية بشكل واضح فيما بينها في جميع مراحل سير التحقيق كما وخلال تنفيذ الإجراءات والتدابير اللازمة لمواجهة الجرائم السيبرانية بالكفاءة المطلوبة.

يجب أن يشمل الإطار القانوني الجديد أنواع العمليات المختلفة، سواء اكانت رفيعة أو منخفضة المستوى، لعل أهمها علم التحاليل الجنائية الرقمي وموضوع الامتثال الإلزامي لأفضل الممارسات المعتمدة في "سلسلة الحيازة" والتي تعتبر الخطوة الاساسية في التحقيقات الجنائية السيبرانية لضمان حسن طريقة حفظ المعلومات المتعلقة بالتحقيق واعتماد المفهوم المنطقي في كل الأدلة الرقمية المحتملة. بعد ذلك، يتم استخدام ما سبق في جميع مسارح الجريمة وسيناريوهاتها المحتملة، مثل استخدام التحاليل الجنائية الرقمية الخاصة بـ الخوادم المضيفة، الخوادم الكبيرة، الشبكات، نظام تحديد المواقع، انظمة السحب، الهاتف المحمول، الطائرات المسيرة، الأتمتة الصناعية، الصوت والفيديو، و انترنت الأشياء. إن الهدف العام للجوانب التقنية للإطار القانوني الجديد هو دائمًا الحفاظ على الأدلة الرقمية في مسارح الجريمة العادية والقائمة على تكنولوجيا المعلومات والاتصالات.

أما في المجال التقني وعلى المستوى الوطني، فيمكن الاستفادة من خبرات وقدرات ودراية القطاع المصرفي فيما يتعلق بتدابير الأمن والدفاع السيبراني. اما بما يتعلق بالأمور على المستوى الدولي، فانه من الضروري القيام بتعزيز علاقات لبنان مع الشركاء الدوليين الموثوق بهم وتطوير شبكات تعاون جديدة مع البلدان الأخرى من أجل تحسين الاقتصاد اللبناني وتبادل المصالح الأمنية. ونظرًا لأن التهديدات ذات طبيعة عالمية، فيجب أن يكون الدفاع عالميًا ايضاً، من خلال التعاون القوي مع الهيئات المهنية الدولية حيث لا توجد دولة قادرة بمفردها على التعامل مع التهديدات السيبرانية. إن التعاون الدولي إلزامي وفقًا للأحكام القانونية اللبنانية.

ينبغي أيضاً على الحكومة أن تكون قادرة على رفع معايير الأمن السيبراني في جميع أنحاء البلاد وعلى فرض تدابير أمان مناسبة لضمان أن يقوم الأفراد والمؤسسات والشركات بتكييف سلوكياتهم للتوافق مع أنماط الأمان المطلوبة من أجل العمل بأمان على شبكة الإنترنت.

ومن منظور تقني، لا شك ان الجرائم والهجمات السيبرانية تستغل تطور التكنولوجيا من جهة وعدم وجود استراتيجية مناسبة للأمن السيبراني أو عدم تنفيذها الفعلي، ان كانت موجودة، من جهة ثانية. بناء على كل ما سبق، بإمكاننا أن نحدد على وجه الخصوص خمسة تحديات رئيسية تمثل تهديدًا حقيقياً إذا لم تتم إدارتها بشكل صحيح:

- **توسع نطاق الأجهزة المستهدفة**: لقد باتت تكنولوجيا انترنت الاشياء وانترنت الاشياء الصناعية توفر لمن يرغب فرصًا جديدة للاستغلال وتزيد من التأثير المحتمل للهجمات السيبرانية، مما قد يتسبب بأضرار مادية بشبكات تكنولوجيا المعلومات والاتصالات كما وتشكل تهديدات جسدية للأفراد يمكن أن تصل في بعض الأحيان الى حالات التسبب بالوفاة. ان التطور السريع في عمليات الربط الشبكي في عمليات التحكم الصناعي في النظم الحيوية لمجموعة واسعة من الصناعات، مثل الطاقة، التعدين، الزراعة، والطيران قد خلق شبكة إنترنت الأشياء الصناعية. هذا قد يسمح بأن نصل الى وضع تصبح فيه هذه الأجهزة والعمليات الصناعية وغير الصناعية التي لم تكن في السابق عرضة للهجمات السيبرانية، لان تكون هدفاً للاختراق السيبراني وللعبث بقدراتها، مما يؤدي حتماً إلى عواقب كارثية عند حدوثه.
- **ضعف "النظافة السيبرانية" والامتثال**: يعتمد هذان العنصران عادة على الحلول التقنية المناسبة والتطبيقات كما ويمكن معالجتهما من خلالهما. الا ان امر معالجتهما بشكل صحيح يعتمد اعتمادا كبيرا على وجود الوعي الثقافي. في الواقع، فمن دون فهم صحيح لأهمية مفهوم "النظافة السيبرانية"، لن

تكون الحلول الدفاعية أو حتى الامتثال الكلي لمعايير الأمن السيبراني الحالية منها أو القادمة كافية للمعالجة المرغوبة على مستوى أمن الفضاء السيبراني.

وإذا لم يتم رفع مستوى الوعي الى المستوى الكافي وتمت المحافظة عليه وتغذيته على أوسع مستوى وطني ممكن، عبر مشاركة جميع المؤسسات العامة والخاصة في البلاد، والمواطنين والأفراد، فلن تكون البلاد وبنيتها التحتية آمنة من التهديدات السيبرانية. في هذا السياق، تقدم القائمة أدناه سرداً للوقائع والسيناريوهات الممكنة والمخاطر المحتملة وعواقبها في حال لم تدرك الحكومة بجميع مؤسساتها العامة والخاصة خطورة هذه التهديدات:

- 99٪ من الهجمات لا تزال غير معتمدة على نقاط الضعف المعروفة بـ "اليوم الصفر" -0 Day Vulnerabilities. وهذا يعني على سبيل المثال، إذا كان المواطنون لا يدركون أهمية الإجراءات الأمنية الأساسية البسيطة جدا، مثل اجراء "تحديث ويندوز"، ولا يعملون على تطبيقها بشكل صحيح ومنتظم، فان أجهزة الكمبيوتر الخاصة بهم ستكون عرضةً وبشكل دائم للهجمات الجماعية التي ستستغل نقاط الضعف المعروفة والمتعارف بها ؛
- ان المؤسسات التي تسمح للموظفين باستخدام اجهزتهم الالكترونية المنزلية للعمل من المنزل تعرضها إلى مخاطر أمنية شبيهة بمخاطر الـ "اجلب جهازك الخاص (BYOD)". من هنا يجب على الموظف الذي يعمل من المنزل أن يدرك أهمية الممارسات الوقائية البسيطة، مثل تغيير كلمة المرور الافتراضية على جهاز التوجيه (router) المنزلي، عوضاً عن استخدام الشبكات الافتراضية الخاصة دائمًا من أجل الاتصال عن بعد بمكتبه / مكتبها ؛
- حالات الابتزاز الجنسي والمالي سوف ترتفع بشكل كبير؛
- إن اتساع الفجوة في المهارات المطلوبة والعدد القليل من الخبراء المدربين المتاحين لملء الشواغر في حقلي الحماية والأمن السيبراني، سيؤدي إلى مستوى غير مناسب / ضعيف في عملية الاختبار والتدقيق والتصديق على الموائمة مع متطلبات ومعايير الأمن السيبراني في بيئات مختلفة ووفقا لسيناريوهات مختلفة.

- **التدريب والمهارات غير الكافية**: ان الفجوة في المهارات السيبرانية هي نقطة ضعف وطنية تحتاج إلى ايجاد حل لها. فهناك نقص في المجالات التالية:

- الخبرات والمعرفة الضرورية لتأمين الأمن السيبراني في كل من القطاعين العام والخاص.
- عملية بناء الوعي واقامة ورش التدريب في الأمن السيبراني لجميع موظفي القطاع العام الذين يتعاملون، بأي شكل من الأشكال، مع أنظمة تكنولوجيا المعلومات.
- التدريب العملي والمحاكاة على التنفيذ الفعلي لتدابير وتقنيات الدفاع عن الأمن السيبراني.

- **الأنظمة المعلوماتية القديمة والغير مرقعة**

- إن استخدام الأنظمة ذات الطراز القديم والتي لا تحتوي على إصدارات محدثة يعني حكماً وجود أنظمة غير مرقعة تجعل من الشبكة بأكملها عرضة للهجمات التي ستؤدي إلى خروقات هائلة للبيانات، مما يسمح للمهاجمين بسرقة الآلاف، إن لم يكن الملايين، من البيانات الشخصية والتجارية ؛
- يؤدي استخدام برامج من دون مساندة تقنية، حيث لم يعد البائع يصدر تحديثات وترقيعات لها، إلى زيادة مستوى الضعف الذي قد يستفيد منه المهاجمون للنجاح في عملياتهم الإجرامية.

- **توافر الموارد المستخدمة في القرصنة**

– ان توفر معلومات حول طرق وادوات القرصنة على نطاق واسع على الانترنت يزيد من الفرص لدى القراصنة من الوصول إلى المعرفة والخبرة اللازمة التي تمكنهم من استخدامها لأغراض إجرامية. هذا الأمر لا يمكن القضاء عليه، كون الانترنت نفسه مصمم بهدف تبادل المعلومات من أي نوع، سواء القانونية منها أو لا.
– ان توفر هذا النوع من المعلومات والموارد االمستخدمة للقرصنة لا يمكن اعتباره جريمة (وبالتالي عدم امكانية انشاء قائمة سوداء لمثل هذه البيانات)، لأن هذه المعرفة والأدوات وكتب الارشاد هي (أو تدعي أن تكون) في نفس الوقت للاستخدام في تعزيز المعرفة حول الأمن السيبراني واختبارات الأمن والامان، على الرغم من أنها في بعض الحالات يمكن استخدامها في تعليم القرصنة.

إن الحل الوحيد لمواجهة جميع التهديدات والهجمات السيبرانية المذكورة أعلاه هو بإنشاء نظام وطني على مستوى الدولة يمكنها من تنظيم استجابة منسقة، ضمن إطار قانوني وتقني موحد.

الفصل الثاني: الدولة هي المسؤولة عن الأمن السيبراني

يتطلب تأمين الفضاء السيبراني الوطني جهداً جماعياً متعدد الأبعاد (بشريًا وفنيًا)، مما يعني ضرورة مشاركة جميع الجهات الفاعلة في المجتمع اللبناني في هذا الجهد. فيما يخصّ الأمن السيبراني، يمكن تحديد أهم الجهات الفاعلة كالتالي:

- الحكومة؛
- الشركات والمؤسسات؛
- الأفراد كمواطنين، وموظفين، ومستهلكين.

لا شك اذاً انه يجب على لبنان، وفي ظل التطور التكنولوجي الرقمي السريع، أن يبذل كل جهوده في سبيل الوصول إلى موقع أفضل فيما يتعلق بأمن الفضاء السيبراني، لا بل يعد هذا شرطاً أساسياً من شروط حماية سيادتنا الرقمية وصونها. ان العالم الرقمي اليوم هو في حالة تغير مستمر وتحول ونمو وتطور دائم. لذلك من المهم أن يضع لبنان نفسه في أعلى المراتب في مجال تطبيق أفضل الممارسات المتبعة في الحماية السيبرانية. كما ويجب أن يكون لبنان مدركًا وجاهزًا ليبقى - ونأمل أن يكون ذلك ممكناً في المستقبل القريب - في صدارة التصدي للتهديدات السيبرانية السريعة التطور وحيث لا يمكن ترك لبنان عرضة للهجمات السيبرانية من دون ان يحرك أي ساكن. لا شك اذاً في ان الأمن السيبراني هو مفتاح رئيسي في عملية الحفاظ على السيادة الرقمية للبلاد.

2.1 دور الحكومة

يتمثل واجب الحكومة الرئيسي في الدفاع عن البلاد ضد الهجمات التي تشنها دول أخرى أو جهات فاعلة غير حكومية، وحماية المواطنين وصون الاقتصاد من الأذى، كما وتحديد الإطار الوطني والدولي الضروري لحماية المصالح الوطنية والحقوق الأساسية، ومكافحة الجريمة وسوق المجرمين وتقديمهم إلى المحاكمة.

ان الحكومة، وبصفتها مخزن مهم للبيانات ومزود للخدمات، يجب عليها أن تتخذ تدابير صارمة لحماية أصول المعلومات الخاصة بها. كما ويقع على عاتقها أيضًا مسؤولية أساسية تتمثل في تقديم المشورة للمواطنين والجمعيات والمؤسسات وإبلاغهم بما يتعين عليهم القيام به من اجل حماية أنفسهم في الفضاء السيبراني، كما وعليها أن تضع عند الاقتضاء، المعايير التي يجب على الشركات والمؤسسات الرئيسية الالتزام بها. في لبنان، هناك خاصيّة اضافية يجب اخذها بعين الاعتبار، اذ يعتبر القطاع الخاص من أهم القطاعات الرئيسية للاقتصاد اللبناني، وأهمها هو القطاع المصرفي. وحين يتعلق الأمر بالأمن السيبراني ومكافحة الجرائم السيبرانية، فإن المسؤولية النهائية عن ضمان المرونة والحفاظ على استمرارية الخدمات والوظائف الأساسية تقع على عاتق الحكومة، التي تقوم بتأمين ذلك عبر الادارة السليمة والتنسيق المدروس والتعاون مع كافة الأطراف كالأجهزة الأمنية من جيش وقوى امن، ووزارة الاتصالات، والهيئات المنظمة للقطاع المصرفي، وجميع المؤسسات الحكومية الأخرى، كل في نطاق اختصاصها، وكذلك مع كافة الشركاء الوطنيين والدوليين.

2.2 دور الشركات والمؤسسات

ان مؤسسات القطاعين العام والخاص تمتلك كماً كبيراً من البيانات الشخصية، وهي مسؤولة عن تقديم الخدمات، وهي تعمل ايضاً على تشغيل أنظمة مخصصة في المجال الرقمي. وفي ظل هذا التحول التكنولوجي وخاصة اذا ما نظرنا الى ما يحدثه الاتصال والتواصل بين أنظمة المعلومات التي تحتوي على البيانات وتلك التي تقدم الخدمات من ثورة في طبيعة عمل هذه الشركات، فإننا نجد أن احدى اهم المسؤوليات التي تقع على عاتق هذه الشركات تتمثل في ثلاثة أمور اساسية: حماية الأصول والبيانات الرقمية التي تحتفظ بها، الحفاظ على الخدمات التي تقوم بتقديمها، وإدماج المستوى المناسب من الأمان في المنتجات التي تقوم ببيعها الى المستهلكين.

واذا كان من الطبيعي أن يعتمد المواطنون والمستهلكون والمجتمع بشكل كبير على الشركات والمؤسسات التي تقدم لهم الخدمات في اتخاذ جميع التدابير المعقولة لحماية بياناتهم الشخصية وتعزيز مرونة أنظمتهم وخدماتهم، فان على هذه الشركات والمؤسسات أن تدرك أنها تعمل في بيئة تجعلها مسؤولة عن العواقب والآثار غير المباشرة للهجمات السيبرانية التي قد يقع كل اولئك ضحية لها.

2.3 دور الأفراد: المواطنين والموظفين والمستهلكين

ان السياق الطبيعي للأمور في الممارسات الوطنية والدولية المتبعة في هذه الايام، يتطلب أن تكون جميع الأصول الثمينة للدولة آمنة، ليس فقط في العالم المادي ولكن أيضًا في العالم الرقمي والافتراضي. ونظرًا لكون كل شيء في العالم الافتراضي متصل ومترابط، فمن الضروري أن يتحمل الجميع مسؤولياته في اتخاذ جميع الخطوات الممكنة لحماية الأجهزة - الهواتف الذكية والأجهزة اللوحية وأجهزة الكمبيوتر المحمولة - والبيانات والبرامج وكذلك الأنظمة وبما يضمن توفر الحرية والمرونة والراحة التي يجب أن يتمتع بها الجميع في حياتهم الخاصة والتجارية.

الفصل الثالث: أركان الاستراتيجية الوطنية للأمن السيبراني

اذا ما نظرنا إلى كافة الوقائع التي أثيرت أعلاه، والى وضع لبنان الحالي، واذا ما استندنا كذلك الى حجم التحديات القادمة، فان الجميع يدرك انه ينبغي على الحكومة إشراك جميع مؤسساتها في تنفيذ استراتيجية شاملة تكون قادرة على تحقيق المهمة الكبرى الا وهي توفير فضاء سيبراني أكثر أمنا وخلق مستوى متزايد من الوعي بين الجهات الفاعلة الرئيسية في المجتمع اللبناني حول هذا الموضوع.

لا شك ان الحكومة اللبنانية تدرك ان الاقتصاد الجديد اصبح شديد الاعتماد على الإنترنت، سواء من المنظور العام أو الخاص. في هذا الاطار، يخلق الانكشاف الأمني المعلوماتي مستويات ثابتة من المخاطر مما سيحفز ويثير محاولات الهجوم السيبراني بشكل دائم.

إن الطريق الواجب على لبنان اتباعه لإنجاز كل خطوة من الخطوات المحددة في هذه الوثيقة والتي تم تحليلها أعلاه، هو بحد ذاته تحد كبير. ولسوف يتطلب الأمر الكثير من الجهد الذي يبدأ قبل كل شيء بعملية حشد الإرادة السياسية الكافية التي تتيح له وضع الأسس والأصول التشريعية والتكنولوجية وركائز الأمن السيبراني، وتنفيذ ذلك بالاعتماد على الموارد البشرية المتخصصة والمكرسة لهذه الغاية.

وبمجرد ان نتمكن من وضع امر التحول إلى هذا النهج الجديد موضع العمل، فان تنفيذ هذه الاستراتيجية سيتطلب فترة قد تصل من سنتين إلى أربع سنوات. **وفي حين انه لا يمكن لاحد الزعم بانه يملك القدرة على القضاء تمامًا على التهديدات التي تهدف الاستراتيجية الوطنية للأمن السيبراني إلى مواجهتها، الا أن المسارعة الى اتخاذ جميع التدابير الممكنة للحد من المخاطر والوصول إلى مستوى مقبول من الأمن يبقى من اولى الأولويات**. يجب أن يوفر لبنان لشركاته ومواطنيه البيئة التي تسمح لهم بالازدهار المستمر والاستفادة من الفرص الهائلة التي توفرها التكنولوجيا الرقمية.

من هنا، يجب على استراتيجية الأمن السيبراني التي تضعها أي حكومة، وهي بالتالي تمثل دولة بأكملها، أن تصوغ أهدافًا واضحة لاستشراف المستقبل وان تتضمن إجراءات مستمرة وطويلة الأجل.

