الاستراتيجية العربية للأمن السيبراني

(2027-2023)

الفهرس

الفصل الثاني: الرؤية، الأهداف، المبادئ والتوجّهات

2.1 : رؤية الاستراتيجية العربية للأمن السيبراني

2.2: الأهداف النوعيّة للاستراتيجية

2.3: المبادئ التوجيهية

2.3.1 : سيادة القانون

2.3.2 : المقاربة المعتمدة على الأطراف المتعددة

2.3.3 : المقاربة القائمة على المخاطر

2.4 : توجّهات الاستراتيجية العربية للأمن السيبراني

2.4.1 : وضع الاستراتيجيات الوطنية للأمن السيبراني

2.4.2 : دعم البحث والتطوير

الفصل الثالث: خطة عمل الاستراتيجية

البرامج المقترحة للاستراتيجية العربية للأمن السيبراني

الفصل الرابع : خاتمة

الملاحق :

ملحق 1: الضوابط الإقليمية والمبادئ التوجيهية المقترحة للأمن السيبراني

1 : إرشادات عامة/ المبادئ التوجيهية العامّة للأمن السيبراني: إطار الأمن السيبراني للمعهد الوطني للمعايير والتقنية NIST National Institute of Standards and Technology

2 : المبادئ التوجيهية لتطوير البرمجيات الآمنة

3 : المبادئ التوجيهية لنشر الخدمة الآمنة

4 : المبادئ التوجيهية لشبكات الاتصال الآمنة: أمن شبكات الجيل الخامس

ملحق 2 : قائمة الرسوم البيانية

ملحق 3 : المراجع

ملخص تنفيذي

أدى التقدم التكنولوجي وتطور البنى التحتية لتبادل وخزن المعلومات إلى إحداث تغيير جذري وشـــامل على الصـــعيد الدولي بصـــفة عامة والعربي بصـــفة خاصـــة. حيث ما فتئت دول المنطقة تحث خطاها نحو مواكبة التقدم العالمي المتسـارع نحو بناء اقتصـاد رقمي يسـتند إلى أنظمة تقنية المعلومات وشـبكات الاتصـال المتطورة وأنظمة التقنيات التشـغيلية. ورغم الانعكاسـات الإيجابية لهذه الجهود على مسـتوى تحسـين جاهزية الدول لرفع التحديات المتعلقة بالذكاء الاصـــطناعي والثورة الصـــناعية الرابعة، إلا أن المخاوف من آثار الهجمات الســـيبرانية شـــهدت تناميا مطردا، ناهيك أن الحوادث الســـيبرانية في البلدان ذوات البنى التحتية المتطورة تواترت حدتها بنسق سريع على مر السنوات الماضية.

الاســـتراتيجية العربية للأمن الســـيبراني (ACSS) هي خطة من الإجراءات مقدّمة لفائدة الحكومات العربية لتنفيذها خلال السـنوات الخمس المقبلة لتشـجيع تبني وتطوير ضـوابط خاصّـة بالأمن السـيبراني على مسـتوى عالمي من حيث الفعالّية ومن حيث التكلفة. وتهدف **الاســـتراتيجية العربية للأمن الســـيبراني** (ACSS) إلى تحقيق تطوّر/ نموّ موحد ومتناغم، داخل المنطقة العربية، لمســـتوى النضـــج لحماية الفضـــاء الســـيبراني من التهديدات السيبرانية التي تتطوّر بشكل مستمر وسريع.

كما تحدّد **الاســـتراتيجية العربية للأمن الســـيبراني** التحدّيات التي تواجه الحكومات العربية عند العمل على تأمين فضاءها السيبراني والطريقة المثلى للتعامل معها، من خلال خمسة مواضيع رئيسية:

- **تنفيذ حوكمة شاملة للأمن السيبراني في الفضاء السيبراني العربي**
- **حماية عملية تطوير التطبيقات**
- **تأمين البنية التحتية للاتصالات**
- **تأمين إدارة البيانات**
- **الإشراف على الفضاء السيبراني العربي**

والغاية الرئيسية من هذه الاستراتيجية هي توفير التوجيه والتأطير بشأن الأمن السيبراني وتقديم أفضل الممارسات التي تشكل الركيزة الأساسية لغالبية البلدان العربية، مهما كان مستوى نضجها في المجال الرقمي: الدول القائدة أو الناضجة أو الناشئة. وسيمكّن ذلك من تنفيذ ضوابط وتدابير هامّة لتحقيق التنمية الآمنة لاقتصاد رقمي مستدام داخل الفضاء السيبراني. بالإضافة إلى ذلك، فإن اعتماد المعايير الدولية سيمكّن من قياس تأثير الضوابط المقترحة بناءا على الأطر الدولية القائمة، وخاصة المؤشر العالمي للأمن السيبراني.

وتشتمل **الاستراتيجية العربية للأمن السيبراني** (ACSS) على مجموعة من أفضل الممارسات مقسمة أساسا إلى سبعة (7) حزم عمل: work packages كالتالي"

- **حزمة عمل WP 1: وضع استراتيجيات وطنية للأمن السيبراني**
- **حزمة عمل WP 2: دعم البحث والتطوير**
- **حزمة عمل WP 3: التدريب والتوعية**
- **حزمة عمل WP 4: التعاون العربي المشترك**
- **حزمة عمل WP 5: إنشاء مراكز وطنية للاستجابة للحوادث**
- **حزمة عمل WP 6: تعزيز مناهج الأمن السيبراني الموجهة نحو سوق الشغل**
- **حزمة عمل WP 7: تحديث أطر حوكمة الأمن السيبراني**

والهدف من حزم العمل work packages هذه هو تقديم مجموعات من الأنشطة الملموسة التي تهدف إلى بناء القدرات والحماية من الجيل الجديد للتهديدات السيبرانية. وبالإضافة إلى الأهداف التقليدية للأمن السيبراني، فهي تشتمل على مفاهيم أوسع من ناحية وأكثر تكاملا من ناحية أخرى مثل : السيادة الرقمية وحماية البنية التحتية الحيوية، .... إلخ

الفصل الأوّل : الإطار والتحدّيات :

في ظلّ بيئة التهديدات السيبرانية الدائمة التغير والتطوّر، تحتاج الدول العربية إلى استراتيجيات مرنة وديناميكية للأمن السيبراني لمواجهة هذه التحدّيات والتهديدات العالمية الجديدة. انطلاقا من المستشفيات إلى خطوط أنابيب النفط، ومن المدارس إلى المطارات، إذ غالبًا ما تتغلّب الهجمات السيبرانية – بحجمها ووتيرتها- على معاييرنا الاجتماعية، وقوانيننا، ومؤسساتنا الديمقراطية، وتتسبب في عدم استقرار وتعقيدات غير مسبوقة إلى جانب الكثير من الخاطر الأخرى.

ومن ناحيتها، تهدف استراتيجيات الأمن السيبراني القوية أيضًا إلى إعداد المنظمات/ المؤسسات بشكل أفضل للاستجابة لتلك الحوادث والتهديدات في حال حدوثها وذلك من خلال منع الحوادث الصغيرة من أن تصبح حوادث كبرى، ويمكن بالتالي للمؤسسات الحفاظ على سمعتها وتقليل الضرر الذي قد يلحق بالموظفين والعملاء وأصحاب المصلحة والشركاء وغيرهم.

الاستراتيجية العربية للأمن السيبراني (ACSS) هي خطة عمل مصمّمة لتحسين أمن ومرونة البنى التحتية والخدمات الوطنية. وهي مقاربة على مستوى عال للأمن السيبراني، تحدد مجموعة من الأهداف والأولويات الوطنية التي ينبغي تحقيقها في إطار زمني محدد. في الوقت الرّاهن، وبما أن العديد من الدول في المنطقة العربية لا تملك إستراتيجية وطنية للأمن السيبراني، يمكنها الاستئناس بمخرجات هذه الاستراتيجية لمساعدتها على معالجة المخاطر والتهديدات السيبرانية التي من شأنها أن تقوّض وتمنع تحقيق الفوائد الاقتصادية والاجتماعية المرجوّة والمنتظرة من الفضاء السيبراني.

وبالإضافة إلى معالجة مخاطر الأمن السيبراني، تؤكّد هذه الاستراتيجية كثيرا على التعاون والشراكة حيث تعتبر أن مشاركة المعلومات على الصعيد الإقليمي وإنشاء شراكات بين القطاعين العام والخاص هي من أهم الركائز لتحسين التعاون المشترك بين جميع أصحاب المصلحة.

1.1دراسة مقاربة benchmarking بين استراتيجيات الأمن السيبراني الوطنية والإقليمية

من الواضح جدا أن وتيرة تطوّر التهديدات السيبرانية أصبحت تسير بشكل متوازي مع التطوّرات التي تشهدها تكنولوجيا الاتصال والمعلومات، وبالتالي أصبحت الهجمات السيبرانية الحديثة معقدة جدّا، بمعنى أنها تؤدي إلى أضرار جسيمة وتؤثر على نطاق واسع. وقد أجبر هذا التطور الدول عبر العالم على تحسين برامج الأمن السيبراني الخاصّة بها من خلال تطوير الإستراتيجيات الوطنية للأمن السيبراني. ووفقًا لمرصد الاستراتيجيات الوطنية للاتحاد الدولي للاتصالات، نجد أن 127 دولة قد طوّرت استراتيجيات وطنية للأمن السيبراني من أجل التعامل مع التهديدات السيبرانية بطريقة عمليّة وأكثر تنظيما.

والجدير بالذكر أن 60 دولة نجحت في إجراء التعديلات الناتجة عن التغذية الراجعة الخاصة بالأمن السيبراني من خلال إصدار نسخة محدثة ومطوّرة من إستراتيجيتها الأولية للأمن السيبراني. ولكن مع تطوّر مستوى نضج العديد من الإستراتيجيات الوطنية للأمن السيبراني، برزت مخاوف جديدة بخصوص القدرة على التنسيق على المستوى الإقليمي. فعلى سبيل المثال، في أوروبا، أكملت جميع الدول تطوير استراتيجياتها الوطنية للأمن السيبراني منذ عام 2017. ومنذ ذلك التاريخ، تشارك وكالة الاتحاد الأوروبي للأمن السيبراني (ENISA)بشكل مكثف في إصدار وثائق توجيهية للبلدان الأعضاء من أجل تحسين نضج وكفاءة الإجراءات والضوابط الأمنية المحددة في استراتيجياتها الوطنية [1،2]. وعلى نفس المنوال، تبذل منظمة البلدان الأمريكية (OAS) www.oas.org جهودًا تنسيقية على المستوى الإقليمي مع التركيز على تطوير الإستراتيجيات الوطنية للأمن السيبراني ؛ الدورات التدريبية وورش العمل في مجال الأمن السيبراني ؛ بالإضافة إلى تطوير شبكة Hemispheric Network التابعة لمنظمة الدول الأمريكية ، والمعروفة باسم CISRTAmericas.org ؛ تمارين/تطبيقات الأمن السيبراني. الأمن السيبراني والحكومة الإلكترونية من أجل الإدارة العامة الفعالة؛ وتحديد المعايير الفنية واعتمادها من أجل بنية أنترنت آمنة [3]. وفي الآونة الأخيرة، في يناير 2021، اعتمد أعضاء برلمان المجموعة الاقتصادية لدول غرب إفريقيا (ECOWAS) الاستراتيجية الإقليمية للأمن السيبراني ومكافحة الجرائم الإلكترونية في المجتمع [4]. وتهدف هذه الاستراتيجية إلى زيادة مرونة الفضاء السيبراني في المنطقة، ومساعدة الدول الأعضاء على تعزيز قدراتها في مجال الأمن السيبراني، وحماية الفضاء السيبراني

والبنى التحتية الحيوية للمعلومات الخاصة بها، فضلاً عن بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات. بالإضافة إلى أنها تستهدف خاصّة مكافحة الجريمة السيبرانية بشكل فعال. وفي عام 2021 أيضًا، طورت رابطة دول جنوب شـــرق آســـيا https://asean.org (ASEAN) / "اســـتراتيجية التعاون في مجال الأمن السيبراني" بهدف تسهيل التنسيق وتبادل المعلومات بين الدول الأعضاء.