في الوقت الذي يستعد فيه لبنان لإنشاء وإطلاق "الاستراتيجية الوطنية للأمن السيبراني" فان من الأهمية بمكان تحديد وتبويب الركائز الأساسية التي يجب أن تستند إليها الاستراتيجية المرتقبة. ومن خلال تحديد هذه الأعمدة التأسيسية وتحديد أولوياتها بشكل واضح، يمكن لنا بالتالي بلورة الاستراتيجية وتأمين تنفيذها وتشغيلها.

بناءً على ما تقدم، يجب أن تستند الإستراتيجية الوطنية للأمن السيبراني إلى المحاور التأسيسية الإستراتيجية والمفصلة التالية، والتي يشار اليها "بأعمدة الاستراتيجية الوطنية":

1. **اتخاذ اجراءات الدفاع، والردع، وتعزيز الجهود لمكافحة التهديدات السيبرانية من الداخل والخارج ؛**
2. **تطوير التعاون الدولي في مجال الأمن السيبراني ؛**
3. **تنمية قدرات الدولة باستمرار لدعم تطوير تكنولوجيات المعلومات والاتصالات ؛**
4. **تعزيز القدرة التعليمية على الأراضي اللبنانية ؛**

5. **تعزيز القدرات الصناعية والتقنية ؛**
6. **دعم تصدير وتدويل شركات وصناعات الأمن السيبراني المحلية ؛**
7. **تعزيز التعاون بين القطاعين العام والخاص ؛**
8. **تعزيز دور أجهزة الأمن والمخابرات وتعزيز التعاون والتنسيق المتبادلين بدعم وإشراف الجهات العليا.**

اننا، وفقط عن طريق التعرف على الركائز المذكورة أعلاه والعمل وفق اسسها، نستطيع البدء في تطوير استراتيجية وطنية للأمن السيبراني مع تحديد أهداف واضحة لها.

3.1 اتخاذ اجراءات الدفاع والردع وتعزيز الجهود لمكافحة التهديدات السيبرانية من الداخل والخارج

يجب على الدولة اللبنانية أن تضع استراتيجية للردع من أجل تقليل عدد الجرائم السيبرانية بشكل جذري. ويجب ان تتضمن استراتيجية الردع في الفضاء السيبراني مجموعة من الإجراءات التي تكون مصممة لوقف الهجوم والتعرف على المهاجمين فور مباشرتهم محاولاتهم الخبيثة الأولى على الشبكة، مع الأخذ في الاعتبار الواقع الذي يقول أن المهاجمين بعد ولوجهم إلى الشبكة، يتبعون دائمًا "سلسلة قتل سيبرانية" يمكن التنبؤ بها.

تمر "سلسلة القتل السيبرانية" هذه عبر ثماني مراحل: الاستطلاع، التسلل، الاستغلال، تصعيد الصلاحيات، الحركة الجانبية، التعتيم، رفض الخدمة، والانسحاب.

خلال مرحلة الاستطلاع، يقوم المتسلل بعملية استكشاف ساكنة للشبكة بشكل خفي تهدف الى جمع كل المعلومات اللازمة له للقيام بعمليته. في هذه الحالة من الضروري للغاية القيام بتطبيق تقنيات وأدوات الردع المناسبة التي تسمح بإعادة توجيه نشاط المهاجمين في مسار خاضع للسيطرة، بحيث يتولى المدافعون معالجته بسهولة.

بعدها، يقوم المخترق بالبدء بمرحلة التسلل مستندًا إلى المعلومات المكتسبة من مرحلة الاستطلاع السابقة. الهدف في هذه المرحلة هو الدخول الى النظام المعلوماتي والوصول إلى البيانات التي يحتويها.

أما في مرحلة الاستغلال التي تلي نجاح مرحلة التسلل، فيقوم المهاجم بشن هجوم نشط، حيث يستخدم المتسلل أنواعًا مختلفة من الثغرات الأمنية التي سبق له ان قام بتحديدها وذلك من أجل استغلال موارد المستهدفين الرقمية بسرعة، والحصول على حق استخدام الانظمة عن بعد أو محليا – ليصبح كانه مستخدم عادي أو حتى كمسؤول عن النظام المعلوماتي.

بعد ذلك يستخدم المهاجمون تقنية تصعيد الصلاحيات للحصول على وصول أكبر إلى الموارد.

اما مرحلة الحركة الجانبية فتهدف إلى السماح بالوصول غير المصرح به إلى الخوادم الداخلية في الشبكة المستهدفة والبيانات التي تختزنها أو تديرها. في بعض الأحيان، يمكن لهذا الوصول أيضًا من تمكين المهاجمين من توسيع نطاق الأعمال الهجومية نحو أطراف ثالثة خارجية، أي نحو الأصول الرقمية الموجودة فعليًا أو منطقيًا خارج محيط شبكة الضحية.

بعد هذه المرحلة، يتم استخدام التعمية والتمويه لإخفاء النشاط والتهرب من أي تحليل جنائي.

اما مرحلة رفض الخدمة فستمنع الجهات المسؤولة من تتبع الهجوم أو حظره وذلك عن طريق تعطيل النشاط العادي للمستخدمين والخوادم في الشبكة المستهدفة.

وتمثل المرحلة الأخيرة، مرحلة الانسحاب، التحدي الحقيقي والأكثر أهمية للمهاجمين، خاصة عند التعامل مع أكثرهم خبرة ومهارة. حيث يتفننون في نقل المعلومات والبيانات المختلفة عن بُعد من خلال تقنيات مختلفة يختارونها، والتي يمكن أن تتراوح من البسيط إلى المعقد للغاية، وغالبًا ما تستخدم بنى تحتية وشبكات مخصصة لذلك.

بعد ان يكون لبنان قد امتثل للمعايير الأساسية للأمن السيبراني وبدأ بتطبيق هذه الاستراتيجية، فان الحكومة والوكالة الوطنية للأمن السيبراني ونظم المعلومات – (NCISA) ستكونان قادرتين على: تقييم مواطن الضعف؛ التنبيه من المخاطر مع تقديم توصيات واضحة بشأن التدابير الوقائية المطلوبة لمواجهة العواقب الرئيسية للهجمات؛ تحديد التهديدات بكافة انواعها؛ الرد السريع والفعال على هذه الهجمات؛ والحفاظ على بيئة سيبرانية لبنانية آمنة. يجدر بنا الذكر هنا الى انه يمكن استخدام العديد من الأدوات والتقنيات لإنشاء إطار وظيفي للردع السيبراني. على كل، وقبل البدء بتطبيق هذه التدابير، من الضروري تطوير القدرات التقنية والقضائية الخاصة بالدفاع السيبراني.

بشكل عام، يتضمن التعريف الشائع والمتفق عليه لمفهوم الردع في الفضاء السيبراني على عنصرين: القدرات الدفاعية (الردع عن طريق المنع) والقدرات الهجومية (الردع بالعقاب). نشير هنا الى أن القدرات الدفاعية تعني هنا الدفاع السيبراني، أي حماية أنظمة المعلومات الأساسية للدولة وتقوية قدراتها على مقاومة الهجمات المستمرة والمتنوعة. من ناحية أخرى، وفي ظل هجوم قائم، تتحقق عملية الردع عبر اتخاذ الإجراءات المناسبة التي تؤدي إلى وقف الهجوم وملاحقة الجناة.

أما العنصر الآخر من عناصر الردع فهي الاستجابة الهجومية، التي تمثل فعلياً ما يعرف بالردع السيبراني. يستند عنصر الردع هذا على التهديد بالانتقام بعواقب لا تطاق، وهي مصممة بهدف إقناع الخصم بعدم القيام بالهجوم في المقام الأول. يتعلق الأمر بعرض قوة يكون كافياً للتخلص من التهديد من دون الحاجة إلى استخدامها فعلياً.

أما تطوير القدرات الدفاعية فيجب أن يتبع مسار العمل التالي:

- إنشاء "نموذج دفاع سيبراني لبناني" نشط، بحيث يستند الى أفضل الممارسات العالمية ويتضمن إجراءات فنية من نوعين، منخفضة المستوى وعالية المستوى مثل الحجب والفلترة والقوائم البيضاء والسوداء وما إلى ذلك، ضد هجمات التصيّد الاحتيالي واغلاق أسماء النطاقات الخبيثة وما يتصل بها من مراكز ادارة وتحكم، وضد الهجمات التي تستند إلى البرمجيات الخبيثة، وضد الهجمات التي تعمل على أساس "اليوم الصفر" وضد أطر الاستغلال، والخداع عبر البريد الإلكتروني، ولحجب عناوين بروتوكول الإنترنت الغير مرغوبة، إلخ.
- استخدام المعلومات المتوفرة المجربة والمعروفة حول الأمن السيبراني لإنشاء قاعدة بيانات تحتوي على تقييم لموثوقية المصادر الموجودة في الفضاء السيبراني، وبما يسمح بالتحكم وبتصفية أفضل للمحتوى الضار والتهديدات الخطيرة. ان الاعتماد على معايير الأمن السيبراني الدولي واتباع أفضل الممارسات في هذا المجال سيسمح لنموذج الدفاع السيبراني اللبناني ليس فقط أن يكون شاملاً ولكن أيضًا بالاستفادة القصوى من الخبرة الواسعة الموجودة التي تمتلكها هيئات وضع المعايير الدولية في مجال الامن السيبراني.

- تصنيف البيانات وتحديد البنى التحتية الحيوية، وبالتالي وضع الأسس لبناء بيئة سيبرانية وطنية أكثر أمنا، من منظور استخدام الدفاع الاستباقي. ينبغي أن يتماشى ذلك مع حماية المؤسسات الحكومية والقطاعات الأخرى ذات الأولوية، ومع مراعاة أحدث معايير الأمن السيبراني وأفضل الممارسات المعتمدة فيه، مثل على سبيل المثال لا الحصر: الترقية إلى أحدث إصدارات البرامج ؛ تطبيق الترقيع للعملاء؛ والمسح بحثًا عن نقاط الضعف المعروفة الخ...

- تغيير السلوك المتبع في القطاع العام وفي قطاع الأعمال، مع التأكد من أن كل مؤسسة، بغض النظر عن حجمها، اصبحت تتخذ كافة الخطوات المناسبة لحماية نفسها في الفضاء السيبراني.

- إدارة الحوادث وفهم التهديدات من وجهات النظر المختلفة: العملانية، الأمن القومي، الجغرافيا السياسية، المنظور التقني، بما يسمح بتحكم أفضل في مخاطر الأمن عبر الجمع بين رد الفعل واستباق الفعل، وكل ذلك من أجل الحد من فرص التعرض للمخاطر السيبرانية. في موازاة ذلك، فان تصميم وبناء وتشغيل حلول أمنية مبتكرة متعددة الطبقات، سوف تسمح بتوقع ومنع الهجمات المتقدمة.

- جعل أنظمة الحاسوب اللبنانية هدفًا أكثر صعوبة للمجرمين السيبرانيين، مما يقلل من الفوائد التي يطمح اليها المتسللون (أو ما يعرف بالردع عن طريق الحظر) وزيادة الأكلاف عليهم (الردع بالانتقام). لذلك من الضروري أن تتوفر القدرة على تحديد مصالح وأهداف المعتدي المحتمل وأن تتوفر قدرات ردع موثوقة ومقنعة بما فيه الكفاية.

- التأكد من أن القدرات الوطنية للدولة ونية الردّ لديها مفهومة بوضوح من أجل التأثير على (تثبيط) اتخاذ القرارات لدى المهاجمين المحتملين.

- القضاء على الفرص التي هي سهلة الاستغلال من قبل الذين يرغبون في اختراق الشبكات اللبنانية وأنظمة تكنولوجيا المعلومات فيها. يجب أن تكون لدى الحكومة الأدوات والقدرات اللازمة لتنفيذ ما يلي: حرمان المهاجمين من الفرص السهلة لتهديد الشبكات والأنظمة اللبنانية ؛ فهم نوايا وقدرات المهاجمين؛ التغلب على تهديدات البرامج الخبيثة الأساسية على نطاق واسع ؛ والرد وحماية الأمة في الفضاء السيبراني.

- منع الناس من الانجذاب إلى عالم الجريمة السيبرانية أو الانخراط فيها من خلال تعزيز تدابير التدخل المبكر.

- وضع خطة عمل منهجية وملقنة يمكنها تأمين خيارات متقدمة للرد على الهجمات السيبرانية، حتى تتمكن السلطات من الاستجابة للأزمة أثناء حدوثها . يجب أن يصبح أمر الاستجابة للتهديدات السيبرانية والهجمات الإلكترونية عقيدة تلقائية. وستكون هذه العقيدة مبنية على فهم لبنان لتطبيق القانون الدولي الحالي في الفضاء السيبراني. في الواقع، لا يمكن للبنان أن يقرر التصرف تلقائياً للرد على الهجوم السيبراني، دون النظر إلى القوانين والأنظمة الدولية القائمة في هذا المجال واحترامها.

- دمج المعايير القانونية الدولية في نظام التصنيف الوطني للهجمات السيبرانية. يُعدّ دمج المبادئ الوطنية والدولية المتعلقة بالأمن السيبراني معاً عنصرا أساسيا في مبدأ العمل الناجح، والذي يؤمن بدوره أداة دعم مهمة للسلطات من أجل اتخاذ قرارات أكثر فعالية واعتبارها كوسيلة مهمة في دعم التعاون الدولي.

- تعزيز القدرات العاملة في مجال تطبيق القانون ودعم كافة الخبرات على المستويات الوطنية والإقليمية والمحلية من اجل تحديد وردع مجرمي الفضاء السيبراني في لبنان والخارج.

- تحسين قدرات السيادة الرقمية، عبر استخدام مراكز البيانات التي هي موجودة فعليًا على الأراضي اللبنانية. ان آفاق نجاح ممارسة السيادة الرقمية على البيانات يجب أن يؤدي إلى إنشاء الحلول القانونية والتقنية المناسبة. علاوة على ذلك، فإن إتقان التقنيات الأساسية هي ايضاً شرطاً ضرورياً لممارسة سيادتنا الرقمية. تشمل التقنيات الرئيسية، على سبيل المثال لا الحصر، تشفير الاتصالات والكشف عن الهجمات السيبرانية وتأمين أجهزة اتصال محمولة محترفة.

- اعتماد إطار لإصدار الشهادات للمنتجات الأمنية عالية المستوى. ان إطار الشهادات الحالي غير مناسب بشكل جيد لتقييم المنتجات الشائعة الاستخدام، مثل الأشياء المتصلة مع بعضها الكترونياً، والتي تكون التكاليف والوقت فيها خارج القدرة. لهذا السبب، يوصى بإدخال نظام أولي لإصدار شهادة الأمن السيبراني على المنتجات، يضاف إلى إطار الشهادات الحالي. وهذا الأخير يبقى مستخدماً في اصدار الشهادات على الأنظمة الحالية في سياقات أخرى غير سياق الأمن السيبراني، مثل وضع علامة "CE" المطلوبة لتسويق بعض السلع والخدمات داخل أوروبا. أما شهادة الأمن السيبراني الأساسية الجديدة فيجب أن تتضمن شروط الامتثال والموائمة مع أفضل الممارسات المعتمدة في الأمن السيبراني، وذلك استناداً الى مواصفات ومعايير محددة مسبقًا. ان اصدار هذه الشهادة يجب أن تقوم به جهة أو هيئة خاصة، حيث تكون مشاركة السلطات العامة مقتصرة على الأعمال غير المباشرة، مثل اصدار التقييمات المعتمدة من قبل الوكالة الوطنية للامن السيبراني NCISA في اعطاء الاعتمادات الخاصة بالأمن السيبراني.

- تعزيز مكافحة الجرائم السيبرانية من خلال الكشف المتقدم عن الادوات المستخدمة في المحاولات الإجرامية؛ عبر تطوير المهارات وزيادة عدد العاملين في هذا المجال وتحسين المواصفات؛ تدريب أصحاب المصلحة المعنيين، مثل القضاة والمدعين العامين، وكذلك موظفي المصارف، إلخ ؛ تأمين المساعدة القانونية لضحايا الجريمة السيبرانية؛ استخدام المثبطات ضد المعتدين والجناة؛ تدريب منتظم على الأمن السيبراني لسلطات تطبيق القانون؛ وأخيرا القيام بالتحديث المنتظم للقوانين والإجراءات تماشيا مع تطور تكنولوجيا المعلومات والاتصالات.

في ظل ظروف محددة، وأثناء العمل على صد هجوم اثناء وقوعه، قد تتحول الاستراتيجية من عقيدة تنفيذية للدفاع فقط إلى ممارسة هجومية. في مثل هذه المناسبات، ينبغي اتخاذ الإجراءات التالية:

- مقاضاة مرتكبي الجرائم السيبرانية. يجب على الحكومة – عن طريق الاستعانة بالسلطات القضائية وأجهزة تطبيق القانون وبالتعاون مع الوكالة الوطنية للأمن السيبراني ونظم المعلومات السعي الى ثني أولئك الذين ينوون الاضرار بمصالح الأمة. ومن اجل تحقيق ذلك، يجب بذل الجهود باستمرار للتوضيح لأي كان أن أي محاولة هجوم سيبرانية، سواء كانت بدافع السرقة أو بهدف ايقاع الأذى، لن تكون سهلة ولا رخيصة الثمن. كما ويجب أن يعرف المهاجمون أنهم لا يستطيعون التصرف من دون عقاب. لذلك يجب أن تكون الحكومة – من خلال السلطات القضائية وأجهزة تطبيق القانون والوكالة الوطنية للأمن السيبراني ونظم المعلومات قادرة على تحديد هوية المهاجمين وعلى التصرف ضدهم بحزم باستخدام الرد الأنسب من بين مجموعة من الأدوات المتاحة لها. كما يجب أن تركز أجهزة تطبيق القانون جهودها على ملاحقة المجرمين الذين يواصلون مهاجمة المواطنين والشركات اللبنانية عبر الفضاء السيبراني. في هذا الاطار، ينبغي على السلطات الوطنية أن تتعاون مع الشركاء الدوليين

في سبيل استهداف المجرمين أينما كانوا وتفكيك بناهم التحتية وشبكات التسهيل الخاصة بهم. كما ويجب أن تواصل أجهزة تطبيق القانون جهودها في سبيل بناء الوعي وتوحيد معايير الأمن السيبراني، بالتعاون الوثيق مع الوكالة الوطنية للأمن السيبراني ونظم المعلومات.

- تعزيز فعالية الاستجابة لدى الأجهزة القضائية من اجل تحسين فرص مكافحة الجرائم السيبرانية، بحيث تكون هذه الاجهزة قادرة على تحديد، عند الضرورة، الجهات التي تقف وراء الهجمات السيبرانية. من أجل التمكن من تحقيق هذا الهدف المعقد، من الضروري وجود الوسائل القانونية المناسبة، إلى جانب توافر القدرات الفنية والخبرات والبنى التحتية والأدوات المتخصصة.