وتؤكد هذه الجهود المبذولة لوضع أطر تعاون إقليمية في مجال الأمن السيبراني على الحاجة إلى إنشاء منصة إقليمية داخل المنطقة العربية للدول الأعضـــاء لتبادل المعلومات وتقديم وجهات النظر المختلفة حول التهديدات الناشئة والقائمة، وتنفيذ الضوابط الأساسية للأمن السيبراني، بالإضافة إلى بناء وتنمية القدرات.

وفي إطار هذا السياق العالمي الذي يدفع باتجاه تطوير استراتيجيات ووثائق إرشادية إقليمية للأمن السيبراني، تهدف هذه الوثيقة إلى وضع النسخة الأولى من "الاستراتيجية العربية للأمن السيبراني" ، والتي تهدف إلى إنشاء إطار عمل اســـتراتيجي تأخذه الدول الأعضـــاء في جامعة الدول العربية في الاعتبار عند إعداد إســـتراتيجياتها الوطنية وتنفيذ خطط عملها للمساعدة على تحسين مستوى أداء الآليات الوطنية للأمن السيبراني و مجابهة الجرائم السيبرانية.

1.2 / الأمن السيبراني في المنطقة العربية

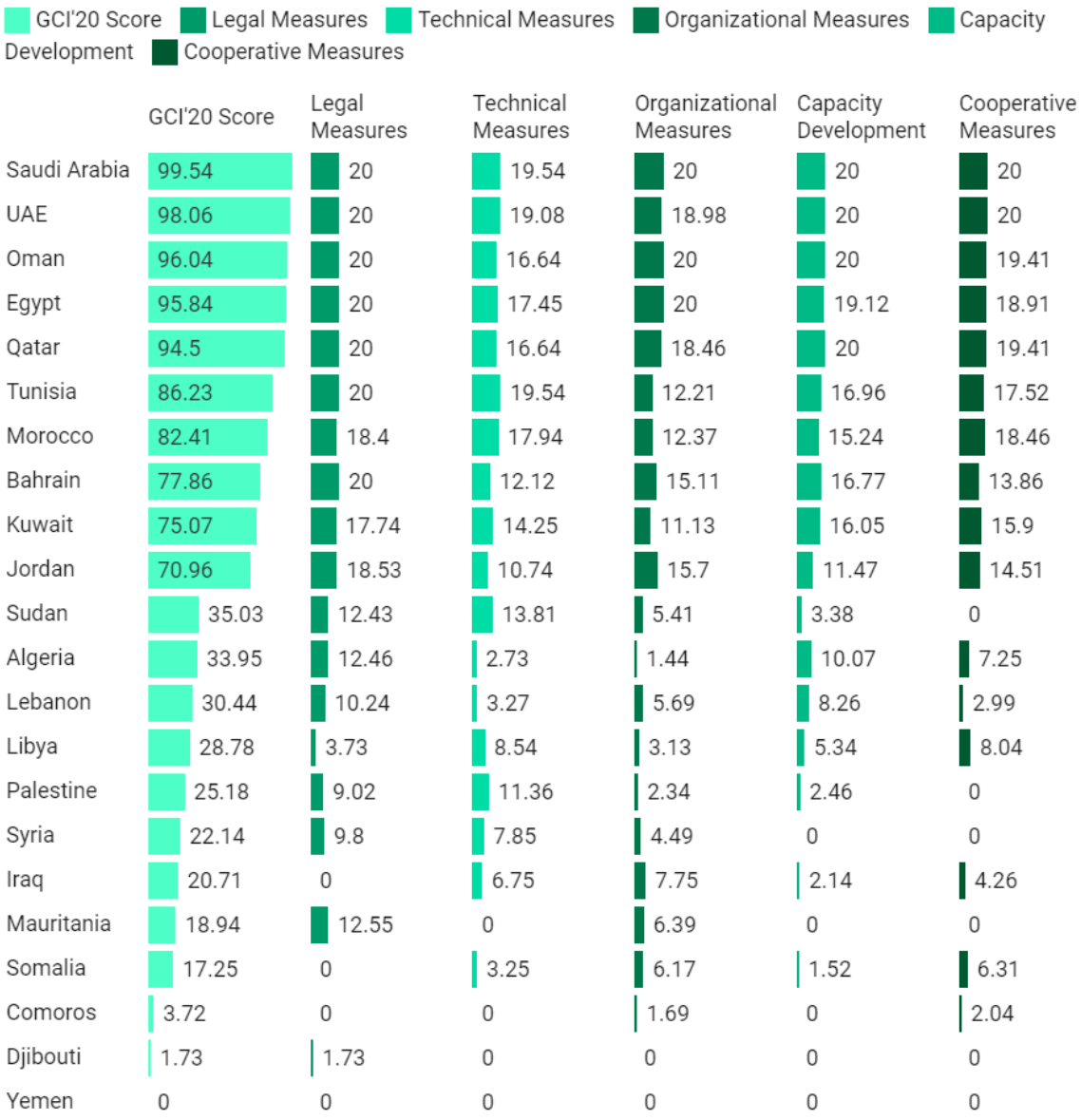
لقد مكّن انتشار التحولات الرقمية على نطاق واسع في جميع أنحاء المنطقة العربية من خلق آثار إيجابية كبيرة على مختلف أوجه حياتنا اليومية، إلا أنه كشف أيضًا عن الأصول assets الحساسة للتهديدات السيبرانية التي أصبحت تستهدف الآن قطاعات اقتصادية حيوية متعددة مثل: التمويل والطاقة وتوزيع الأغذية والرعاية الصحية والنقل وغيرها.

في المنطقة العربية، يفوق معدل انتشـــار الإنترنت بشـــكل عام الـــ 90٪ ، وفي بعض الحالات ، مثل الكويت والإمارات العربية المتحدة وقطر ، يقترب من 100٪. ومن هنا، أدركت العديد من الدول العربية أن أمن الفضاء السـيبراني هو جزء لا يتجزأ من أنظمتها الاقتصـادية وهو مسـألة تتعلق أسـاسـا بالأمن القومي. نتج عن هذا الوعي وضـع عدد هام من السـياسـات والإجراءات: فوفقا للمؤشـر العالمي للأمن السـيبراني للاتحاد الدولي للاتصـالات(ITU) ، تصـنف دول مثل: المملكة العربية السـعودية، الإمارات العربية المتحدة، سـلطنة عمان، جمهورية مصـر العربية ودولة قطر ضـمن أفضـل 20 دولة على مسـتوى العالم. بالإضـافة إلى أن العديد من الدول العربية الأخرى، احتلت، على مدى السنوات الأخيرة، مراتب أعلى من العديد من الدول الأوروبية.

إن السعي لتحقيق الأمن السيبراني هو مسعى عالمي بقدر ما هو مسعى محلي وعربي وإقليمي أيضًا، والمنطقة العربية تمكنت في السنوات الأخيرة من تسريع وتيرة الجهود والإنجازات في مجال الأمن السيبراني. وفي هذه الوثيقة، سنستعرض المبادرات الرئيسية المتعلقة بالأمن السيبراني في المنطقة العربية، ونقدم تقريرًا عن تطور وضع الأمن السيبراني، وأيضا سبل التعاون العربية والدولية الممكنة في مجال الأمن السيبراني.

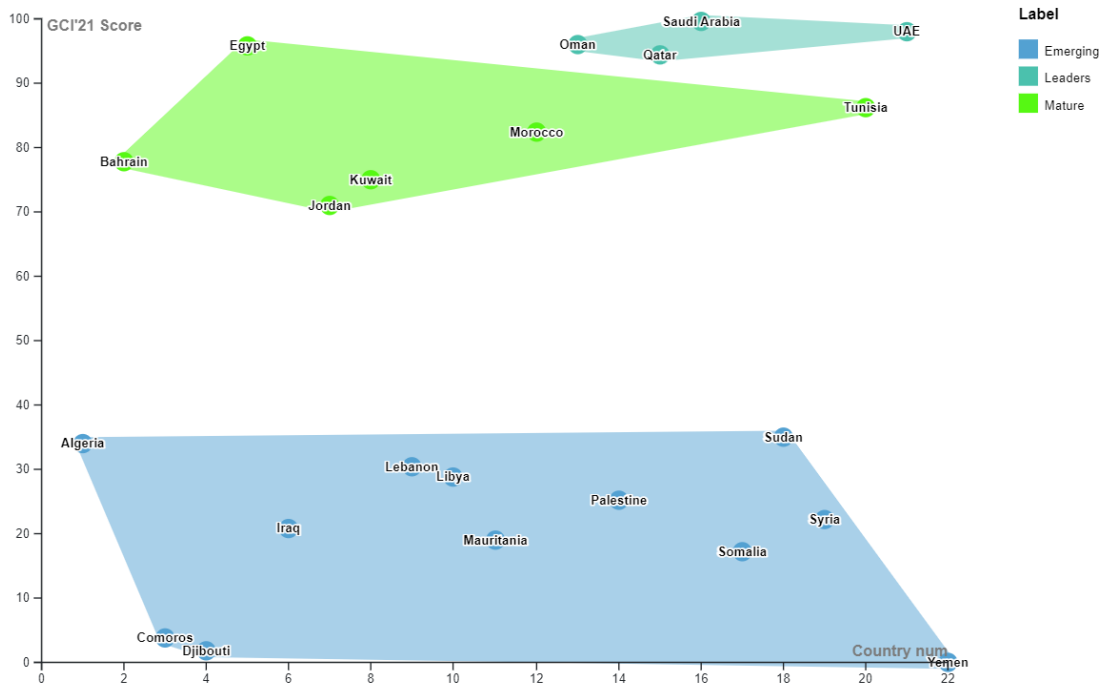
وفقًا للمؤشر العالمي للأمن السيبراني 20 (GCI'20)، الذي أصدره الاتحاد الدولي للاتصالات في عام 2021، احتلت المملكة العربية السعودية المرتبة الثانية عالميا والمرتبة الأولى على مستوى المنطقة العربية، مما جعلها رائدة عالميا في مجال الأمن السيبراني. ووفقًا لهذا المؤشر، يتم قياس أداء كل دولة ضمن خمس فئات، وهي التدابير القانونية والتدابير الفنية والتدابير التنظيمية وبناء القدرات والتعاون الدولي. وعليه فإن عامل النجاح الرئيسي للمملكة هو القدرة على تنفيذ رؤية 2030 وبرنامج التحول الوطني 2020 الذي شمل جهود كل القطاعات بما في ذلك القطاع العام والقطاع الخاص وأيضا القطاعات غير الربحية.