- تعزيز فعالية أجهزة تطبيق القانون بشكل تتمكن من خلاله من اثبات اسناد الهجوم السيبراني الى الجهة الفعلية التي قامت به. كما ويجب اعطاء الصلاحية في اعتماد مثل هذا النوع من الإجراءات، بحكمة، لمؤسسات حكومية محددة وفقًا لطبيعة الإجراء.

- تطوير شبكة دولية للتعاون بين القضاة والمحققين، وكذلك تقديم دورات تدريبية وبرامج تعليمية مخصصة في الهيئات الوطنية والدولية الموجودة في الأراضي اللبنانية.

3.2 تطوير التعاون الدولي في مجال الأمن السيبراني

من اجل تعزيز الآثار الإيجابية الناتجة عن تنفيذ الإستراتيجية الوطنية للأمن السيبراني، من الضروري للبنان أن يعمل عن كثب مع الجهات الإقليمية والدولية الفاعلة. بهذا الخصوص، ينصح باتباع الإجراءات التالية:

- العمل مع الشركاء الدوليين، كالإنتربول، ومنظمات الأمم المتحدة (الاتحاد الدولي للاتصالات، مكتب الأمم المتحدة المعني بالمخدرات والجريمة، معهد الأمم المتحدة الأقاليمي لبحوث الجريمة والعدالة، وما إلى ذلك...)، بعثة الاتحاد الأوروبي في لبنان والمؤسسات والوكالات الأوروبية (مجلس أوروبا، EUROPOL، CEPOL، ENISA وما إلى ذلك)، فضلاً عن التعاون مع المعاهد الدولية الأخرى التي تعنى بمقاييس الأطر (NIST، EBIOS، وما إلى ذلك)، بالاضافة الى التنسيق مع فرق الاستجابة لحوادث المعلوماتية (CSIRT) الدولية منها والإقليمية.

- استخدام شبكة العلاقات القائمة حالياً مع الشركاء الدوليين الرئيسيين للحكومة والعمل على بناء روابط جديدة مع كافة الجهات ومؤسسات الدولية الأخرى في سبيل تبادل المعلومات حول التهديدات الحالية والناشئة، مما يشكل قيمة مضافة إلى الجهود والخبرات الحالية.

- إقامة علاقات ثنائية استراتيجية وفتح قنوات حوار مع أصحاب المصلحة الرئيسيين لتبادل المعلومات حول الحوادث المحتملة.

- بناء شراكات دولية لوضع حد للإفلات من العقاب الواضح لمجرمي الفضاء السيبراني الذين يعملون ضد لبنان من خلال تقديم المجرمين في الولايات القضائية في الخارج إلى العدالة.

- التعاون مع المجتمع الدولي في قضايا الفضاء السيبراني من اجل انشاء مجموعة مشتركة تعنى بمواءمة وتطوير القوانين والانظمة. سيسمح ذلك للحكومة باستغلال جيد لعامل الوقت وبتقليل الإجراءات والتكاليف في هذا الموضوع، وبالتالي يمكنها من التكيف بشكل جيد مع الآليات المشتركة لإدارة الأزمات، واستخدام فعال لآليات التواصل، وامكانية تخفيف حدة التصعيد عند الضرورة. أيضاً،

يجب أن يواصل لبنان العمل من أجل تعميم المعايير المطبقة دولياً في حماية الفضاء السيبراني بهدف تعزيز أمنه، وأن يستند هذا النهج على ثلاثة مبادئ:

- **الوقاية والمنع**: يجب أن تشجع حقيقة أن هناك صعوبة في تحديد القائم الفعلي بالهجوم وبالتالي امكانية تنسيب الهجوم السيبراني الى جهة معينة الدول الراغبة في حماية امنها السيبراني على أن تركز جهودها على اعتماد التدابير الوقائية؛
- **التعاون**: ان التعاون داخل المجتمع الدولي بشأن قضايا الفضاء السيبراني يعد بحد ذاته وسيلة فعالة لزيادة الاستقرار من خلال زيادة التفاهم المتبادل وخلق الثقة بين أصحاب المصلحة. ان ذلك سيؤدي أيضًا إلى إنشاء آليات مشتركة لإدارة الأزمات، للتواصل، والحد من التصعيد.
يجب على لبنان العمل من أجل إبرام اتفاق دولي يحدد للدول التي يمكن استخدام بنيتها التحتية لأغراض مؤذية، كمثل اعتمادها "منصات إطلاق الهجمات" لمهاجمة الدول الأخرى بالوكالة ("تثليث" الهجوم السيبراني)، وغير ذلك من انواع الهجمات، الالتزامات التي عليها القيام بها لمنع مثل هذه الحالات.
- **الاستقرار**: يجب أن يواصل البلد تعزيز مبدأ أن الدول التي تقع ضحية الهجمات السيبرانية لديها كامل الحقوق في اتخاذ التدابير المناسبة للدفاع ضدها، ولكن مع احترام مبدأ الحفاظ على السلام والأمن الدوليين.

3.3 تنمية مقدرات الدولة في سبيل تطوير تكنولوجيا المعلومات والاتصالات

يقع على عاتق الدولة واجب الشروع في برنامج مخصص لأغراض التوعية والتدريب وتكون مهمته اعداد الموظفين المدنيين العاملين في قطاع تكنولوجيا المعلومات والاتصالات وكذلك المواطنين والمهنيين لان يتقنوا جيداً الممارسات الآمنة في الاستخدامات الرقمية. بناء عليه، فان المستخدمين، ومن خلال إدراكهم للمخاطر السيبرانية ومن خلال تدريبهم على تبني السلوك المناسب، سيكونون أكثر قدرة على مواجهة التحديات السيبرانية. إن المواطنين الذين يملكون ما يكفي من العلم والوعي هم الذين يمثلون السدّ الأول في مجال حماية المعلومات، سواء في سياق الاستخدام الخاص (مثال على ذلك حين يتعرض الشباب منهم على وجه الخصوص، لمحتوى غير لائق أو لمضايقات ولأذى بعض الجهات على الإنترنت) أو خلال الممارسات المهنية (الإدارات والشركات). كما يجب اعتبار التدريبات السيبرانية الأمنية جزءًا من الإستراتيجية الوطنية لضمان أن يكون كافة صانعي القرار على دراية كافية بالمخاطر وبكيفية التعامل مع التهديدات. في هذا السياق، يبدو انه من الضروري على الدولة أن تعزز قدراتها البحثية وقدراتها الصناعية كما وتحسّن القدرات الدفاعية للقطاع العام، وان تعمل على إشراك القطاع العام في حوار مع القطاع المصرفي والقطاع الخاص حول سبل تطوير وحماية الاقتصاد الرقمي.

3.4 تعزيز القدرة التعليمية على كامل الأراضي اللبنانية

في سبيل مواجهة النقص الحاصل في المتخصصين والتقنيين الماهرين في مجال الأمن السيبراني، يجب على الحكومة، وإلى جانبها باقي الجامعات والمدارس والمنظمات وبالخصوص الجامعة اللبنانية، الاستثمار في برامج التوعية حول الأمن السيبراني عبر خلق منصة أكاديمية سيبرانية متخصصة. كما يجب عليهم إعداد مناهج جامعية متخصصة لتدريب مختصين رفيعي المستوى يكونون موهوبين ومؤهلين لسد الفجوة الموجودة بين العرض والطلب في مجال الأمن السيبراني.

كما وينبغي أن يكون موضوع الوعي بمسائل الأمن الرقمي جزءًا أساسيًا من مناهج التعليم العالي غير المتخصص بما يضمن تعريف متخرجي المستقبل بمجال الأمن السيبراني. بالتالي، فانه يتعين على كل مؤسسة من هذا النوع أن تضمن قيام الجهات التي تقدم لها دورات تدريبية أولية أو مستمرة بدمج دروس توعية في مجال الأمن السيبراني في مناهج دوراتها المختلفة وأن تعتمد هذه المواد مع كل تدريب مهني يقدم لطلابها.

أيضاً سيكون من المرغوب جداً به أن يعمل على دمج "الأمن السيبراني" في صلب المواد التعليمية التي تختصّ بتكنولوجيا المعلومات في نظام التعليم الوطني (مناهج ما قبل الجامعة)، بما في ذلك ادخال موضوع الأمن السيبراني ضمن المناهج المدرسية واجراء لأنشطة مبتكرة ومحفزة ضمن الفصول والحصص الدراسية واقامة المباريات الاكاديمية والبرامج التدريبية الصيفية وغيرها...

كما ويجب على الدولة وبرعاية من الوكالة الوطنية للأمن السيبراني ونظم المعلومات أن تقوم باجراء تقييم شامل لاحتياجات برامج التدريب الأولية والمستمرة في المديات القصيرة والمتوسطة والطويلة. وهذا يتطلب تعاونًا نشطًا مع وزارة التربية والتعليم وجميع الجهات الفاعلة ذات الصلة في الإدارة العامة و في مؤسسات القطاع الخاص، على أن يشمل ذلك ايضاً النقابات العمالية.

كما ينبغي على الدولة تحديد التكنولوجيات الرئيسية التي تتطلب معرفة متعمقة في عمليات الأمن السيبراني من اجل بناء وتطوير بيئة رقمية موثوقة.

أيضاً وكجزء من عملية التعليم المستمر، ينبغي أن تعمل وحدات الموارد البشرية في المؤسسات والشركات، وخاصة تلك الموجودة في البيئات المهنية المسؤولة ضمن القطاعات الاجتماعية والحكومية، على الاستفادة من التدريب الرقمي والذي يتضمن ايضاً برامج لبث الوعي حول قضايا الأمن السيبراني.

كما ويجب أن تتم دعوة كلية الموظفين المدنيين في المعهد الوطني للإدارة وبالشراكة مع النقابات المهنية المختصة، من اجل العمل معاً لتطوير وتنفيذ برامج التعليم المستمر المصممة لسد احتياجات موظفي الإدارة العامة ومديريها لتصبح متناسبة مع وتيرة النمو والتطور الموجودة لدى القطاع الخاص في مجال الادارة الرقمية والأمن السيبراني.

ولا شك في ان الدولة بأغلب قطاعاتها باتت تدرك جيداً الحاجة إلى تعزيز البحث العلمي والتكنولوجي في المجالات الرقمية، بحيث يجب العمل على تشجيع الجامعات ومعاهد البحوث اللبنانية على أن تقوم بجذب أفضل العقول في مجال الأمن السيبراني. لذلك من المفترض ان تبدأ الحكومة بطرح خطط في هذا المجال من اجل العمل على تشجيع الشراكة الفعالة بين معاهد التدريب والقطاع الصناعي والمهني، وهذا سيؤدي إلى خلق حوار تعاوني حقيقي ومنفعة متبادلة بين الدولة من جهة والجهات الفاعلة في الأمن السيبراني من جهة ثانية. ولتحقيق هذا الهدف، ينبغي النظر في الإجراءات التالية:

- تحديد المجالات العلمية والتكنولوجية التي تعتبرها الحكومة من جهة واوساط الصناعة السيبرانية والأوساط الأكاديمية من جهة ثانية على انها مهمّة و العمل على تحديد الثغرات المحتملة التي يواجهها لبنان في هذا المجال.
- القيام بتمويل ودعم مراكز التميّز الأكاديمي ومعاهد البحوث ومراكز التدريب للدكتوراه من اجل تمكينهم من مقاربة المجالات البحثية المهمة، مثل تحليل البيانات الضخمة وتأمين أنظمة التحكم الصناعية الموثوقة والأبحاث القائمة على العلوم وغيرها...

- العمل على إنشاء مراكز تميّز (وايضاً تشجيع المراكز الحالية) يكون من صلب اهتمامها جذب العلماء والباحثين الكفوئين، والعمل ايضاً من ناحية ثانية على تعميق الشراكة النشطة بين الجامعات والحكومة والصناعة السيبرانية. كما ويجب التركيز على وجه الخصوص، على اهمية دعم صناعة وتطوير المنتجات السيبرانية الرائدة وتشجيع إنشاء شركات جديدة نشيطة في مجال الأمن السيبراني.

- تمويل البحوث وتشجيع الصناعات على تطوير معدات أمنية رفيعة المستوى لتحسين مستوى أمن المنتج للشركات والجمهور العام على حد سواء.

- توفير التمويل والدعم الحكومي لمراكز التميز الأكاديمي ومعاهد البحوث التي تعنى بالبحوث المهمة في التقنيات الرقمية. كما والقيام برعاية طلاب الدكتوراه وحائزي شهادات الدكتوراه لزيادة عدد الخبراء اللبنانيين في مجال الامن السيبراني.

- تعزيز الشراكة بين مراكز البحوث وقطاع الصناعة المعلوماتية، من خلال تشجيع المنح الدراسية والتمويل الثنائي والأبحاث الممولة من جانب الدولة. كما ويحترم هذا الشكل من التعاون مبادىء المساواة والجدارة بشكل دائم، مما يعزز المهارات التقنية في مجال الأمن السيبراني للأشخاص المعنيين.

- انشاء فريق من الخبراء لإدارة الثقة الرقمية والذي ستعهد اليه المهمات التالية:

  - تحديد التقنيات الرئيسية التي تتطلب مهارات ومعرفة معمقة في مجال الأمن السيبراني؛
  - تقييم الاحتياجات التعليمية الأولية والمستمرة؛
  - رصد البحوث ودعم تطويرها؛
  - دعم الشباب من حملة الدكتوراه؛
  - تشجيع التمويل ودعم البحث والتطوير الصناعي في مجال التقنيات الرقمية.

لا شك في أن الموظفين العاملين في القطاع العام، وبصفتهم يمثلون جهات فاعلة رئيسية في الحياة العامة، يحتاجون إلى أن يدركوا، وعلى مختلف مستويات وظائفهم، أهمية حماية البيانات التي لديهم. لذلك ومن اجل تحسين حماية جميع مكونات البلد ومنع أي تهديد سيبراني، يجب على الدولة ان تعمل على:

- تعزيز أمن نظم المعلومات الخاصة بها من خلال تطوير سياسة أمان خاصة بنظم المعلومات لديها وبشبكة الاتصالات والمعلوماتية التي تربط بين الإدارات كما وضمان امن الأجهزة المحمولة.

- اجراء تقييم سنوي لمدى تطبيق سياسة الأمن السيبراني على نظم المعلومات الحكومية ولمدى فعالية التدابير المتخذة في هذا المجال. كما يجب إبلاغ مجلس النواب واللجان المختصة فيه، بالمؤشرات التي تظهر مدى التطبيق الفعلي لسياسات الامن السيبراني وتطور تنفيذها، وتلك التي تشمل أيضًا مدى الاستجابة لتوصيات المجلس الصادرة في مجال الأمن السيبراني. وبصورة أعم، سيضمن المسؤولون الكبار عن قياس الجودة أن المسائل المتعلقة بتعزيز أمن نظم المعلومات مأخوذة بعين الاعتبار في عملية وضع المعايير، والتي سيتم العمل على قياسها على أساس منتظم.

- العمل على اجتذاب المتخصصين السيبرانيين المؤهلين والمدربين تدريباً فعالاً للمساعدة في مهمات الحفاظ على الأمن السيبراني القومي، ويشمل ذلك ايضاً، تقديم المساعدة في عملية التأقلم مع تأثيرات الفضاء السيبراني على العمليات الأمنية التقليدية.

- إدراج عناصر برنامج الأمن السيبراني في جميع برامج التدريب على الخدمة العامة وفي امتحانات التوظيف الخاصة بمهندسي نظم المعلومات والاتصالات، لانهم سيعالجون لاحقاً، بصفتهم موظفين في القطاع العام، البيانات الحساسة والتي يجب أن يعرفوا كيفية حمايتها على مستوى كل وزارة وادارة.

- التأكد من أن تجربة الموظفين العاملين في القطاع العام في مجال الأمن السيبراني هي على المستوى الأمثل طوال فترة خدمتهم.

- منح أجهزة تطبيق القانون والسلطات العامة، والقطاع المصرفي، درجة عالية من الاستقلالية في المسائل المتعلقة بالأمن السيبراني، البنية التحتية، سير العمل الإلكتروني، والقرارات التشغيلية، من حيث صلتها بالمهام الداخلية الموكلة بها. ويجب أن يتوافق هذا النهج العام دائمًا مع استراتيجية الأمن السيبراني للحكومة، والتي يجب ضمانها من خلال وكالة وطنية تشكل على أعلى مستوى في الدفاع الوطني.

- يتلقى رئيس الوزراء تقريرًا سريًا نصف سنوي نتيجة لعمليات التدقيق في التهديدات والهجمات ونقاط الضعف السيبرانية والاستجابة المنسقة من جميع الجهات المعنية.

- الحفاظ على استقلالية لبنان في صنع القرار السيبراني، بما في ذلك تعبئة الموارد البشرية اللازمة ووضع الميزانية.

3.5 تعزيز القدرات الصناعية والتقنية

يجب على لبنان تطوير بيئة مؤاتية لتنمية الاقتصاد الرقمي المحلي وأن يعمل للترويج على المستوى الدولي لمنتجاته وخدماته الرقمية. كما يجب على الدولة أن تضمن أن تكون كافة مكونات البلد من إدارات وشركات ومواطنين باستطاعتها الحصول على المنتجات والخدمات الرقمية التي تحظى بمستويات من الثقة والأمان تتلاءم مع التهديدات السيبرانية. لهذا الغرض، يجب على الدولة العمل على:

- تطوير وتعزيز المعروض الوطني من المنتجات والخدمات والحلول الأمنية السيبرانية، وذلك بالتعاون مع الوزارات والادارات المختلفة (الاتصالات، الصناعة، الاقتصاد، الداخلية، الدفاع، الشؤون الخارجية، مكتب وزير الدولة لشؤون التنمية الادارية، إلخ ...) وايضاً بالتنسيق مع الوكالة الوطنية للأمن السيبراني ونظم المعلومات. كما ويجب على الدولة أن تعتمد سياسة صناعية وطنية تهدف عبرها الى تعزيز الشركات الوطنية وتشجيعها على تطوير منتجات وخدمات الأمن للحاسوب. كما ويجب على الدولة أيضًا أن تأخذ على عاتقها أمر تشجيع وتسهيل عمل الشركات الجديدة والناشئة حديثاً والتي تعمل في مجال صناعة الأمن السيبراني وتمكينها من تطوير وإنتاج منتجات سيبرانية متطورة وقادرة على المنافسة.

- التعاون مع كافة أصحاب المصلحة - الشركات العاملة في مجال الأمن السيبراني على وجه الخصوص - ومع المؤسسات الأكاديمية من اجل توفير فرص التدريب والمشورة اللازمين لسد احتياجات القطاعين العام والخاص. ونظرًا لأن وجود قطاع مزدهر ومتطور يعمل في مجال الأمن السيبراني بات يعد من ضرورات الاقتصاد الرقمي الوطني الحديث، فإن على الدولة أن تسعى إلى تطوير فرص التعاون مع القطاع الخاص في مجالات التدريب والتعليم وأن تعمل على تعزيز المرافق التي تعمل في هذا المجال في سبيل الحفاظ على المهارات وتعزيز عملها. من جانبها، يتعين ايضاً على الشركات التي

تعمل في مجال الامن السيبراني أن تزود الحكومة والشركات من جانبها بما تحتاجه من التقنيات المتطورة، ومن تدريب، وكما وتقديم ما يلزم من المشورة.