وكان وضع الخطط والإجراءات الوطنية في مجال الأمن السيبراني من بين القوى الدافعة الرئيسية الذي جعل المملكة تصل إلى مرتبة البلدان القليلة الأولى التي حققت مستوى عالٍ من النضج في مجال الأمن السيبراني (أكثر من 99٪). ويوضح **الرسم البياني 1** أن المملكة العربية السعودية وصلت تقريبًا إلى أعلى مستوى نضج (أي 20) وفقًا للركائز الخمس التي أخذها المؤشر في الاعتبار. والجدير بالذكر أيضًا أن الإمارات العربية المتحدة تظهر في المراكز الخمسة الأولى في تصنيف المؤشر العالمي للأمن السيبراني GCI بدرجة نضج عالمية تبلغ 98.06. وتعتبر هذه قفزة كبيرة بـ 28 مرتبة مقارنة بإصدار 2018 من مؤشر GCI، حيث نفذت الإمارات بنجاح تدابير فعالة إلى حد كبير للتعامل مع تهديد الأمن السيبراني. ويظهر تحليل الأداء الإقليمي العالمي فيما يتعلق بالأمن السيبراني أن الدول السبع الأعلى مرتبة فقط وصلت إلى مستوى نضج أكثر من 15 من حيث التدابير الفنية، والتدابير التنظيمية، وبناء القدرات، والتعاون الدولي.



	GCI'20 Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
Saudi Arabia	99.54	20	19.54	20	20	20
UAE	98.06	20	19.08	18.98	20	20
Oman	96.04	20	16.64	20	20	19.41
Egypt	95.84	20	17.45	20	19.12	18.91
Qatar	94.5	20	16.64	18.46	20	19.41
Tunisia	86.23	20	19.54	12.21	16.96	17.52
Morocco	82.41	18.4	17.94	12.37	15.24	18.46
Bahrain	77.86	20	12.12	15.11	16.77	13.86
Kuwait	75.07	17.74	14.25	11.13	16.05	15.9
Jordan	70.96	18.53	10.74	15.7	11.47	14.51
Sudan	35.03	12.43	13.81	5.41	3.38	0
Algeria	33.95	12.46	2.73	1.44	10.07	7.25
Lebanon	30.44	10.24	3.27	5.69	8.26	2.99
Libya	28.78	3.73	8.54	3.13	5.34	8.04
Palestine	25.18	9.02	11.36	2.34	2.46	0
Syria	22.14	9.8	7.85	4.49	0	0
Iraq	20.71	0	6.75	7.75	2.14	4.26
Mauritania	18.94	12.55	0	6.39	0	0
Somalia	17.25	0	3.25	6.17	1.52	6.31
Comoros	3.72	0	0	1.69	0	2.04
Djibouti	1.73	1.73	0	0	0	0
Yemen	0	0	0	0	0	0

الرسم البياني 1: ترتيب البلدان العربية حسب المؤشر العالمي للأمن السيبراني

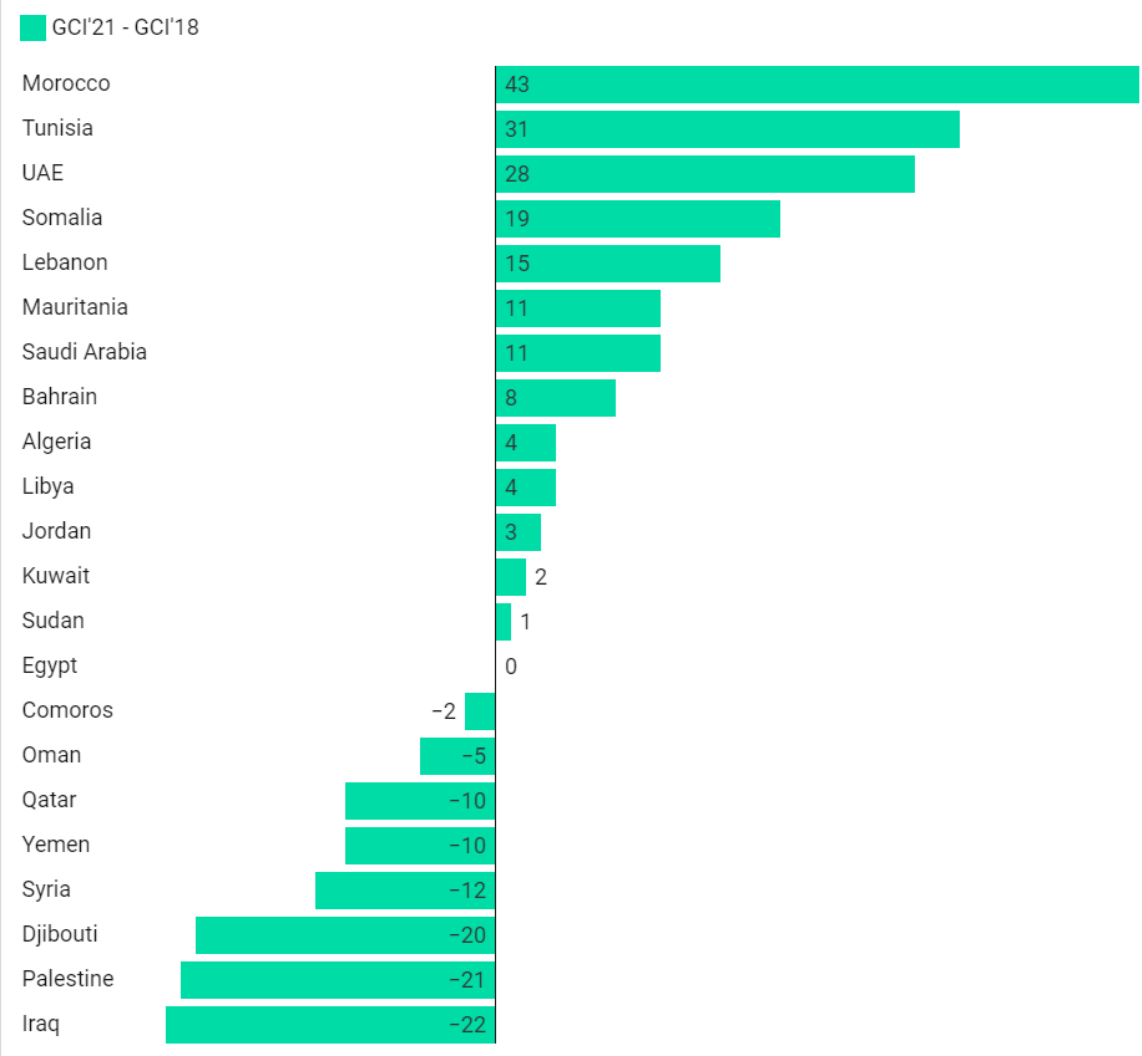


الرسم البياني 2: الأمن السيبراني في المنطقة العربية - الدول القائدة والناضجة والناشئة

يجسد الرسم البياني عدد 2 تصنيف الدول العربية من حيث نضج الأمن السيبراني: دول قائدة، دول ناشئة و دول ناضجة. وتشمل الفئة الأولى وهي فئة "القادة" 5 دول في حين تنتمي 7 دول إلى الفئة الناشئة في حين تعتبر 11 دولة ذات مستوى ناضج في مجال الأمن السيبراني. وبالتالي يجب بذل جهود كبيرة في المستقبل للحصول على أداء إقليمي أكثر تناسقا من حيث الاستعداد والجاهزية في مجال الأمن السيبراني.

الرسم البياني 3: الدرجات التفاضلية للمؤشر العالمي للأمن السيبراني (2018-2020)

وفقًا للرسم البياني عدد 3، فقد تم تحقيق أهم القفزات في الترتيب من طرف المغرب (43) وتونس (31). وتظهر النتائج التفصيلية التي توصلوا إليها والموضحة في الرسم البياني 1 أنه، في حالة حدوث تحسن في ركيزة التدابير التنظيمية، ستكون هذه البلدان قادرة على الانضمام إلى "مجموعة القادة" في المستقبل القريب.

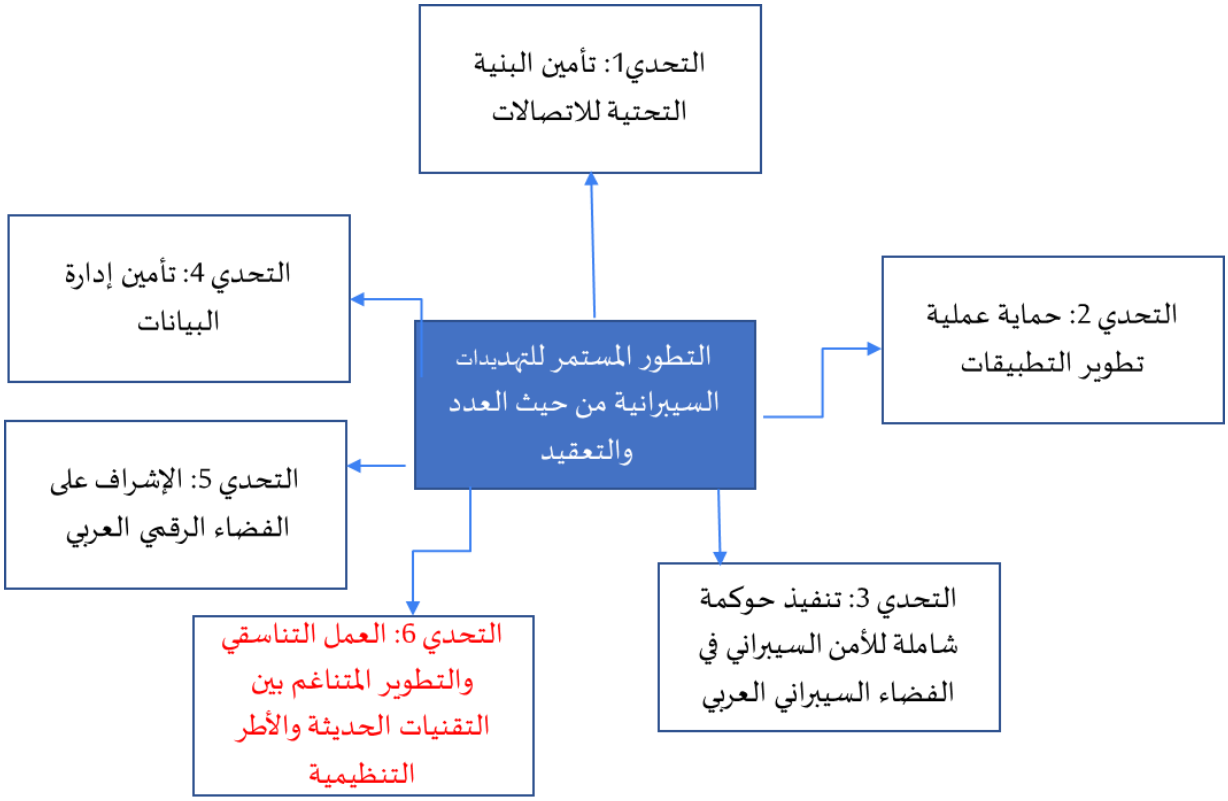


الرسم البياني 4: المراتب التفاضلية المصنفة للمؤشر العالمي للأمن السيبراني (2018-2020)

ويوضح الرسم البياني عدد 4 الجهود التي يجب بذلها لتحسين ترتيب البلدان التي انخفض فيها ترتيب المؤشر العالمي للأمن السيبراني بين عامي 2018 و2020.

1.3التحديات الإقليمية للأمن السيبراني

بناءً على التحليل السابق، يحدد هذا القسم نطاق واتجاهات الخطط الخاصة بالإستراتيجية العربية للأمن السيبراني من خلال تحديد التحديات وعوامل النجاح. من خلال تحليل الدوافع والفرص الرئيسية التي تؤثر على التحوّلات في مجال الأمن السيبراني، سيتم تفصيل الأهداف الإستراتيجية "**للإستراتيجية العربية للأمن السيبراني**" في القسم التالي.