- انتاج / شراء المعدات الموثوقة في مجال الأمن السيبراني لكشف التهديدات وتأمين الحماية من الهجمات السيبرانية، بالأخص لمشغلي البنى التحتية ذات الأهمية الحيوية بالإضافة الى العمل على تأمين الحاجة الى منتجات رقمية محمولة آمنة لجميع القطاعات. ان معظم الأجهزة والمنتجات الرقمية المتاحة في السوق اليوم لا تملك مستوى كافي من الامان الرقمي. لذلك فان العمل على تأمين منتجات تحتوي على مستوى أمان كافي هو بحد ذاته سيعتبر ميزة تنافسية بين الشركات. من هنا يجب الاهتمام بوضع عملية لتقييم واعطاء شهادات أمن سيبراني تظهر مدى مطابقة المعدات المستخدمة في المهمات الحيوية للمعايير الموضوعة في مجال الامن والامان السيبراني.

- العمل من خلال الوكالة الوطنية للأمن السيبراني ونظم المعلومات على تحديد وتسمية جميع مشغلي البنى التحتية ذات الأهمية الحيوية في البلد بهدف ضمان تطبيقهم لسياسات الأمن السيبراني المخصصة لهم ودفعهم الى اعتماد أفضل الممارسات والمعايير المتبعة في هذا المجال.

- العمل على تأهيل منتجات الأمن السيبراني والأجهزة والخدمات المتعلقة بها وتحديد مدى مناعتها بخاصة تلك التي يمكن أن تعرض أنشطة تكنولوجيا المعلومات في البلد للخطر من خلال ضعف مناعتها اتجاه التجسس السيبراني والهجمات السيبرانية التي ترعاها الحكومات.

3.6 مساعدة شركات الأمن السيبراني المحلية على المستوى الدولي

من الضروري للبنان أن يدعم قطاع صناعي متطور مختص في مجال الأمن السيبراني، ولأجل ذلك يجب على الحكومة القيام بـ:

- دعم المبادرات التعاونية بين المكونات المختلفة العاملة في الصناعة الرقمية على مستوى القطاع الخاص. كما ويجب على الحكومة ان تشجع التنمية الاقتصادية لقطاع صناعة الأمن السيبراني بهدف تشجيع التطوير المحلي لمنتجات وخدمات الأمن السيبراني والتي تضمن عدم اعتماد لبنان على منتجات الأمن الأجنبية والتي يخضع استخدامها في العادة لسيطرة وشروط الدول المنتجة لها.

- تعزيز صورة وقدرة المعروض اللبناني التنافسية في الخارج وتسهيل امر دخول الشركات الصغيرة والمتوسطة والشركات الناشئة إلى الأسواق الدولية. ويجب ان تتم هيكلة وتعزيز التنسيق بين الإدارات المختلفة من اجل العمل على تحقيق هذا الغرض. كما يجب وضع وتنفيذ خطة منظمة وشاملة لدعم الشركات تتجاوز حدود الإجراءات التي تقوم بها عادة كل واحدة من الوزارات والهيئات الحكومية، والتي غالباً ما تكون معزولة ومنفردة وغير كافية. كما يجب توضيح كافة الإجراءات التي تحكم عمليات تصدير حلول الأمن السيبراني والخطوات اللازمة التي تهدف الى تحسين وتشجيع هذه المنتجات.

- إنشاء أنظمة دعم محددة للجهات الفاعلة في الأمن السيبراني، مع شروح واضحة لشروط الوصول اليها وكيفية التطبيق. بالتوازي، يجب توضيح وتحسين شروط الوصول وتطبيق أنظمة الدعم الحالية.

- وضع إجراءات واضحة للتحكم في تصدير حلول الأمن السيبراني.

- دمج معايير الأمن في شروط وعمليات اختيار وشراء المنتجات والخدمات الرقمية في كافة المشتريات العامة.

3.7 تعزيز التعاون بين القطاعين العام والخاص

ان الحكومة وبصفتها جهة فاعلة رئيسية في الاقتصاد ومزود رئيسي للخدمات، تعتبر المستخدم الأول والرئيسي لمنتجات الأمن السيبراني عالية المستوى. كما وان خلق نفاذية أكبر في العلاقة بين القطاعين العام والخاص في لبنان سيضمن تعزيز الجهود الوطنية في مجال الأمن الرقمي يوماً بعد يوم، كما سيمكن كل مستفيد من هذه المنتجات من اكتشاف التهديدات السيبرانية والتعامل معها بشكل أفضل. لذلك سيكون من الضروري على الدولة ان تعمل على:

- تشجيع إنشاء وتطوير قطاع خاص يعنى بصناعة الأمن السيبراني، وذلك بالتعاون بين الهيئات الحكومية والأوساط الأكاديمية والقطاع الخاص.
- تعزيز التعاون بين الحكومة وقطاع الصناعة المعلوماتية بهدف حصول كل منهما على ما يكفيه من معلومات استباقية حول التهديدات، وبهدف ضمان توافر المعلومات التي يجب على كل طرف منهما أن يقدمها بهدف تعطيل هذه التهديدات.
- تشجيع الشراكة بين الحكومة وقطاع الصناعة المعلوماتية لمساعدته في تحديد أوجه المساعدة التي تحقق له النمو والابتكار وخاصة في مجال صناعات الامن السيبراني.
- إنشاء نطام تحفيز ودعم للشركات الناشئة المختصة بالأمن السيبراني.
- التعاون مع القطاع المالي من اجل جعل لبنان بيئة محصنة في وجه الذين يسعون إلى بيع المسروقات الرقمية، وصولاً الى تفكيك وتعطيل شبكاتهم التي يعملون بواسطتها.
- العمل مع الوكالة الوطنية للأمن السيبراني ونظم المعلومات على تسهيل عملية نقل المعرفة المكتسبة لديها إلى القطاع الخاص، من أجل مساعدته على الاهتمام بالأمن السيبراني الخاص به، مع العمل على تحديد دقيق لموفري الخدمة المؤهلين والجديرين بالثقة، لان هذا الأمر يساعد في اكتشاف ووقف النمو الحتمي في عدد الهجمات السيبرانية الذي يستهدف قطاع الأعمال. كما يجب العمل على دمج متطلبات الأمن السيبراني في اعمال الشراء العامة ومسودات التشريعات المتعلقة بتكنولوجيا المعلومات والاتصالات، مع الحرص على تحفيز النمو في قطاع الأمن السيبراني، وكل ذلك عبر:
  - دمج معايير الأمن في اختيار المنتجات والخدمات الرقمية في عمليات الشراء العامة ؛
  - تقديم عامل مكافأة اضافي إذا كان العرض المقدم مصحوبًا بتحليل مخاطر للأمن السيبراني ؛
  - التأكد من تضمين القوانين في القسم المخصص فيها بتقييم الآثار المترتبة على تطبيقها، قسماً مخصصًا للتكنولوجيا الرقمية بما في ذلك عن الأمن السيبراني.

3.8 دور أجهزة تطبيق القانون

بهدف تحسين قدرات الأمن السيبراني، يجب على الأجهزة المكلفة تطبيق القانون اتخاذ الإجراءات التالية:

- زيادة قدرة كافة أجهزة تطبيق القانون، بالتنسيق مع الجهات الدولية الشريكة، على امكانية توقع وتحديد وتعطيل جميع الأنشطة السيبرانية المعادية. وهذا الأمر سيساعد كافة الأجهزة على تحسين عملية جمع المعلومات الاستخبارية واستغلالها، وفي الحصول على معلومات وقائية حول نوايا وقدرات المهاجمين السيبرانيين.

- تعزيز جهود مختلف الأجهزة المكلفة تطبيق القانون من اجل زيادة فعالية استهداف وتوقيف ومحاكمة المجرمين أينما كانوا وبالتنسيق مع الشركاء المحليين والدوليين. ان واجب هذه الأجهزة في كل وقت هو التصدي للمجرمين السيبرانيين الذين يصرون على مهاجمة المواطنين أو الشركات أو المؤسسات اللبنانية، وذلك من خلال العمل على تفكيك بناهم التحتية والشبكات التي تسهل عملهم.

- يجب على الأجهزة المكلفة تطبيق القانون من جهة، كما على القطاع المصرفي من جهة ثانية، أن يواصلا جهودهما التي تساهم في زيادة ونشر وتعميم الوعي حول قضايا الأمن السيبراني.

- تحسين الإجراءات القضائية التي تتبعها أجهزة تطبيق القانون في اجراء التحقيقات والتي تتم عادة بإشراف السلطة القضائية المختصة.

- وبما أن أهم عامل في التمكين هو التدريب الفني المهني الرفيع المستوى، فان هذا التدريب يجب أن يشمل تدريبات عملية، ودورات، وتمارين، مبنية على العمل المخبري. ويمكن لهذه الجهات عبر وضع اجراءات اضافية لتعزيز الجودة أن تسرع وتعزز هذه العملية التدريبية – وتشمل هذه الاجراءات العلاقات الإجرائية والتقنية والتشغيلية المخصصة مع الهيئات والمؤسسات الأمنية والفرق المتخصصة في الأمن السيبراني الدولي، مدعومة بالتبادل المنتظم للمعلومات.

- تعزيز التنسيق بين مختلف الأجهزة المكلفة تطبيق القانون، بما في ذلك تبادل المعلومات والتحاليل حول كافة التهديدات.

- جعل عملية الترقب والوقاية أولوية للسلطات المختصة التي تتعامل مع أمن نظم المعلومات. ويمكن تحقيق ذلك عبر انشاء "منصة الاستخبارات للتهديدات السيبرانية -CTI". تتلقى هذه المنصة بيانات بصورة متواصلة من كافة المصادر المحلية (جميع الوكالات الوطنية العاملة في هذا المجال) وايضًا من المصادر الأجنبية. كما قد يتم الحصول على هذه البيانات من خلال شراء مجموعات من البيانات التجارية ("التلقيمات") من عدد قليل من الشركات المتخصصة، والتي توفر معلومات محايدة بنسبة 100 ٪، أي غير مدعومة لا رسميًا أو غير رسمياً من قبل أي حكومة أجنبية. كما سوف تعمل "منصة الاستخبارات للتهديدات السيبرانية" كنواة الفريق الوطني استجابة لطوارئ المعلوماتية -CERT) (LB، **والذي يجب إنشاؤه في كنف الوكالة الوطنية للأمن السيبراني ونظم المعلومات**. ويجب على فريق الاستجابة الوطني توفير تلقيمات البيانات والتنبيهات والإنذارات المبكرة وما إلى ذلك إلى كافة مراكز خدمات امن المعلومات المحلية (SOCs).

- تعزيز قدرات الأمن السيبرانية لأجهزة الاستخبارات والجيش، من خلال، على سبيل المثال، تأمين الدورات التدريبية والدعم، وجعلها تعتمد على أفضل الممارسات المتبعة من وكالات الأمن السيبراني المماثلة في معظم البلدان المتقدمة.

- تسهيل التنسيق بين كافة الأجهزة الوطنية المكلفة تطبيق القانون، من خلال، على سبيل المثال، استضافة اجتماعات دورية مشتركة لمناقشة مسائل الأمن السيبراني، وتوفير التسهيلات اللازمة فيما

بينها من أجل الاجتماع والرد على الحوادث السيبرانية الوطنية، واستضافة تدريبات الاستجابة للحوادث السيبرانية المحلية.

الفصل الرابع: الأهداف

يجب على الاستراتيجية الوطنية للأمن السيبراني أن تؤمن للقطاعين العام والخاص وكذلك للمواطنين، خطة دفاعية استراتيجية ضد التهديدات السيبرانية، وان يتم العمل على ضمان استدامة عملها من خلال إضفاء الطابع المؤسسي عليها، وذلك يتم عبر تحديد هيكلية عملانية وأهداف واضحة. من ناحية أخرى، يجب أن تتضمن استراتيجية الأمن السيبراني ما يكفي من إجراءات حاسمة في سبيل حماية الاقتصاد اللبناني وضمان خصوصية المواطنين اللبنانيين. بالتالي فان الهدف الرئيسي لهذه الاستراتيجية الوطنية يتمثل بشكل رئيسي في وضع مجموعة من القرارات التي يجب أن تترجم لاحقاً بإجراءات عملانية تجعل من لبنان بلداً واثقًا وقادرًا ومرنًا ومحصناً في عالم رقمي سريع التطور.

بناء على ما سبق، فان هذه الاستراتيجية تصبو الى تحقيق الأهداف الرئيسية التالية:

- تشجيع كل من الحكومة والمؤسسات والشركات والأفراد على ان يؤدي كل واحد منهم دوره كما هو مطلوب في سياق هذا الجهد الجماعي الذي يهدف الى تأمين الفضاء السيبراني الوطني؛
- العمل على تأمين توافر وسهولة استخدام الخدمات السيبرانية، وتعزيز الشفافية الرقمية، وتشجيع المواطنين على المشاركة في الحوكمة وأخيراً العمل من اجل خفض مستوى التهديدات السيبرانية وكلفة الهجمات السيبرانية في القطاعين العام والخاص؛
- العمل على تطبيق آلية مناسبة وفعالة مهمتها إدارة الانذارات عند وقوع الحوادث وكيفية التعامل معها عند وقوعها؛
- إدارة التعامل مع الحوادث الأمنية السيبرانية بطريقة تؤدي الى تقليل المخاطر الناتجة عنها، وتمكن بالتالي من اكتساب المقدرة على تقدير التهديدات السيبرانية الحالية والقادمة بدقة؛
- الاستجابة السريعة والفعالة للتهديدات السيبرانية، واستخدام القدرات التي تتناسب مع حجم الحوادث الكبرى في الفضاء السيبراني فور حدوثها من اجل التمكن من الحفاظ على أمان ومرونة وعمل الشبكات والبيانات والأنظمة المعلوماتية؛
- العمل على تطوير كافة الأطر والوسائل القانونية والإجرائية والتقنية اللازمة للدفاع عن لبنان ضد التهديدات السيبرانية المتطورة بشكل مستمر، مع تأمين استجابة فعالة ضد الحوادث، وضمان حماية شبكات وبيانات وأنظمة البلد والحفاظ على مرونة خدماتها؛
- تحسين القدرات المحلية القادرة على الاستجابة للهجمات السيبرانية وذلك من خلال اتخاذ التدابير المناسبة والعمل على زيادة مناعة البلاد امام اكثر التهديدات السيبرانية شيوعًا. ان الحكومة تحتاج في هذا المجال إلى الاستفادة من قدراتها وكذلك من كافة قدرات صناعات الامن السيبراني المحلية، ولذلك يقع على عاتقها ايضاً دعم هذه الصناعات بشكل نشط من اجل تمكينها من تطوير قدراتها. أخيراً ان الحكومة مسؤولة عن تنفيذ تدابير الدفاع السيبراني الفعالة التي تهدف الى لتحسين مستويات أمان تكنولوجيا المعلومات والاتصالات بشكل كبير على الشبكات المحلية؛

- تقديم الدعم والمساعدة للمؤسسات فور وقوع الحوادث الأمنية السيبرانية. كما يجب على الدولة، على وجه الخصوص، ضمان تعاون القطاع العام بنشاط مع القطاع الخاص، سواء عند اتخاذ الاجراء الوقائي أو عند الاستجابة لحادث ما. وهنا نشير الى انه يجب على عمليات إدارة الحوادث الوطنية أن تتبع نهجًا شاملاً يمكن لها من خلاله التعلم من الشركاء وتبادل تقنيات التخفيف من الآثار؛

- ضمان أن **يتم الإبلاغ عن الحوادث إلزاميًا وفوريًا إلى الوكالة الوطنية للأمن السيبراني ونظم المعلومات**، مما يسمح للجميع بفهم حجم التهديد ونطاقه وشدته؛

- تحديد الأسباب الجذرية المسببة للهجمات على المستوى الوطني، والحد من حالات الاستغلال المتكرر التي تطاول العديد من الضحايا والقطاعات؛

- استخدام العلاقات التي تملكها الأطراف المعنية مع فرق الاستجابة الأخرى، على الصعيدين المحلي والدولي، ليكون هذا التنسيق جزءاً من بروتوكول إدارة الحوادث؛

- القيام بقياس لمستوى تطور الجريمة السيبرانية باستخدام إحصائيات وتحليلات موثوقة للجرائم الرقمية، وذلك بهدف التمكن من توجيه العمل المناسب عند الاستجابة للحوادث. لأنه في حال غياب مثل هذه الإحصاءات، لا يمكن للسلطات العامة إعادة تقييم السياسات بشكل مستمر واتخاذ التدابير المناسبة. في هذا الاطار، يجب على وزارة الداخلية مثلاً أن تستخدم أدوات جديدة لرصد تطور الجريمة السيبرانية بهدف استخدام النتائج في توجيه العمل العام؛

- إنشاء قاعدة بيانات مختصة بالحوادث السيبرانية من اجل تمكين كل الاطراف من الاطلاع الواسع على التفاصيل المتعلقة بها والحصول بالتالي على تحليل مفصل يحدد اتجاهات التهديد السيبراني بطريقة تمكنهم من تحديد حلول الأمن المناسبة و / أو معرفة الاحتياجات الى منتج محدد أو خدمة معينة. من شأن ذلك كله أن يفيد صناعة الأمن السيبراني بكافة مكوناتها، والتي تعتمد في تقييمها للمخاطر، على البيانات الإحصائية والتاريخية عن تطور الحوادث السيبرانية ؛

- تأمين بيئة سيبرانية آمنة لعمل مشغلي البنى التحتية ذات الأهمية الحيوية. من جهتهم، يجب على كل مشغل منهم وضع وتنفيذ تدابير الأمان واتباع السياسات الأمنية الخاصة به بشكل يتماشى مع اهداف هذه الاستراتيجية، وأن يعملوا على تفعيل مراكز العمليات الأمنية الخاصة بهم ليتمكنوا من رصد الحوادث الأمنية والتفاعل معها بكفاءة وأن يرتكزوا على كافة التقنيات اللازمة لذلك، كتقنيات تحليل السلوك، والترابط الذكي وعبر الاستفادة من فلترة التنبيهات.الأمنية المتوافرة لهم.