رسم بياني عدد 5: تحديات الأمن السيبراني في المنطقة العربية

1.3.1التحدي الأول : تأمين البنية التحتية للاتصالات

نظرًا لأن الفضاء السيبراني اكتسب شعبيّة أكبر وأصبح أكثر ترابطًا عبر الحدود الإلكترونية والمادية، يجب على جميع مقدمي الخدمات الترويج لفكرة "المهمة المضمونة" "mission assured" وتطبيق إدارة المخاطر على هذه المتغيّرات في الفضاء السيبراني. يجب ضمان أمن الفضاء السيبراني حتى يتمكن جميع الأفراد وأصحاب المصلحة المشاركين في هذا الفضاء من المشاركة بكل ثقة. تحقيقا لهذه الغاية، تتخذ الإدارات المركزية نهجا شاملا للأمن السيبراني وتعمل مع أصحاب المصلحة لخلق بيئة مستقلة لإدارة المخاطر من خلال المساعدة الذاتية والتعاون. بالنسبة للبنية التحتية الاجتماعية والاقتصادية التي تضمن سلامة وأمن المواطنين/ الناس، تقود الحكومة المجتمع كوحدة متكاملة من خلال تقديم مبادرات متطوّرة وتنفيذ دفاع إلكتروني شامل باستخدام جميع الموارد المتاحة. وتندرج أهمية البنية التحتية والأنظمة الحيوية لأهمية الخدمات التي توفرها وذلك في إطار مقاربة مبنية على تحليل المخاطر التي تهدد جميع الأنظمة والتطبيقات والبيانات ذات الطبيعة الحساسة. ويتم ذلك أثناء المراجعة المستمرة للدفاعات والأصول الهامة للحماية من الهجمات السيبرانية والعمل مع أصحاب المصلحة المعنيين لضمان أمن وموثوقية الفضاء السيبراني. من خلال هذه المبادرات، ستحقق الحكومات دفاعات سيبرانية متعددة الطبقات تعتمد على المساعدة الذاتية والاستنتاج والدعم العام من جميع المشاركين في الفضاء السيبراني، مما يقلل المخاطر ويدعم / يزيد الاستقرار في جميع أنحاء المنطقة.

نظرًا لانفتاح الفضاء السيبراني أكثر وأكثر على العامة، من الضروري إرساء مجتمع أين يمكن لجميع أصحاب المصلحة الاستمتاع بالراحة والأمن السيبراني. حيث تتعاون الحكومة الوطنية مع أصحاب المصلحة المعنيين في هذا الجهد، وتعمل على تصور الركائز التكنولوجية والخدمات التي تشكل الفضاء السيبراني وتحسين إمكانية التتبع في حالة وقوع حادث. هذه التحسينات من شأنها أن تعزّز البيئة التي يمكن لكل صاحب مصلحة اختيار خيارات إدارة المخاطر المناسبة التي تتناسب مع احتياجاته. بالإضافة إلى ذلك، من خلال تأمين إمكانية التتبع وتشجيع ضحايا الجرائم السيبرانية على إبلاغ الشرطة وإخطار الوكالات العامة، ستتمكن الحكومة الوطنية من القضاء على العوامل والبيئات التي تتسامح مع الجرائم السيبرانية. سيتم متابعة هذه المبادرات على أساس مبدأ "ضمان التدفق الحر للمعلومات". ومع حدوث مثل هذه التغييرات في الفضاء السيبراني، يصبح تأثير الحوادث معقدًا بشكل متزايد وقد ينتشر على مساحة واسعة. ومع ظهور مثل هذه المخاطر على الواجهة، ستعمل الحكومة مع أصحاب المصلحة المعنيين لخلق بيئة تشمل الممارسات المعيارية التي تسمح لمقدمي الخدمات بتكوين نظرة/فكرة شاملة على الترابط والعلاقات المتبادلة عبر الفضاء السيبراني خلال عملهم

وسعيهم إلى إدارة المخاطر بشكل شامل، مع التركيز، ليس فقط، على المستخدمين المباشرين ولكن أيضًا على المستخدمين النهائيين.

ستدعو "**الإستراتيجية العربية للأمن السيبراني**" إلى إنشاء آليات لتبادل المعلومات لتمكين تبادل المعلومات واليقظة حول التهديدات السيبرانية التي يمكن استغلالها في القطاعين العام والخاص وفيما بينهما. يمكن أن تساعد برامج تبادل المعلومات الرسمية وغير الرسمية في تعزيز التنسيق الفعال والاتصالات المتواصلة والدقيقة والمناسبة أثناء الاستجابة للحوادث وأنشطة التعافي ؛ تسهيل التبادل السريع للمعلومات الاستباقية المتعلقة بالتهديدات بين الأطراف المتضررة وأصحاب المصلحة الآخرين ؛ المساعدة في تحسين فهم القطاعات التي تم استهدافها وكيفية الاستهداف ؛ نشر المعلومات حول الأساليب التي يمكن استخدامها للدفاع عن الأصول والتخفيف من حدّة الأضرار التي لحقت بها ؛ و في النهاية تقليل نقاط الضعف و إمكانيات التعرض لهذه المخاطر. ستحدّد الاستراتيجية العربية للأمن السيبراني (ACSS) واحدًا أو أكثر من الهياكل المؤسسية (أي السلطات المختصة) المسؤولة عن نقل المعلومات الدقيقة والقابلة للتنفيذ بين الفاعلين في الأمن السيبراني الوطني، بما في ذلك القطاعين العام والخاص. كما يجب أن تكون عملية تبادل وتراسل المعلومات مفعلة في اتجاهين. فإذا كانت الحكومات على استعداد لمشاركة المعلومات التي تحتفظ بها، فإن هذه الإجراءات ستثبت لهيئات القطاع الخاص أن الحكومة هي بالفعل شريك في تبادل معلومات التهديد، وتساعد على ضمان أن للمستجيبين قدرة واستعداد للاستجابة للتهديدات الأساسية.