- تشجيع بائعي الأجهزة والبرامج والحلول الرقمية على تطوير وبيع المنتجات التي يفترض أن تكون فيها عناصر التحكم في الأمان مفعلة بشكل تلقائي ؛

- يجب على الوكالة الوطنية للأمن السيبراني ونظم المعلومات أن تعمل، بعد امتثال البيئة السيبرانية اللبنانية للمعايير الأساسية للأمان على مستوى المنتج / العنصر التكنولوجي الفردي كما على مستوى المستخدم الفردي (أصحاب المصلحة)، على توفير معايير جديدة تتماشَّى مع الهدف الرئيسي الا وهو الحصول بالكامل على *أمان من* ضمن *التصميم* لكل جهاز مستخدم في تكنولوجيا المعلومات والاتصالات أو أي جهاز آخر يكون عنده قابلية الاتصال بالشبكة العامة عبر عنوان انترنت – IP – من العناوين العامة المخصصة للبنان؛

- العمل على أن يمتثل جميع مقدمي الخدمات للقوانين والانظمة الصادرة بمجال الأمن السيبراني. ويكمن التحدي في هذا المجال في التأكد من قدرة المشغل أو مقدم الخدمة على إجراء تغيير جذري في عناصر الأمان المضمنة في البرامج والأجهزة والتي تم وضعها من قبل الشركة المصنعة، بما يجعلها تتوافق مع المعايير اللبنانية الموضوعة من قبل الوكالة، وذلك قبل إطلاق هذا المنتج في السوق المحلي. كما ويجب أيضاً على المستخدم ان يكون قادرًا على الاستفادة من أقصى قدر من الأمان الممنوح على أي منتج أو خدمة قابلة للتطبيق تجاريًا، مع حفاظه في نفس الوقت على سياق الإنترنت المفتوح والمتاح بحرية؛

- التأكيد على القيم الإنسانية في الفضاء السيبراني، عبر العمل على تعزيز معايير احترام حقوق الإنسان وضمان اعطاء الأفراد كافة الوسائل التي تسمح لهم بالحصول على حق تقرير مصير رقمي وخصوصية كاملة وحماية كافية لمعطياتهم الشخصية؛

- العمل على تغيير السلوكيات السائدة بما يضمن أن تمتلك الجهات والمؤسسات الحكومية والمؤسسات والشركات الأخرى كافة ومعهم الأفراد المعرفة والمهارات اللازمة التي تخولهم من الدفاع عن أنفسهم في الفضاء السيبراني، واتخاذ التدابير المناسبة لحماية أنفسهم وعملائهم من الأذى الناجم عن الهجمات السيبرانية؛

- توعية الشعب اللبناني على الممارسات الآمنة في الفضاء السيبراني عبر إطلاق برنامج طموح يتّبع خطوات العمل التالية:

  - دمج موضوع التوعية حول مفاهيم الأمن السيبراني في جميع برامج التعليم العالي والتعليم المستمر؛ كما ودمج مواضيع الأمن السيبراني في نظام التعليم ما قبل الجامعي (في شكل أنشطة في الفصول الدراسية ومباريات ودورات تدريبية صيفية) كما وفي البرامج الدراسية المخصصة لمجالات محددة، في محال المعلوماتية؛ والعمل ايضاً على تنفيذ برامج التوعية بأمن الفضاء السيبراني بالشراكة مع الجامعات والمدارس والمؤسسات الخاصة؛
  - إطلاق دعوة للتعبير عن الاهتمام بإنتاج محتوى لزيادة الوعي السيبراني موجه إلى عامة الجمهور؛
  - إطلاق مبادرات وطنية بالشراكة مع الأجهزة الأمنية لزيادة الوعي بمخاطر الإنترنت وتعليم طلاب المدارس الابتدائية عليها؛
  - إنشاء بوابة رقمية مختصة بالتعليم الرقمي بالتعاون مع المجتمع الأكاديمي؛
  - تطوير مشاريع لحملات تواصل كجزء من "قضية وطنية كبرى" (لبناء الثقة في المنتجات الرقمية)؛
  - الترويج لأفضل الممارسات المتبعة في مجال الأمن السيبراني وإطلاق حملات توعية لإشراك كافة شرائح المجتمع والعمل على زيادة الوعي من مخاطر تلاعب الاعداء بالمعلومات في الفضاء السيبراني.

- ضمان حصول تغيير جذري في السلوك العام في موضوع التعامل مع التهديدات السيبرانية، مع العمل على توجيه مجموعة رسائل متماسكة بشكل دوري تعنى بالتوجيه الأمني السيبراني، تصدر من طرف كل من الحكومة وشركائها حول هذا الموضوع؛

- تحسين ثقافة الأمن السيبراني في شرائح المجتمع اللبناني المختلفة من خلال تشجيعهم على فهم المخاطر السيبرانية وعبر الترويج لثقافة "النظافة السيبرانية"؛

- إعلام الجمهور دورياً بالمخاطر الناتجة عن التلاعب بالمعطيات وبتقنيات الدعاية المستخدمة من قبل الجهات الخبيثة على الإنترنت. كما يجب أن يعي الجميع ضرورة استخدام أجهزة الدفاع والأمن المناسبة كونها هي الكفيلة بكشف الدعاية الضارة و دفع حوادث الإرهاب السيبراني، كما يجب أن يتم تقديم توصيات للحكومة حول انجع السبل في اتخاذ التدابير والاجراءات المضادة. ان من الأهمية بمكان في هذا السياق، العمل على إنشاء منصة معلومات مختصة تعمل على الرد على الأعمال التي تهدف الى بث الدعاية العدائية أو زعزعة الاستقرار؛

- العمل على تعزيز أمن أكثر نظم المعلومات حساسية في البنى التحتية الحيوية لدى المشغلين في القطاعين العام والخاص، وذلك عبر وضع تدابير تشريعية مناسبة يتم تحديثها بانتظام. وأن يتم توسيع هذه العملية تدريجياً لتشمل كافة المشغلين في القطاعين العام والخاص المشاركين في إدارة أو إدارة نظم المعلومات الحساسة؛

- التأكد من أن جهات المكلفة تطبيق القانون تملك أقوى الامكانيات الدفاعية المخصصة للحفاظ على شبكاتها ومنصاتها الرقمية آمنة ومرنة. يجب أن يكون جميع أصحاب المصلحة هنا قادرين على مواصلة العمل والحفاظ على حريتهم في العمل في ظل التهديدات السيبرانية، وأن تكون هناك قدرة على تقديم المساعدة في حالة وقوع هجوم سيبراني واسع النطاق على المستوى الوطني؛

- إعداد المتطلبات القانونية والتشغيلية اللازمة لإضفاء الطابع المؤسسي على الاستراتيجية الوطنية من خلال العمل على إنشاء سلطة مركزية تعمل على أعلى مستوى من اجل تأمين الأمن السيبراني للبلد: الوكالة الوطنية للأمن السيبراني ونظم المعلومات – NCISA.

الجزء الثاني – المأسسة
الوكالة الوطنية للأمن السيبراني ونظم المعلومات
(NCISA)

لا شك في أن أمن أنظمة المعلومات في المؤسسات العامة والخاصة هو أمر ذو أهمية حاسمة عند مجموعة واسعة من المؤسسات والجهات الفاعلة، العامة منها والخاصة، وعلى الصعيدين المحلي والدولي على حد سواء.

وسواءً أكان متصلاً بأمر ضمن المجال السياسي أو الدبلوماسي أو الاقتصادي أو العسكري أو غيرها من المجالات، فلقد أصبح الأمن السيبراني اليوم مصدر قلق جماعي وأمر حساس ذو أولوية وطنية. ولم يعد خافياً على أحد أننا نشهد تزايداً مضطرداً في التهديدات والهجمات السيبرانية والتي يمكن أن تلحق أضرارًا جسيمة بمصالح الأمة كافة. في مواجهة هذا الخطر، يجب أن يكون لدى لبنان، مثله مثل العديد من البلدان الأخرى حول العالم، نظام دفاع حاسوبي وطني قوي وموثوق.

من اجل تحقيق هذا الهدف، خلصت اللجنة الوطنية للأمن السيبراني إلى أن إنشاء وكالة وطنية لأمن أنظمة المعلومات هو خطوة ضرورية وأساسية في سبيل اتباع نهج منسق ونشط في إدارة مشاكل الأمن السيبراني وتتبع نمو وتنوع التهديدات السيبرانية والتعامل بقوة مع تطورها المتزايد.

أن وضع مرجعية هذه الوكالة مباشرة لدى رئاسة الحكومة وجعلها جزءاً من المجلس الأعلى للدفاع هي ايضاً، وبلا أدنى شك خطوة حاسمة أخرى تظهر جدية واصرار الدولة على الاستجابة للتحديات الكبرى الحالية والمستقبلية في مجال الأمن السيبراني.

هذا ومن المفترض أن تؤدي هذه الوكالة مهامها بالتنسيق الوثيق مع كافة الوزارات والمؤسسات العامة وجهات تطبيق القانون، ولكن من دون التنازع حول الأدوار القانونية المفوضة لكل منها.

وبالتالي فان هذه الوكالة ستمكن لبنان من جعل عملية اتخاذ القرارات المتعلقة بالامن السيبراني عملية مركزية سريعة وفعالة كما وسيسهل وجودها أمر تنسيق هذه القرارات على مستوى مختلف الخدمات الحكومية، وهذا امر حاسم في زيادة قدرة وفاعلية البلاد على مواجهة التهديدات السيبرانية.

استناداً الى ما تقدم، يقدم الجزء الثاني من الاستراتيجية الوطنية وصفًا تفصيليًا لدور الوكالة ووظائفها والقطاعات المختلفة التي ستعمل ضمنها.

الفصل الخامس: إنشاء وتأسيس الوكالة الوطنية للأمن السيبراني ونظم المعلومات

ان الوكالة الوطنية للأمن السيبراني ونظم المعلومات (NCSIA) هي هيئة حكومية، تعمل تحت إشراف المجلس الأعلى للدفاع، وتكون هي المسؤولة عن وضع سياسات وإجراءات الأمن السيبراني لكافة أنظمة المعلومات في لبنان. وتماشياً مع مندرجات الاستراتيجية الوطنية اللبنانية للأمن السيبراني، تقوم الوكالة بتأدية واجباتها العامة وفقًا للتشريعات والقواعد والأنظمة المتعلقة بأمن الفضاء السيبراني.

يشمل نطاق عمل هذه الوكالة، من جملة ما يشمل، وضع السياسات، تحديد الإجراءات، وضع الخطط، تقييم مواطن الضعف، تحديد التهديدات، تعزيز الوعي، واصدار التنبيهات - مع توصيات – وكل ذلك بهدف تأمين الاستجابة السريعة والفعالة ضد الهجمات السيبرانية، بما يؤدي الى الحفاظ على بيئة سيبرانية لبنانية آمنة، نظيفة ومرنة.

إضافة إلى ذلك، ستقوم الوكالة كذلك بتحديد وتسمية البنى التحتية المعلوماتية الحيوية، كما وستساعد على تصنيف البيانات التي تحتويها، وتحدّد إطاراً وطنياً مهمته المصادقة على المعايير المطلوبة لمنتجات الأمان الرقمية عالية المستوى وإصدار شهادات المطابقة معها. علاوة على ذلك، تضع الوكالة نصب أعينها هدفًا مهماً هو رفع مستوى الوعي لمخاطر التهديدات السيبرانية ونشر أسس المعرفة حول مفاهيم الأمن السيبراني من خلال وضع ونشر برامج التوعية والتدريب المختصة، وكذلك عبر تطبيق المفاهيم العامة للتعاون الدولي.

ستلعب الوكالة أيضاً دور اساسي كمنسق ومسهّل: ستنسق عمل جميع الأجهزة الحكومية والوزارات والمؤسسات العامة المعنية كما وستعزز وتسهل التعاون بين القطاعين العام والخاص وبين اوساط الصناعات ذات الصلة والأوساط الأكاديمية.

كما ويدخل أيضاً في صلب مهام الوكالة، تقديم المساعدة والدعم الى جميع الأطراف المعنيين بالأمن السيبراني في القطاعين العام والخاص. علاوة على ذلك، تقدم الوكالة الوطنية المشورة الفنية وتضع مبادئ توجيهية تعكس أولويات الحماية السيبرانية وتبيّن أفضل الممارسات المتعلقة بالأمن السيبراني لكافة شركات ومؤسسات القطاعين العام والخاص على حد سواء.

هذا وستعمل الوكالة عن كثب مع الأطراف المعنية بالأمن السيبراني، من وزارات ومؤسسات عامة وخاصة بالإضافة الى الأجهزة الأمنية واجهزة تطبيق القانون والقطاع الصناعي، في سبيل تقييم وتبادل المعلومات حول أحدث التهديدات السيبرانية الاجرامية، ولمساعدة كافة أصحاب المصلحة المعنيين، وذلك من أجل الدفاع ضد التهديدات، وتخفيف عواقب الهجمات السيبرانية على كافة المستهدفين بها في لبنان (إدارات عامة، مؤسسات، شركات، صناعات وأفراد...)، كما ستعمل من أجل انشاء مفهوم وطني شامل حول كيفية التعامل مع حالات الطوارئ في الفضاء السيبراني.

5.1 تفويض الوكالة على المستوى الوطني

سوف تكتسب الوكالة الوطنية للأمن السيبراني ونظم المعلومات (NCSIA) شرعيتها من تفويض وطني يُعطى لها، يتم من خلاله تحديد دورها كما وتحدد وظائفها ومسؤولياتها، وفقًا للاحتياجات الوطنية للأمن السيبراني، وعلى النحو المحدد في استراتيجية الحكومة.

وفقاً لذلك، سيتم تكليف الوكالة بالمهام التالية:

1. الإشراف على، وتسهيل عملية تصميم وتنفيذ وتنسيق وسائل الاتصال الإلكتروني الآمن بين الوزارات / بين الأقسام على المستوى الحكومي.
2. الاشراف على، وتطوير وتنفيذ سياسة الأمن السيبراني في كافة نظم المعلومات في البلد، كما وعليها أن تتأكد من فعالية التدابير المعتمدة لذلك بالاستناد الى تقرير المراجعة والتقييم السري الذي يتم تقديمه سنويًا إلى رئيس الوزراء.
3. إنشاء وادارة فريق على المستوى الوطني للاستجابة لحوادث الأمن السيبراني (CSIRT) والذي مهمته العمل يوميًا بالتعاون والتنسيق الكامل مع الوزارات والمؤسسات وكافة الجهات المكلفة تطبيق القانون. ان الـ CSIRT هو بمثابة مستوعب مركزي للحوادث السيبرانية في جميع أنحاء البلد، حيث يتبادل عبره جميع أصحاب المصلحة إخطاراتهم حول الهجمات الإلكترونية وتفاصيلها. ويدعم الفريق أيضاً عمل جميع المشاركين في التصدي والدفاع والوقاية من الهجمات المبلّغ عنها. كما أنه يحدد مقياس التهديدات السيبرانية ويصدر تقريرًا سنويًا عن المراقبة الوطنية للتهديدات. إن هذا الفريق سيعمل بالتعاون والتنسيق الكاملين مع مجتمع الـ CSIRT الدولي (FIRST).
4. إنشاء نظام معلوماتي للكشف عن الحوادث والتهديدات التي يمكن أن تؤثر على أمن أنظمة معلومات الدولة وتقوم بعمل التنسيق اللازم والتدخل استجابةً لمثل هذه الحوادث والتهديدات.
5. تنظيم دورات تدريبية وورش عمل عند الاقتضاء حول الأمن السيبراني، كما وتقوم بحملات توعية للمؤسسات الحكومية وموظفيها وكافة الجهات ومؤسسات الخاصة المهتمة بمجال أنظمة المعلومات والأمن السيبراني والدفاع السيبراني.
6. مساعدة وتوجيه الإدارات والمؤسسات العامة ومؤسسات القطاع الخاص على وضع حيز التّطبيق أنظمة معلوماتية آمنة يكون بإمكانها مقاومة الهجمات السيبرانية. كما وتهتم الوكالة بنشر تقييم مفصل عن التهديدات المستجدة وتطرح التوصيات المناسبة بشأنها للقطاعين العام والخاص وللمواطنين.
7. تطبيق معايير الأمن السيبراني المناسبة والتأكد من اعتمادها في جميع المؤسسات الحكومية.
8. توفير كافة المعلومات الاستقصائية والمحدثة المتعلقة بالتهديدات السيبرانية الإجرامية وذلك بالاستناد الى قاعدة بيانات تكون متوفرة لكافة الشركاء، بما يسمح لهم بالتفاعل بشكل فعّال مع هذه المعلومات والدفاع بشكل أفضل عن انفسهم.
9. تحديد المعايير والممارسات ونصائح السلامة المتعلقة بالحوادث التي تمّ تشخيصها أو تلك التي تبلغت بها في مجال الأمن السيبراني.

10. التعاون مع كافة المشغلين المعنيين، بخاصة منهم مشغلي البنى التحتية ذات الأهمية الحيوية، وذلك من اجل تحديد وتوصيف كافة التهديدات والهجمات السيبرانية.

11. حماية الأصول الرقمية والمعلومات الحكومية السرية أو تلك المصنفة حساسة للغاية من خطر الهجمات السيبرانية.

12. تحضير وتنفيذ تدريبات واجراء مناورات حول طرق إدارة الأزمات والتهديدات السيبرانية، على أن تجري هذه التدريبات والمناورات على المستوى الوطني وعلى أن تشمل تدريجياً البلد بأكمله وكافة القطاعات والنشاطات ذات الأهمية الحيوية للبلد.

13. يجب على كافة الجهات المولجة تطبيق القانون وكذلك على الوزارات / الإدارات العامة وعلى كافة المؤسسات المعنية، وبالتعاون مع الوكالة الوطنية للأمن السيبراني، متابعة العمل الحثيث لبناء قدراتها التشغيلية اللازمة التي تمكنها من القيام بالدفاع السيبراني الفعال والتعامل مع الجرائم السيبرانية الكبرى عند الحاجة.

5.2 الوكالة والعامّة: من الأفراد الى الشركات

تقوم الوكالة بتقديم سبل الدعم والتوصيات عالية الجودة للمواطنين والشركات في كل ما يتعلق بالتهديدات السيبرانية. من اجل تحقيق هذا الهدف، ستعمد الوكالة الى وضع قاعدة بيانات يمكن الوصول إليها بسهولة تحوي المعلومات حول نظم الحماية السيبرانية، كما وستقوم بحملات توعية تهدف إلى رفع مستوى الوعي لدى عامة الجمهور حول التهديدات السيبرانية.

وكجزء من دورها اتجاه العامة، يجب على الوكالة أن:

- تتخذ التدابير اللازمة والفعالة للدفاع عن أجهزة وأنظمة معلومات المواطنين اللبنانيين ضد التهديدات المعروفة والمستجدة وذلك من خلال إنشاء منصة تسمح للمواطنين / الجهات والمؤسسات بإبلاغ الوكالة عن اية تهديدات سيبرانية أو اختراقات يواجهونها.
- تتولى، في سبيل خلق ثقافة وقائية مناسبة، وضع التوصيات اللازمة كما واقتراح الحلول التقنية المختصة ووضع برامج التدريب المناسبة التي تهدف إلى حماية وضمان امن النطاق الرقمي، ويشمل ذلك اجراء التدريبات والمناورات الوطنية والدولية والتي يمكن لجميع المؤسسات والشركات وعامة الناس المشاركة فيها والاطلاع عليها بهدف تحسين الاستعداد الشامل لحماية الفضاء السيبراني.
- تشارك في توجيه البحوث الأكاديمية والدراسات وتطوير البرمجيات والأجهزة والتقنيات المتعلقة بأمن أنظمة المعلومات.

5.3 دور الوكالة في تأهيل واختيار ومراقبة المنتجات

وفي سبيل ضمان جودة المنتجات والخدمات الرقمية، تقوم الوكالة بالمهام التالية:

- ضمان المراقبة النشطة لتقنيات الأمان الرقمية المستخدمة من قبل حكومة البلد والشركات والمواطنين.
- المساعدة في تأهيل ومراقبة منتجات وخدمات الأمن السيبراني ودعم تطوير أصول أمان ومنتجات أمنية رقمية جديدة تعكس أحدث الاتجاهات والتغيرات في أنماط الاستخدام.

- المساهمة في تعزيز نشر تقنيات محلية وخلق المعرفة والدراية الوطنية في صناعة أمن نظم المعلومات والخدمات المتعلقة بها، وذلك من خلال تطوير إطار يسمح بمساعدة المنتج الوطني على التأهل ليكون على المستوى المطلوب وإصدار شهادات الموائمة له بما يتماشى مع أهداف الحكومة وتأمين سيادة الدولة وكفايتها في هذا المجال.

5.4 الوكالة في مواجهة التهديدات السيبرانية

تلعب الوكالة دوراً أساسياً في تحليل وادارة المخاطر السيبرانية في كل ما يتعلق باعتماد التكنولوجيات الجديدة وفي كل ما يستجد من تقنيات في عالم التحول الرقمي. وبالتالي تكون الوكالة هي المسؤولة عن:

- انشاء إدارة مختصة بحوادث الأمن السيبراني الوطني تعمل على وضع خريطة نظم المعلوماتية الوطنية الاكثر حيوية، كما وتقوم بتحليل التهديدات السيبرانية، والكشف عنها وفهمها.
- متابعة التحديثات التكنولوجية وتوقع التغييرات التي تطرأ وتقترح الابتكارات اللازمة في أمن نظم المعلومات.
- إجراء عمليات تدقيق على الأنظمة المعلوماتية الخدماتية وجمع المعلومات التقنية بغرض وحيد هو إدارة حوادث الأمن السيبراني التي تؤثر على عمل هذه الأنظمة.
- تعزيز مكافحة الإرهاب السيبراني والجرائم السيبرانية المنظمة وذلك عبر تعزيز ودعم الجهات المسؤولة عن تطبيق القانون في عملية مكافحة الإرهاب والجريمة السيبرانية المنظمة وذلك من خلال العمل على تحسين الوسائل لمواجهة الحالات التالية:
  - مواجهة الجهات الأجنبية السيبرانية المعادية؛
  - منع الإرهاب السيبراني؛
  - مواجهة الفكر والسلوك الراديكالي المحلي المتطرف عبر وسائل الفضاء السيبراني.

5.5 الوكالة وحماية "المشغلين ذوي الأهمية الحيوية"

يعرف المشغل ذي الأهمية الحيوية أو البنية التحتية الحيوية على أنه أي كيان عام أو خاص يتولى ويدير البيانات ذات الطابع الحساس أو الخدمات القطاعية الهامة، مثلاً على سبيل المثال لا الحصر، مشغلو البنية التحتية للاتصالات، قطاع الطاقة، البنية التحتية الصحية، منصات البيانات الشخصية الوطنية، إلخ...

أما دور الوكالة في حماية المشغلين ذي الأهمية الحيوية، فيتمثل بالإجراءات التالية:

- تعزيز وسائل الحماية لدى المشغلين المصنفين كمشغلين حيويين أو اساسيين، لا سيما العاملين منهم في مجالات خدمات التواصل الإلكتروني وفي مجال تزويد خدمات الكهرباء والطاقة، بالإضافة إلى شركات الخدمات الرقمية، وذلك من خلال اعتماد متطلبات قوية لانظمة وقواعد أمن السلامة السيبرانية.
- تشجيع مشغلي خدمات التواصل السيبراني ومضيفي خدمات الويب على اعتماد أنظمة مختصة داخل شبكاتهم تمكنهم من الكشف المبكر على الهجمات السيبرانية التي تستهدف المشتركين فيها (باستخدام مجسات، مستشعرات، ادوات تحليل سلوك ... إلخ).

- توفير أدوات وأنظمة مستقلة مهمتها تحليل المخاطر لتقييم مستوى الأمان ودرجة موثوقية الأمن السيبراني في المنتجات والخدمات الرقمية المستخدمة من قبل الصناعات ذات الأهمية الحيوية.

أما في حال كانت المنتجات والخدمات الرقمية مخصصة لتخزين البيانات الشخصية أو كانت مخصصة للصناعات ذات الأهمية الحيوية، عندها تقوم الوكالة بتقديم المساعدة اللازمة في إجراء تحليل للمخاطر وفي تأمين أفضل الطرق المعتمدة في الحماية السيبرانية.

كما ستساهم الوكالة أيضًا في إنشاء آليات تقييم مستقل لمستوى الأمان والموثوقية لهذه المنتجات والخدمات، ولتزويد مستخدميها المحتملين بالحمايات المناسبة من خلال وضع ملصقات مختصة. في سبيل تحقيق هذا الهدف، ستقوم الوكالة بما يلي:

- تحديد أفضل الممارسات والآليات المتبعة لتعزيز البنى التحتية الوطنية الرئيسية / الحيوية وحمايتها ضد الهجمات السيبرانية. ان الوكالة وبالتعاون مع الإدارات اللامركزية والسلطات المسؤولة الأخرى، ستساعد المنظمات والمؤسسات الوطنية على اتخاذ كافة التدابير اللازمة التي تبقي هذه البنى آمنة أو تلك التي تؤمن لها درجة كافية من المقاومة والمرونة ضد الهجمات السيبرانية.

- ضمان أن تكون البنى التحتية الوطنية الحيوية، العامة منها والخاصة، على دراية تامة بمستوى التهديدات التي تواجهها وعلى ان تكون قادرة على تنفيذ تدابير مكافحة الجرائم السيبرانية المناسبة. من هنا يجب تعي كافة المؤسسات العامة والشركات والمؤسسات الخاصة المستوى الحقيقي للتهديد السيبراني للبنى التحتية لديها وأن تضع تدابير كفيلة بالمساهمة بحماية المصلحة والسيادة السيبرانية الوطنية والحفاظ عليها.

- مساعدة الشركات التي تملك أو تدير بيانات حساسة على إدارة مخاطرها وتغطية نقاط الضعف الخاصة بها.

5.6 الإطار المعياري للوكالة داخل نظامها البيئي

بما أن بناء الإطار القانوني يتطلب هيئات مختصة ذات خبرة عالية، فسيتم بناء الإطار المعياري للوكالة بمساعدة وتعاون دولي قوي ومنتظم يحترم سيادة لبنان ودستوره. يشمل النظام البيئي للوكالة شركاء محليين رئيسيين، مثل الحكومة بشكل عام ووزارة الاتصالات ومشغليها وهيئة أوجيرو وكافة الجهات المولجة تطبيق القانون والوزارات المستفيدة، ومكتب وزير الدولة لشؤون التنمية الادارية، والمؤسسات الأكاديمية ومقدمي خدمات الإنترنت في لبنان والجمعيات المهنية. كما وسيقوم الشركاء الدوليون المدرجون في ورقة الاستراتيجية الوطنية بدعم هذا النظام البيئي.

ولضمان وجود إطار قانوني مناسب للأمن السيبراني، يجب أن تنفذ الوكالة الخطوات التالية:

- خلق واعتماد إطار تنظيمي يحكم التقنيات الناشئة الجديدة: من اجل ذلك، ستقوم الوكالة بإبلاغ الوزارات والمؤسسات الحكومية والسلطات المحلية والشركات والمواطنين وبانتظام بكل ما يتعلق بالتهديدات التي تواجه الأنظمة الرقمية من خلال قنوات الاتصال المخصصة لكل منهم.

- إعداد البيئة القانونية المناسبة لاستيعاب المنتجات والخدمات الرقمية الجديدة.

- تطوير إرشادات الدفاع السيبراني وتنفيذ تدابير بهدف تحسين مستويات الأمن السيبراني بشكل كبير عبر شبكات الكمبيوتر.
- وضع وإصدار التراخيص اللازمة لكافة الأجهزة والآليات الأمنية المصممة لحماية امن الشبكات وأنظمة المعلومات، التي تحتوي على معلومات مصنفة بأنها سريّة وحيوية للدفاع الوطني.
- المشاركة في المفاوضات الدولية والتواصل مع النظراء الأجانب.
- تحديد وتقييم درجة الأمان في الأجهزة والخدمات المقدمة من قبل مقدمي الخدمات، والضرورية لحماية أنظمة المعلومات والبنى التحتية.
- تحديد إطار الأمن السيبراني اللازم للتوقيعات الإلكترونية المؤهلة قانونًا.
- إعداد اطر الاعتماد والشهادات المتعلق بالأمن السيبراني والتوقيعات الإلكترونية والسجلات / الآثار / البراهين الرقمية الملزمة قانونًا.
- التقرير بشأن المختبرات المعترف بها والتي بإمكانها ان تجري تقييمات أمنية رقمية وتعطي شهادات لمنتجات حماية أنظمة تكنولوجيا المعلومات (هذه الأطر القانونية غير معتمدة حاليًا في لبنان).
- وضع أطر للاعتماد والشهادات والمعايير التقنية المتعلقة بأنظمة الأمن السيبراني بما يتماشى مع القوانين والانظمة الحالية. يتم تحديد هذا الإطار بالتعاون مع الوزارات المعنية والجهات المكلفة تطبيق القانون والمؤسسات الحكومية، كلٌّ في دائرة اختصاصها .

الخاتمة

في الختام نشير الى انه هناك افتراضات نهائية وحاسمة واستراتيجية يجب إبرازها والاضاءة عليها من اجل حسن تطبيق الاستراتيجية الوطنية للأمن السيبراني في لبنان:

- ان هذه الوثيقة تدعو اولاً، وبصورة عاجلة، إلى اتخاذ إجراء تطبيقي هام وحساس لحسن تنفيذ هذه الاستراتيجية، الا وهو الإنشاء الرسمي للوكالة الوطنية للأمن السيبراني ونظم المعلومات لانه من دونها، لا يمكن متابعة أو تنفيذ أي من بنود هذه الاستراتيجية؛
- ان الوكالة الوطنية للأمن السيبراني تحتاج إلى التزام قوي من الحكومة، مما سيمكنها من بدء إجراءات متعددة، مثل التخطيط التشغيلي المفصل، الجدولة الزمنية، وتحديد الموازنة اللازمة؛
- ان الوكالة تحتاج إلى التزام رسمي حازم بميزانية تشغيلية، لأنه من دونها، لا يمكن تحقيق أي شيء. وفي حين أنه من المستحيل تحديد ميزانية دقيقة لها في هذه المرحلة المبكرة للغاية، يمكن بالتأكيد تحديد نطاقات الميزانية بصورة تقريبية بناءً على خطة العمل الموافق عليها؛
- أنه بعد المصادقة على الاستراتيجية، سيكون للفريق الوطني الذي عمل على وضعها ولاية جديدة لدعم الحكومة في المرحلة التأسيسية، ولكن بتفويض جديد وشركاء محددين بوضوح للمساعدة في تنفيذ الاستراتيجية؛
- انه إذا لم يتم تنفيذ الخطوات المذكورة في الإستراتيجية الوطنية اللبنانية للأمن السيبراني أعلاه، فسوف يواجه البلد المخاطر التالية:
  - سيظل لبنان مدرجًا كواحد من أكثر البلدان تخلفًا في العالم، وفقًا لمؤشر الأمن السيبراني للدول الذي يصدره الاتحاد الدولي للإتصالات والذي يقيّم قدرة أي بلد على التعامل مع احتياجات الأمن السيبراني في القرن الحادي والعشرين خاصة في ظل الحرب العالمية التي تخاض ضد تهديدات الجريمة السيبرانية وحرب المعلومات والإرهاب الإلكتروني؛
  - ستتعرض جميع الأصول الحكومية والأسواق وقطاعات الأعمال التجارية والمواطنين في لبنان بشكل اكيد وبشدة وخطورة كبيرين للتهديد السيبراني. وسيتكبد لبنان الخسائر الاقتصادية، وسيعيش في الخوف وعدم اليقين وتحكمه الشكوك في التعامل مع التحول الرقمي العالمي الجاري، والذي لا يزال لبنان متأخرا جدا فيه؛
  - لن يكون لبنان قادراً على التطور وسيخسر المزيد من القدرات التنافسية على المستوى الدولي؛
  - أن ضعف الحماية من التهديدات والهجمات والجرائم السيبرانية سوف يجذب المزيد من مجرمي الفضاء السيبراني. وهذا بدوره سيزيد من استنزاف الثقة في البلاد. وبذلك قد يخسر لبنان كثيراً من الاستثمارات الأجنبية، خاصة في مجال صناعات وخدمات تكنولوجيا المعلومات والاتصالات، على الرغم من الحوافز الاقتصادية المشجعة وتمكين الأعمال التجارية، التي وضعتها الحكومة اللبنانية خلال السنوات الماضية ؛

- ان لبنان موطن لعدد كبير من اللاجئين المسجلين وغير المسجلين، والعمال الأجانب الشرعيين وغير الشرعيين، وما إلى ذلك. هذه المجتمعات هي على اتصال مباشر أو غير مباشر، عن علم أو بدون علم، مع عدد لا يحصى من المنظمات والجهات والمؤسسات (بينهم عدد كبير من المنظمات غير الحكومية) سواء على الأراضي اللبنانية أو في بلدانهم الأصلية. هؤلاء الأفراد والجماعات إما انهم يخضعون لإشراف ضعيف للغاية أو إنهم لا يخضعون للإشراف على الإطلاق من قبل الحكومة اللبنانية، وبالتالي يمكن أن يكونوا غير محصنين ضد التهديدات السيبرانية المحتملة كما ويمكن أن يصبحوا هم أنفسهم وبسهولة منصة للتهديدات السيبرانية المحتملة وغيرها من الأعمال الإجرامية السيبرانية، والتي قد تضع لبنان تحت مخاطر محتملة متزايدة من نوع الجريمة المنظمة؛
- لقد ساهم كل ما سبق ذكره في تغذية التصور المستمر للبنان على انه دولة "متخلفة في مجال الامن السيبراني."

وأخيراً، فانه لا يمكننا أن نحمي لبنان ومؤسساته العامة وقطاعه الخاص ومواطنيه من التهديدات المذكورة فيما سبق، إلا عبر استراتيجية وطنية قوية ومتماسكة وشاملة ومؤسسية وتعاونية للأمن السيبراني تستند إلى معالجة أركان الأمن السيبراني المحددة، بطريقة منهجية، وعلى مستوى الوطن، وضمن خطة عمل شاملة ومتطورة.

لائحة المختصرات

المختصر	العبارة الكاملة
APT	Advanced Persistent Threat
BYOD	Bring Your Own Device
CCB	Cyber Crime Bureau
CEPOL	European Union Agency for Law Enforcement Training / Collège européen de police
CERT	Computer Emergency Response Team
CTI	Cyber Threat Intelligence
DoS	Denial Of Service
EBIOS	Expression des Besoins et Identification des Objectifs de Sécurité / Expression of Needs and Identification of Security Objectives
ENA Liban	Ecole Nationale d'Administration Libanaise / Public National Administration School of Lebanon
EUROPOL	Agence européenne de police criminelle / European Union Agency for Law Enforcement Cooperation
ICP	Industrial Control Process
ICT	Information and Communication Technology
IIOT	Industrial Internet Of Things
INTERPOL	Organisation internationale de police criminelle / International Crime Police Organization
IOT	Internet Of Things
FSI/ISF	Internal Security Forces / Forces de Sécurité Intérieure
ITU	International Telecommunication Union
LEA	Law Enforcement Agency: Army, Internal Security Forces, General Security and State Security
KPI	Key Performance Indicator
NCISA	National Cyber Security and Information System Agency (of Lebanon)
NIST	National Institute of Standards and Technology
OGERO	Organisation pour la Gestion des Équipements de Radio Orient Entreprise libanaise de télécommunications / Lebanese telecommunications company
OIV/CI	Opérateur d'Importance Vital/Critical Infrastructure
OMSAR	Office of the Minister of State for Administrative Reform
ONU	Organisation des Nations unies
SSH	Secure SHell
SSL	Secure Sockets Layer
UNICRI	United Nations Interregional Crime and justice Research Institute
UNODC	United Nations Office on Drugs and Crime
VPN	Virtual Private Network

قاموس المصطلحات

المصطلح عربي/فرنسي/انكليزي	الشرح
التهديد المستمّر المتقدم/ Menace persistante avancée/ Advanced Persistent Threat	هجوم إلكتروني مطوّل ومحدد الهدف يدخل خلاله شخص غير مصرح له إلى الشبكة ثم يرحل دون أن يلاحظه أحد ولفترة طويلة من الوقت. أما أهداف هجوم من هذا النوع فهي عموما تكون بهدف مراقبة نشاط الشبكة وسرقة البيانات بدلا من تقويض عمل الشبكة أو النظام المعلوماتي.
الروبوتات/ Botnet	الروبوتات (أو شبكة من آلات الزومبي) هي عبارة عن مجموعة من أجهزة الكمبيوتر المتصلة بالإنترنت والتي، دون علم أصحابها، قد تم برمجتها لنقل المعلومات بما في ذلك البريد المزعج أو (الفيروسات) لأجهزة كمبيوتر أخرى متصلة بالإنترنت. ويطلق على واحد من أجهزة الكمبيوتر هذه "الزومبي" أو "جهاز تتبع - Bot"، وتخدم عادة مصالح مؤلف البريد المزعج أو الفيروس.
أحضر جهازك الخاص/ Prenez vos Appareils Personnels (PAP)/ Bring Your Own Device (BYOD)	هي ممارسة لاستخدام المرء المعدات الشخصية (الهاتف الذكي، الكمبيوتر المحمول، الكمبيوتر اللوحي، الخ) في السياق المهني لعمله.
الفريق الوطني للاستجابة لطوارئ أو لحوادث الحاسب الآلي/ Computer Emergency Response Team (CERT) or Computer Security Incident Response Team (CSIRT)	هو مركز متخصص للتنبيه والاستجابة لهجمات الكمبيوتر، ومخصص عادة لحماية الشركات أو الإدارات، ولكن معلوماته تكون متاحة عموماً للجميع.
الحوسبة السحابية/ Cloud Computing	هو عبارة عن استغلال لطاقة الحوسبة أو التخزين لخوادم الكمبيوتر عن بعد عبر شبكة، وعادة ما تكون هي الإنترنت. ويتم استئجار الخوادم عند الطلب، وغالبًا عن طريق استخدام اجزاء من خدماته، وفقًا للمعايير الفنية (الطاقة، عرض النطاق الترددي، إلخ)، ولكن أيضًا بالسعر المحدد سلفاً. تتميز الحوسبة السحابية بمرونتها الكبيرة: بناءً على مستوى مهارة المستخدم العميل، يمكنه مثلاً من إدارة الخادم الخاص به كلياً أو ببساطة استخدام بعض التطبيقات التي فيه عن بعد كما في وضع الـSaaS.
الشبكة السحابية/ Cloud Network	هي عبارة عن شبكة كمبيوتر داخل بنية تحتية سحابية توفر الاتصال بالتطبيقات والخوادم المستندة إلى الخدمات السحابية.
الخدمات السحابية/ Cloud Services	هي خدمة متاحة للمستخدمين عند الطلب عبر الإنترنت من خوادم توفر تقنية المعلومات السحابية وليس من الخوادم المحلية للمؤسسة التي يعملون بها.
الحادث السيبراني/ Cyberincident	محاولة غير مصرح بها، سواء كانت ناجحة أم لا، للوصول إلى شبكة أو نظام كمبيوتر أو محاولة تعديل عمله أو إتلافه أو حذفه أو جعله غير متوفر للخدمة.
النشاط السيبراني الضارّ/ Cyberactivité malveillante/ Malicious cyber activity	هو نشاط غير مسموح به أو غير قانوني، يسعى إلى المساس بسرية أو سلامة أو توفر أجهزة الكمبيوتر أو نظم المعلومات أو الاتصالات أو الشبكات أو البنى التحتية الافتراضية التي تدار بواسطة أجهزة الكمبيوتر أو أنظمة المعلومات، والمعلومات التي تحتويها.
هجوم سيبراني/ Cyberattaque/ Cyberattack	هو عمل ضار ضد جهاز كمبيوتر أو نظام معلوماتي أو خدمات رقمية عبر شبكة سيبرانية (الكترونية)

المصطلح عربي/فرنسي/انكليزي	الشرح
جريمة سيبرانية/ Cybercrime	هي "جريمة جنائية يُحتمل أن تُرتكب على نظام كمبيوتر متصل بشبكة أو من خلاله" وتعد شكلًا جديدًا من أشكال الجريمة والانحراف تختلف عن الأشكال التقليدية من حيث أنها تقع في الفضاء الافتراضي، "الفضاء الإلكتروني". في السنوات الأخيرة، كان إضفاء الطابع الديمقراطي في حرية الوصول إلى أجهزة الكمبيوتر وعولمة الشبكات من العوامل التي ساهمت في تطور الجريمة السيبرانية.
تجسس سيبراني/ /Cyberespionnage Cyberspying	هو التجسس عبر استخدام الانترنت.
نظافة سيبرانية/ Cyberhygiene	هي وسيلة لضمان الحماية والصيانة الكافية للأجهزة الطرفية والأنظمة الحاسوبية، ولتطبيق أفضل الممارسات في مجال الأمن السيبراني.
حماية سيبرانية/ /Cybersécurité Cybersecurity	هي عبارة عن مصطلح جديد يشير الى دور جميع القوانين والسياسات والأدوات والأجهزة والمفاهيم والآليات الأمنية وطرق إدارة المخاطر والإجراءات والتدريب وأفضل الممارسات والتقنيات التي يمكن استخدامها لحماية الأفراد والأصول الحاسوبية الملموسة وغير الملموسة (المتصلة بشكل مباشر أو غير مباشر بشبكة معلوماتية) للأفراد والدول والمؤسسات.
"الجنوب السيبراني"/ /CyberSud CyberSouth	هو مشروع مشترك بين الاتحاد الأوروبي (أداة الجوار الأوروبية) ومجلس أوروبا. الغرض منه هو المساعدة في تعزيز التشريعات والقدرات المؤسسية والأدلة الرقمية لمكافحة جرائم الإنترنت في منطقة الجوار الجنوبي لاوروبا، مع احترام حقوق الإنسان وسيادة القانون. البلدان ذات الأولوية: الجزائر، الأردن، لبنان، المغرب وتونس.
الفضاء السيبراني/ /Cyberespace Cyberspace	"مجموعة البيانات الرقمية التي تشكل عالم من المعلومات ومن وسائل الاتصال، المتصلة بدورها بالترابط العالمي لأجهزة الكمبيوتر والمعلوماتية".
تهديد سيبراني/ /Cybermenace Cyberthreat	هو أي ظرف أو حدث محتمل قد يؤثر سلبًا على شبكات وأنظمة المعلومات ومستخدميها والأفراد المعرضين لها.
حرب سيبرانية/ /Cyberguerre Cyber war	هو استخدام أجهزة الكمبيوتر والإنترنت لشن الحرب على الفضاء السيبراني لاحدى الجهات أو الدول أو على مجوعة منها.
ارهابي سيبراني/ /Cyberterrorist Cyberpunk	مبرمج يقتحم أنظمة الكمبيوتر بغرض سرقة أو تغيير أو تدمير المعلومات كشكل من أشكال الإرهاب الإلكتروني.
هجوم حجب الخدمة/ Attaque par déni de /service Denial of Service Attack /(DoS) Distributed Denial Of Service attack (DDoS)	هو هجوم على الكمبيوتر لجعل الخدمة عبره غير متاحة، لمنع المستخدمين الشرعيين للخدمة من استخدامها. في الوقت الحالي، أتتي الغالبية العظمى من هذه الهجمات من مصادر متعددة، (لذلك يطلق عليه هجوم الحرمان من الخدمة الموزع DdoS– أنواعه:). - هجوم فيضاني لاغراق شبكة معلوماتية بهدف تعطيلها؛ - هجوم لقطع الاتصالات بين جهازين، مما يمنع الوصول إلى خدمة معينة؛ - عرقلة وصول شخص معين إلى خدمة ما؛ - -أيضا إرسال مليارات البايت إلى نطاق إنترنت معين.

المصطلح عربي/فرنسي/انكليزي	الشرح
التحول الرقمي/ Digital Transformation	هو استخدام التكنولوجيا الرقمية لحل المشاكل التقليدية. وتحمل هذه الحلول الرقمية في طياتها حلولاً جديدة مبدعة ومبتكرة عوضاً عن مجرد دعم وتحسين طرق العمل التقليدية. بمعنى ادق، تشير عبارة "التحول الرقمي" إلى مفهوم "الانتقال الى بيئة عمل خالية من التعامل الورقي" كما وتشير الى الوصول إلى حالة من "نضج الأعمال الرقمية" وما يستتبعه ذلك من تأثير على الأعمال الفردية وكذلك على عمل شرائح مجتمعية كاملة، كالحكومة ووسائل التواصل الجماهيري والفن والطب والعلوم.
عبارة مختصرة تعني "التعبير عن الاحتياجات وتحديد الأهداف الأمنية"/ EBIOS	هي طريقة لتحليل وتقييم واتخاذ الإجراءات لمواجهة االمخاطر في نظم المعلومات في مؤسسة ما ويكون من نتائجها الوصول الى سياسة مناسبة تلبي الاحتياجات الأمنية لهذه المؤسسة. تم إنشاء هذه الطريقة في العام 1995 من قبل الوكالة الوطنية لأمن نظم المعلومات في فرنسا، وهي دائرة تابعة لرئيس الوزراء الفرنسي.
الخدمات الرقمية/ e-services	هي الخدمات التي تقدم باستخدام وسائل تكنولوجيا المعلومات والاتصالات. ان المكونات الثلاثة الرئيسية التي يتألف منها نظام الخدمات الرقمية هي: الطرف المزود الخدمة والطرف المستقبل للخدمة وقنوات تقديم الخدمة.
الاستغلال/ Exploit	عبارة عن برنامج ضارّ يستفيد من ثغرة عدم وجود الحصانة الكافية للتسبب في حدوث سلوك ضار أو غير مرغوب به على أنظمة وبرامج االحاسوب المستهدف.
الاختراق/ Hack	هو الإجراء الذي تتم من خلاله عملية الاختراق دون ترخيص إلى شبكة سلكية أو لاسلكية. لكن هذا المصطلح ياخذ معناه كاملاً في الشبكات اللاسلكية ويرجع الفضل في ذلك إلى الطابع المفتوح لهذه الشبكات، حيث يمكن لأي كان اعتراض اشارتها التي تبث عبر الأثير. لكن المبدأ هو نفسه بالنسبة للهجوم والقرصنة على أحد مواقع الإنترنت: الا وهو الوصول إلى مجال عمل خاص دون ترخيص، بحيث تكون هناك قدرة على تعديل أي محتوى داخله عند الرغبة بذلك.
الهاكر/ /Hackeur Hacker	هو متخصص في تكنولوجيا المعلومات يستخدم معرفته بأمن الكمبيوتر للبحث عن نقاط الضعف فيه واستغلالها.
القرصنة/ Hacking	إنها ممارسة تهدف إلى تبادل "سري" للمعلومات غير القانونية أو الشخصية. تظهر هذه الممارسة، التي أنشأها المتسللون أو المخترقون، بدأت مع بداية ظهور أجهزة الكمبيوتر المنزلية الأولى ويمكن أيضًا تعريف القرصنة على أنها مجموعة من التقنيات لاستغلال نقاط الضعف لعنصر أو مجموعة من العناصر المادية أو البشرية.
ناشط مخترق/ Hacktivist	الناشطون المخترقون" هم القراصنة الذين يسعون للتعبير عن افكارهم وعقائدهم وميولهم وانتمائاتهم عن طريق القرصنة وهجمات الكمبيوتر.
هندسة اجتماعية/ /Ingénierie sociale Social engineering	هي عبارة عن ممارسة للتلاعب النفسي لأغراض الاحتيال. تستغل ممارسات الهندسة الاجتماعية نقاط الضعف النفسية والاجتماعية على نطاق واسع للأفراد أو المنظمات للحصول على مكاسب عن طريق الاحتيال (سلعة أو خدمة أو تحويل مصرفي أو وصول فعلي أو عبر كمبيوتر، والكشف عن معلومات سرية، وما إلى ذلك). ويتم ذلك عادة باستخدام المهاجم لمعرفته، أو جاذبيته، أو إحساسه بالتفوق أو بالهيمنة، وحيث يسعى المهاجم إلى استخدام نقاط ضعف الهدف كالجهل واستغلال الصداقة للاساءة اليه والحصول على ما يريد.
تهديد/ /Menace Threat	هو سبب محتمل لوقوع حادث، والذي يمكن أن يؤدي إلى تلف في النظام أو المؤسسة.
تهديد داخلي/ /Menace interne Internal threat	حين يصدر التهديد الضار من عنصر من عناصر المؤسسة ذاتها، مثل الموظفين أو الموظفين السابقين أو المقاولين العاملين في الداخل أو الشركاء التجاريين الذين لديهم معلومات حول ممارسات الأمان والبيانات وأنظمة تكنولوجيا المعلومات الخاصة بالمؤسسة.أو بالشركة.

المصطلح عربي/فرنسي/انكليزي	الشرح
عالم افتراضي/ Monde virtuel/ Virtual world	هو عالم تم إنشاؤه بشكل مصطنع بواسطة برامج الكمبيوتر ويمكنه استضافة مجتمع من المستخدمين المتواجدين فيه مع القدرة على التحرك والتفاعل معه. يمكن تمثيل هذا العالم وسكانه في بعدين أو ثلاثة أبعاد. يمكن لهذا العالم أن يحاكي العالم الحقيقي، بقوانينه الفيزيائية، مثل الجاذبية أو الطقس أو المناخ أو الجغرافيا أو على العكس، يمكن أن يكون عالم يحكمه الآخرون. ويمكن أيضًا استنساخ القوانين الإنسانية فيه. وغالباً ما يكون التواصل بين المستخدمين في بينهم فيه على شكل نص أو عبر الصوت والصورة.
برامج انتزاع الفدية/ Rançongiciel/ Ransomware	هو برنامج كمبيوتر ضار، يأخذ البيانات المخزنة كرهينة. يقوم البرنامج بتشفير الملفات الموجودة على جهاز الكمبيوتر الخاص بك ويحظر وصولك اليها ويطلب المهاجم الفدية في مقابل الحصول على مفتاح لفك تشفيرها.
المرونة أو القدرة على الصمود/ Résilience/ Resilience	هي قدرة النظام أو بنية الشبكة على متابعة العمل في حالة التعرض لهجوم أو لعطل فيها.
نظام حساس أو حرج/ Système critique/ Critical system	هو نظام يمكن أن يؤدي انهياره إلى عواقب وخيمة، مثل التسبب بالوفاة أو الإصابة الخطيرة أو الحاق أضرار مادية كبيرة أو عواقب وخيمة على البيئة التي يشرف عليها. ويشمل مصطلح نظام حرج اليوم كل عناصر النظام الذي يسمح، اليوم أكثر فأكثر، بعمليات التحكم في الكمبيوتر، حتى لو كانت أيضاً عناصر ميكانيكية أو بشرية.
المتطفلون على البرمجيات الخبيثة أو المخترقون المبتدئون أو "أطفال النصوص"/ Script Kiddies	هو مصطلح ازدرائي من أصل إنكليزي يقصد به وصف المبتدئين، الذين يفتقرون إلى المهارات الأساسية في مجال أمن تكنولوجيا المعلومات، والذين يقضون معظم وقتهم في محاولة التسلل إلى الأنظمة، باستخدام البرامج النصية أو البرامج التي تم تطويرها من قبل الآخرين. وعلى الرغم من انخفاض مستوى التأهيل أو حتى انعدامه، فإن "أطفال النصوص" يشكلون أحيانًا تهديدًا حقيقيًا لأمان انظمة المعلومات: في الواقع، فإلى جانب حقيقة أن بعضهم يلحق الأضرار من دون أن يدري ماذا يفعل، فان بعضهم الآخر، وهم كثر، عنيدون إلى درجة انهم قد يقضون أحيانًا عدة أيام لتجربة كل المجموعات الممكنة من كلمات المرور، مع احتمال تمكنهم من ذلك، لكن في اعلب الأحيان أيضاً يكونون هم من يصاب بالبرنامج الضار الذي يستخدمه.
بروتوكول القشرة الآمنة/ Secure SHell (SSH)	هو عبارة عن برنامج كمبيوتر وبروتوكول اتصال آمن في نفس الوقت. حيث يقوم بروتوكول الاتصال بطلب تبادل مفاتيح التشفير في بداية الاتصال. وبعدها، تتم مصادقة وتشفير جميع أجزاء بروتوكول التحكم بالنقل (TCP).
بروتوكول طبقة المنافذ الآمنة/ Secure Sockets Layer (SSL)	هي مجموعة بروتوكولات لتأمين التبادلات الآمنة على الإنترنت. تم تطوير SSL في الأصل بواسطة شركة Netscape ثم واصلت الـ IETF تطويرها من خلال إعادة تسميتها "أمان طبقة النقل"(TLS) لذلك نتحدث أحيانًا عن SSL / TLS للإشارة إلى SSL أو TLS.
ابتزاز جنسي/ Sextorsion	هي جريمة تعتمد على القيام بالابتزاز عبر الإنترنت من اجل الحصول على خدمات جنسية أو مكاسب مالية. وغالبًا ما يتم ذلك الى الابتزاز عبر اساءة استخدام آلة التصوير الرقمية أو كاميرا الويب.

المصطلح عربي/فرنسي/انكليزي	الشرح
العمل عن بعد/ Télétravail/ Teleworking	تعني منظومة عمل معينة، وهي عبارة عن ممارسة نشاط مهني، كلياً أو جزئياً عن بعد (أي خارج المكان الذي تكون نتيجة العمل فيه، وعادة يكون مقر صاحب العمل) من خلال استخدام تقنيات المعلومات والاتصالات (الإنترنت والهاتف المحمول والفاكس وغيرها). ويمكن أن يتم العمل عن بعد من المنزل أو من مركز اتصالات أو مكتب عبر الأقمار الصناعية أو أي مكان آخر (أماكن عمل مختلفة حسب النشاط الذي يتعين القيام به)، وهو يقع عادة في سياق العمل المدفوع الأجر، ولكن أيضًا يمكن أن يتم عبر استخدام المساحات المشتركة (العمل المشترك Coworking)، في سياق العمل عن بُعد المستقل. هذا وقد تم تشجيع "العمل عن بعد" من خلال انتشار العولمة الاقتصادية.
الأنظمة غير المصححة أو غير المحمية/ Systèmes non corrigés/ Unpatched Systems	الأنظمة غير المصححة هي برامج لا يتوفر لها إصلاح عاجل يصحح ثغرة أمنية أو يعدل نظامًا أو تطبيقًا أو برنامجًا آخر أو لم يتم تطبيق هذا الاصلاح عليها لسبب من الأسباب.
ثغرة أو هشاشة أو نقطة ضعف امنية/ Vulnérabilité/ Vulnerability	الثغرة الأمنية هي نقطة ضعف في نظام الكمبيوتر تسمح للمهاجمين بخرق امن وسلامة هذا النظام، وهذا يعني امكانية تغيير طريقة تشغيله الطبيعية أو الاطلاع على سرية أو سلامة البيانات التي يحتوي عليها. وهذه الثغرات الأمنية هي في العادة نتيجة لضعف في تصميم البرنامج أو في مكون من مكونات البرنامج أو، ولكن هذه غالبًا ما تكون عبارة عن شذوذ في البرامج ناتج عن أخطاء في البرمجة أو عن الممارسات السيئة. وعادة ما يتم تصحيح مثل هذه الأعطال فور اكتشافها، ولكن يمكن يبقى المستخدم عرضةً لهذا التهديد طالما لم يتم نشر وتثبيت الإصلاح المطلوب بالسرعة الممكنة. لهذا السبب من المهم الحرص على تحديث البرامج باستخدام تصحيحات مقدمة من بائعي البرامج.

الملاحق

LEBANESE REPUBLIC
President of the Council of Ministers

4/10/2018

No: 1637

H. E. Christina Lassen
Head of Delegation the European Commission
Charles Malek Avenue
Aschrafieh

Subject: National Cyber Security Strategy for Lebanon
Appointment of a National Focal point
Establishment of a National Commission
Project: **Cyber Crime initiative funded by the EU**

Dear Ambassador Lassen,

Reference is made to the initiatives conducted by the European Delegation and to the joint effort conducted by the Prime Minister the General Secretary of the High Council of Defense, and the EU delegation representative, and to our meeting of the 21st of Sept,

We believe, however that much work remains to be done, and that we must continue to collaborate with the various levels,

And due to the urgency of the matter, I would like to propose Dr. Lina OUEIDAT (National ICT Coordinator) to assume the responsibilities of the National Focal Point of the Commission.

Dr. Lina OUEIDAT supported the General Secretary of the High Council of Defense to issue the Roadmap for the Preparation of the "**National Cyber Security Strategy and the Fight against Cybercrime**", and she will be the **Rapporteur Member** of the National team composed of representatives of Ministries and concerned public and private agencies.

You will find joined to this letter:
- The Road Map for the establishment of a national Security Strategy
- The nomination of Dr. Lina Oueidat as an advisor and National ICT Coordinator
- The resolution of the National Cyber Security Strategy Team

Saad Hariri

REPUBLIQUE LIBANAISE
Présidence du Conseil des Ministres

No: 1638 4/10/2018

S.E. Christina Lassen
Chef de la Délégation Européenne au Liban
Avenue Charles Malek
Ain Najm

Sujet : préparation de la stratégie nationale de cyber sécurité et pour la lutte contre la cybercriminalité
Mission d'experts niveau décideurs
Project: EU Cyber Crime initiative

Chère Ambassadeur Lassen

En référence aux visites engagées par la Délégation Européenne et particulièrement aux dialogues engagés depuis Octobre 2017 avec le Secrétariat General de la Défense, et à la visite du Secrétaire General Hamad avec des hauts fonctionnaires en France en Avril 2018,

Nous avons le plaisir de vous informer que cette collaboration a conduit à l'élaboration par Dr.Lina OUEIDAT de la Feuille de route et à l'établissement de la Commission Nationale qui doit établir la Stratégie Nationale pour la Cyber Sécurité, et pour la lutte contre la cybercriminalité pour le Liban

Et en vue de l'élaboration du cadre stratégique de la future politique publique en matière de cyber sécurité, et continuation des efforts entrepris, nous soumettons la sollicitation du Haut Conseil de Défense auprès de la Commission Européenne pour organiser à Beyrouth dans une prochaine étape une mission d'expertise (niveau décideurs) d'un Etat membre de l'UE de préférence la France pour cette mission afin de permettre un échange avec les services du Premier Ministre et les parties prenantes des administrations concernées ,sur les enjeux d'un modèle organisationnel et d'une doctrine pouvant inspirer le Liban.

La préférence de la France plus particulièrement pour cette mission a pour objectif de poursuivre le dialogue déjà entrepris sur l'aspect organisationnel au sein de la Présidence du Conseil des ministres vu la similitude des lois cadres relatives aux institutions administratives des deux pays.

Il serait opportun de joindre cette mission d'expertise à la mission en cours de préparation avec Cyber South le 16 novembre 2018, sur la convention de Budapest au Grand Séral

Nous souhaitons également le support des services de l'ambassade de France pour aider à l'organisation de cette mission spécifique et nous vous serions gré de les informer par vos propres soins.

REPUBLIQUE LIBANAISE
Président du Conseil des Ministres

Vous trouvez ci-joint également la résolution de l'établissement du comite (no. 173/2018) et la nomination de Dr. Lina OUEIDAT Conseiller du Premier Ministre (no. 172/2018) qui est à votre disposition pour la coordination de tous ces efforts

Saad Hariri

cc : Mr. Bruno Foucher Ambassadeur de France à Beyrouth

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

DIRECTORATE GENERAL
HUMAN RIGHTS AND RULE OF LAW

INFORMATION SOCIETY - ACTION AGAINST CRIME DIRECTORATE

THE DIRECTOR

Ref ► DGI/JK/AS/VS/MAW/le195

Prime Minister of Lebanon
His Excellency Saad HARIRI
Grand Sérail
Rue des Capuchins
Beirut

Strasbourg, 26 October 2018

Dear Prime Minister,

The Council of Europe welcomes the intention of the Government of Lebanon to develop a National Cyber Security Strategy.

We are prepared to support this effort and suggest holding meetings on 15 and 16 November in Beirut.

The meeting on 15 November would permit the sharing of good practices between the National Commission of Lebanon responsible for the establishment of the cybersecurity strategy and international experts.

The meeting on 16 November would be aimed at discussing the benefits of the Budapest Convention on Cybercrime for Lebanon with members of the National Commission and representatives of other relevant Ministries.

Both events would be supported under the joint project CyberSouth of the Council of Europe and the European Union.

Should this proposal find your approval, I would suggest that your authorities contact Ms Marie AGHA-WEVELSIEP, project manager of CyberSouth (marie.agha-wevelsiep@coe.int, +40 21 201 78 09; + 40 744 673 826) for further information and practical arrangements.

Yours sincerely,

Jan Kleijssen

COUNCIL OF EUROPE
F-67075 Strasbourg Cedex
Tel ► +33 (0)3 88 41 21 10
Fax ► +33 (0)3 88 41 37 39
Mail ► jan.kleijssen@coe.int
Site ► www.coe.int/justice
www.coe.int

الجمهورية اللبنانية
رئاسة مجلس الوزراء

قرار رقم ١٧٢ / ٢٠١٨

تشكيل فريق وطني لوضع خطة لمواجهة مخاطر جرائم المعلوماتية واعداد استراتيجية وطنية لمأسسة عمل الامن السيبراني

ان رئيس مجلس الوزراء،

بناء على المرسوم رقم ٢ تاريخ ٢٠١٦/١٢/١٨ (تسمية السيد سعد الحريري رئيساً لمجلس الوزراء)،

بناء لضرورات المصلحة العامة،

يقرر ما يأتي :

المادة الاولى : يشكل فريق وطني لوضع خطة لمواجهة مخاطر جرائم المعلوماتية واعداد استراتيجية وطنية لمأسسة عمل الامن السيبراني قوامها السادة :

- أمين عام المجلس الأعلى للدفاع	رئيساً
- ممثل عن رئاسة الجمهورية	عضواً
- ممثل عن مجلس النواب	عضواً
- ممثل عن وزارة العدل	عضواً
- ممثل عن وزارة المالية	عضواً
- ممثل عن قيادة الجيش – وزارة الدفاع الوطني	عضواً
- ممثل عن المديرية العامة لقوى الامن الداخلي	عضواً
- ممثل عن المديرية العامة للامن العام	عضواً
- ممثل عن المديرية العامة لامن الدولة	عضواً
- ممثل عن المديرية العامة للاحوال الشخصية – وزارة الداخلية والبلديات	عضواً
- ممثل عن وزارة الاتصالات	عضواً
- ممثل عن مكتب وزير الدولة لشؤون التنمية الادارية	عضواً
- ممثل عن مصرف لبنان	عضواً
- ممثل عن المجلس الاعلى للخصخصة	عضواً
- الدكتورة لينا عويدات المنسق الوطني لتكنولوجيا المعلومات والاتصالات	عضواً مقرراً

تتم تسمية الاعضاء من قبل الوزير المختص ورؤساء الادارات المعنية

المادة الثانية : تكون مهمة الفريق:

- وضع خطة لمواجهة مخاطر جرائم المعلوماتية وأعداد استراتيجية وطنية لمأسسة عمل الامن السيبراني.
- اجراء تقييم للمخاطر والتهديدات فيما يخص الاعداد للاستراتيجية الوطنية للامن السيبراني ومكافحة جرائم المعلوماتية واقتراح الاولويات والخطط والمشاريع اللازمة.
- اعداد استراتيجية عمل الامن السيبراني وفقاً لخارطة الطريق المعدة من قبل الامانة العامة للمجلس الاعلى للدفاع بالتنسيق مع مفوضية الاتحاد الاوروبي في لبنان.
- اقتراح آلية المأسسة لتنفيذ هذه الاستراتيجية.

المادة الثالثة : يمكن للفريق الاستعانة بمن يراه مناسباً لتأدية مهامه.

المادة الرابعة : على الفريق المذكور ان يرفع الى رئيس مجلس الوزراء تقريراً دورياً كل شهر على ان يرفع تقريره النهائي خلال مهلة ستة أشهر اعتباراً من تاريخ صدور هذا القرار.

المادة الخامسة : يبلغ هذا القرار حيث تدعو الحاجة.

بيروت ، في : ٢٠١٨/ ٩/ ٢٦

رئيس مجلس الوزراء

سعد الحريري

الجمهورية اللبنانية
رئاسة مجلس الوزراء

قرار رقم ١٧٢ / ٢٠١٨

تكليف الدكتورة لينا عويدات مستشار رئيس مجلس الوزراء لشؤون المعلوماتية القيام بمهام منسق وطني لتكنولوجيا المعلومات والاتصالات

ان رئيس مجلس الوزراء،

بناء على المرسوم رقم ٢ تاريخ ٢٠١٦/١٢/١٨ (تسمية السيد سعد الحريري رئيساً لمجلس الوزراء)،

بناء على عقد اتفاق رقم ٢٨/أ تاريخ ٢٠١٧/٢/٢٥ فيما بين الدولة اللبنانية ممثلة بدولة رئيس مجلس الوزراء والدكتورة لينا عويدات للقيام بمهام مستشار رئيس مجلس الوزراء لشؤون المعلوماتية،

يقرر ما يأتي :

المادة الاولى : تكلف الدكتورة لينا عويدات مستشار رئيس مجلس الوزراء لشؤون المعلوماتية القيام بمهام منسق وطني لتكنولوجيا المعلومات والاتصالات.

المادة الثانية : يبلغ هذا القرار حيث تدعو الحاجة.

بيروت ، في : ٢٠١٨/٩/٢٦

رئيس مجلس الوزراء

سعد الحريري

رئاسة مجلس الوزراء

الأمانة العامة للمجلس الأعلى للدفاع

خارطة طريق لإعداد الإستراتيجية الوطنية للأمن السيبراني ولمكافحة جرائم المعلوماتيـة

الأهـداف

تتجه معظم الدول مرغمة الى التحول الرقمي بسبب التطور السريع لتكنولوجيا المعلومات والاتصالات. إن انتشار المعلوماتية والانترنت وخدمات الاتصالات الرقمي تفرض على الدولة ومؤسساتها اعداد استراتيجية وطنية تساعد في الصمود والتحصين امام كافة انواع التهديدات والاعتداءات الالكترونية خارجية كانت ام داخلية.

إن الامتثال الاداري الى الخدمات الالكترونية وانتشار ربط المؤسسات مع المواطن يحمل في طياته مكامن الخطأ والخطر وإمكانية الولوج الى انظمة المعلوماتية لغير المخولين لذلك، وبالتالي على الدولة ان تضع لكافة اجهزتها الأمنية والمدنية خطة استراتيجية مع التفكير بمأسسة هذا العمل لضمان الديمومة وفق هيكلية واضحة لمعالجة هذه المشاكل التي هي مرشحة الى الازدياد والتعقيد كماً ونوعاً لاسيما مع التطور التقني.

ومن اهم المحاور لأية استراتيجية هي:

1- **الدفاع والردع والتحصين** من تهديدات الداخل والخارج.

2- **التطوير المستمر** توازياً مع تطور تكنولوجيا المعلومات والاتصالات، اذ يجب ان تكون الدولة مصانة ومحصنة تجاه التهديدات الالكترونية على تنوعها، وان تكون قادرة على الصمود وعلى الرجوعية (Resilience)، وان يكون لديها ضمان لأمن المعلومات وتكاملها (integrity)، وموثوقية عالية عند كل تطور باتجاه التحول الرقمي السريع، وخصوصاً ان لبنان قد تأخر ولم يتخذ الاجراءات القانونية والإدارية والفنية المتعلقة بالحكومة الالكترونية. فالتحول الرقمي مهمة صعبة ومحفوفة بالمخاطر في حال عدم وجود استراتيجية وطنية لأمن المعلومات وللأمن السيبراني.

3- **رفع مستوى قطاع المعلوماتية الوطني في الادارات العامة** ضمن عمليات ممكننة سليمة وممنهجة وبشكل متواز ما بين الادارات وداخلها، وبشكل يتناسب مع تطور القطاع العام وحاجاته كما حاجات المواطن.

4- **تعزيز دور الاجهزة الامنية والاستخباراتية** وتوسيع نطاق التنسيق في ما بينها بدعم واشراف من السلطات العليا (رئاسة مجلس الوزراء والاجهزة المرتبطة بها) وخصوصاً الامانة العامة للمجلس الأعلى للدفاع والتي تعود مرجعيتها لرئيس مجلس الوزراء...

5- **تطوير الموارد البشرية كما الادوات، ومكونات التكنولوجيا وكيفية استخدامها**، بالشراكة مع قطاع المعلوماتية في المرافق العامة والخاصة والجامعات والجمعيات التي تعنى بهذا المجال، وبعد التأكد من موثوقية كلٍ منها.

6- **مأسسة العمل المركزي لأمن وأمان المعلومات** ضمن رئاسة الحكومة وضرورة مركزية الأمن الالكتروني على المستوى الوطني، حيث يوجب ذلك مركزية الرصد وتبادل الخبرات والمعلومات والمساندة الوطنية، وتعزيز الخبرة ومواكبة التطور ومكافحة هذا النوع من التحديات والارهاب، إضافة إلى الجريمة المنظمة وتفرعاتها.

ملاحظة: معظم الدول في استراتيجياتها قد مأسست هذا العمل على الصعيد الوطني وضمن العمل الحكومي. ان شرط النجاح هو وجود مستوى عالٍ من التنسيق بين اجهزتها.

في غياب إستراتجية التطوير الإداري وما ينتج عنها، يعتبر لبنان من بين الدول الأضعف ترتيبا وفقا لمنظمة UIT والتي يكون لبنان عضواً فيها حيث جاء ترتيبه 118 مقارنة بسلطنة عمان التي جاءت بالمرتبة الرابعة (4)

وحيث ان الأمانة العامة للمجلس الأعلى للدفاع هي جهاز يتبع مباشرة لرئيس الحكومة وقد ساهم بشكل دؤوب لرفع مستوى الوعي في هذا المجال، (مجال الأمن السيبراني)،

وحيث ان المفوضية الأوروبية قد طرحت منهجية وابدت استعدادها لدعم الدولة اللبنانية في هذا المضمار، شرط ان تكون العلاقة بين المفوضية والدولة اللبنانية علاقة مركزية بهدف عدم شرذمة الجهود، وان تكون الدولة اللبنانية جاهزة لطرح حاجاتها بشكل علمي وسليم، وان تقدم الدولة اللبنانية لذلك خارطة طريق موحدة واستراتيجية واضحة والية تنفيذية لهذه الاستراتيجية مع خطة تمويل محددة ومضمونة النتائج،

وحيث أن المفوضية الأوروبية قد سبق أن وضعت توجهاتها لمواكبة رؤية التطوير هذه وذلك لصالح الأجهزة العسكرية والأمنية والقضائية، كما وأنها مستعدة لوضع الخبرات اللازمة من الدول الأعضاء لصالح اي مبادرة مركزية تتقدم بها الدولة اللبنانية بهذا الخصوص،

وبما ان رئيس مجلس الوزراء والأمانة العامة لمجلس الوزراء بصدد طرح خطة للبدء بتطوير الأمانة العامة لرئاسة مجلس الوزراء لتكون المؤسسة الرائدة الوطنية للمكننة عن طريق مكننة اعمالها تباعاً، وتحديث هيكليتها، وخصوصاً في ما يخص المعلوماتية وتقنياتها كافة، كما الانشطة المتعلقة بها بما فيها مركزية أمن المعلومات،

لذلك، وبعد الاجتماعات المتكررة، توصلنا الى طرح خارطة طريق اولية تقضي بإنشاء الهيئة الوطنية للحد من جرائم المعلوماتية ولأمن المعلومات واعداد الإستراتيجية الوطنية للأمن السيبراني ولمكافحة جرائم المعلوماتية تكون مهمتها:

رئاسة مجلس الوزراء

الأمانة العامة للمجلس الأعلى للدفاع

1) وضع استراتيجية وطنية للدفاع والردع والتحصين من الهجمات والجرائم الالكترونية.
2) المشاركة في اعداد الهيكلية الادارية للمؤسسة الوطنية التابعة لرئاسة مجلس الوزراء والتي ستتولى هذه المهام والتنفيذ المستمر لمضمون الاستراتيجية الوطنية للدفاع والردع والتحصين من الهجمات والجرائم الالكترونية، وبما لا يتعارض مع المهمة الحالية لتطوير هيكلية رئاسة مجلس الوزراء، وتحديداً في كل ما يرتبط بالمعلوماتية والاتصالات والأمور الفنية والتقنية في هذا المضمار.
3) وبهدف مشاركة جميع المعنيين، الدعوة لتعين كل ادارة او مرفق مشارك ممثل له في هذه الهيئة الوطنية، ويحدد للممثل الخبرة المطلوبة ونوع النشاط الاداري المطلوب منه من ضمن المخطط للعام.

كما انه من الضروري ان تتمثل في هذه الهيئة الوطنية كافة الجهات العامة العسكرية والمدنية التي تعنى بهذا الموضوع الذي اصبح بحد ذاته قطاعاً متكاملاً نظراً لتعدد المهام والتقنيات والاجراءات والتطور السريع الذي يرافقه.

الجهات المشاركة في الهيئة

- رئاسة الجمهورية
- رئاسة مجلس النواب
- رئاسة مجلس الوزراء - الأمانة العامة للمجلس الأعلى للدفاع - المنسق الوطني لتكنولوجيا المعلومات والاتصالات
- وزارة المالية
- وزارة العدل
- وزارة الدفاع – قيادة الجيش – مديرية المخابرات
- وزارة الداخلية والبلديات: الأمن العام – قوى الأمن الداخلي– أمن الدولة
- وزارة الاتصالات (المديريات العامة – OGERO)
- مكتب وزارة الدولة لشؤون التنمية الإدارية OMSAR
- مصرف لبنان – قطاع المصارف - SIC
- المجلس الأعلى للخصخصة

تستعين هذه الهيئة بممثلين عن الإدارات التالية:

- وزارة الخارجية والمغتربين
- وزارة الاقتصاد والتجارة
- وزارة الصناعة
- المجلس الاقتصادي
- الهيئة الناظمة لقطاع الاتصالات
- مكتب وزير الدولة لشؤون التنمية الادارية
- وزارة التربية والتعليم العالي
- الجامعة اللبنانية
- إي مؤسسة أوهيئة أخرى

رئاسة مجلس الوزراء

الأمانة العامة للمجلس الأعلى للدفاع

فريق العمل

عن الدولة اللبنانية

اللواء الركن سعد الله الحمد	امين عام المجلس الأعلى للدفاع
العميد المهندس وجدي شمس الدين	عن الأمانة العامة للمجلس الأعلى للدفاع
الدكتورة لينا عويدات	مستشار رئيس مجلس الوزراء لشؤون المعلوماتية والاتصالات National ICT Coordinator

عن المفوضية الأوروبية

السيد جيروم ريبو غايارد: خبير في مكافحة الأرهاب

المراجـع

- كافة الوثائق المتداولة من قبل جميع الأفرقاء
- دراسة القاضية هاتيا الحلوة
- استراتيجيات دول اوروبية حديثة
- تقارير وتحقيقات عن جرائم المعلوماتية