1.3.2التحدي الثاني: حماية عملية تطوير التطبيقات :

ستحدد الإستراتيجية العربية للأمن السيبراني منهجية مشتركة لإدارة مخاطر الأمن السيبراني مما يضمن الفعالية والتناسق بين جميع المنظمات ويسهل تبادل معلومات التهديدات والمخاطر عبر الأنظمة المتداخلة. ويجب تفضيل المنهجية القائمة على المعايير الدولية لأنها قد تساعد في تقليل التكاليف من ناحية وتفاعل أفضل مع القطاع الخاص من ناحية أخرى. ستوفر المنهجية إرشادات حول تحديد الأدوار والمسؤوليات لمختلف جوانب إدارة المخاطر، مثل تقييم التهديدات، وتقييم / تقدير الأصول، وتنفيذ تدابير الحماية و الحرص على تطبيقها، وقبول المخاطر المتبقية. يجب أن تتضمن المنهجية برنامج اعتماد للمساعدة في تقييم الامتثال وتحسينه في نهاية المطاف. والأهم من ذلك، بالنسبة لشراء وتطوير البنى التحتية أو الخدمات، يجب أن توفّر منهجية إدارة المخاطر إرشادات لتقليل المخاطر إلى الحد الأدنى من خلال هندسة وتصميم آمنين وإجراء عمليات تقييم وتدقيق منتظمة، مع الوعي بأن الأمن يتم تحقيقه على أفضل وجه عندما يكون جزءًا لا يتجزأ من عملية التصميم والتطوير والتنفيذ لمنتج أو عملية أو خدمة (التأمين عند التصميم)

والهدف من ذلك هو خلق تعاون فعال وتناغم أفضل بين المؤسسات البحثة والشركات والحكومة لتحسين القدرة على الانتقال من التطوير في المؤسسات الجامعية إلى التطبيق في القطاع الخاص والخدمات العامة. ويمكن النظر إلى السوق الضخم في المنطقة على أنه ميزة بالنسبة لمرحلة الحاضنة/مرحلة الاحتضان ، حيث يمكن أن ينتقل المنتج الموجّه إلى المجتمع سريعا إلى مرحلة الاكتمال.

إن أهم شرط أساسي لتحقيق هذا الهدف الاستراتيجي هو ضمان آليات تعاون فعالة بين المؤسسات الأكاديمية والشركات الخاصة والمؤسسات الحكومية، مما يضمن أن الأولويات الاستراتيجية ستكون هي الموجّهة لتركيز البحث والتطوير في الأوساط الأكاديمية وكذلك في القطاع الخاص، وبالتالي ضمان وجود الكفاءات الرئيسية لفائدة المنطقة.
والجدير بالذكر، أن المنطقة العربية تفتقر إلى خطة بحث وتطوير موحدة تتعامل مع مجتمع المعلومات والأمن السيبراني والحلول التقنية التابعة لهم. وتتمثل الخطوة التالية في ضوء الإستراتيجية العربية للأمن السيبراني في إنشاء آلية تنسيق وتحديد مجالات التركيز للبحث والتطوير في مجال الأمن السيبراني. وبناءً على قضايا البحث ذات الأولوية للمنطقة في هذا الصدد، يمكن، في المستقبل، تقديم المبادئ التوجيهية للبحث والتطوير الذي يتم إجراؤه في الجامعات والشركات، لتوفير دعم إضافي للتدابير الخاصة بالشركات والمشاريع التعليمية والمنح الدراسية.

ومن أجل تمكين التعاون الفعال بين القطاعين العام والخاص لإنتاج حلول جديدة تتبناها الهيئات الإقليمية، يجب أيضًا تحديث اللوائح الخاصة بالتعامل مع الملكية الفكرية، حيث أنها تركز في الوقت الراهن على المنتجات والخدمات التي يتم تداولها في الفضاء المادي، دون الأخذ بعين الاعتبار الخصائص الأساسية للبيئة الرقمية. في المرحلة الأولى، سوف يتم تقديم مزيد من التفاصيل حول الوضع الحالي ومجموعة المشاكل والتحدّيات، مع الأخذ في الاعتبار ممارسات الشراء والتراخيص الحالية في المؤسسات وأفضل الممارسات واللوائح في البلدان الأخرى والمميّزات المحددة لحلول الأمن السيبراني. بناءً على التحليل الذي تم إجراؤه، يمكن تطوير استراتيجية حقوق ملكية فكرية إقليمية متكاملة للبرامج، استراتيجية من شأنها دعم تطوير شركات البرمجيات العربية وقدرتها التنافسية في العالم وإدخال التعديلات التشريعية اللازمة لجعل ذلك ممكنًا. الهدف هو خلق المرونة الكافية لإحداث الفرص وتسويق البرمجيات التي تطلبها الهيئات الإقليمية بطريقة تعزز تطوير الشركات بحيث يمكن أن تكون حقوق الملكية الفكرية للبرمجيات مملوكة من قبل الشركات الخاصة التي طوّرتها مع إيجاد سبل تتيح استعمالها من جهات عربية أخرى وهذا يمنح للمنطقة إمكانيات أكبر لتعديل هذه البرمجيات وتطويرها بشكل يخدم الغايات التي طوّرت من أجلها.

1.3.3 التحدي الثالث : تنفيذ حوكمة شاملة للأمن السيبراني في الفضاء الرقمي العربي

على الرغم من أنه لا يمكن التنبؤ بشكل دقيق بالمخاطر المستقبلية، سيتعين على المنطقة العربية تطوير المبادئ العامّة ونقاط الارتكاز السياسية حول القضايا الرئيسية المتعلقة بالتكنولوجيات المستقبلية. وسوف يتطلب التعامل مع المخاطر السيبرانية المستقبلية نقاشًا واسعا في المجتمع، وللقيام بذلك، يتعيّن على الدول تقديم المعلومات المعقدة والرسائل الفنية بطريقة مفهومة، دون "إغفال بعض الأمور" والتغاضي عن التفاصيل الأساسية. من خلال هذه المقاربة، سوف نتأكد من إمكانية معالجة المخاطر غير المحددة بناءً على الكفاءة والمعرفة، وليس بشكل رد الفعل وعلى أساس المخاوف.

ولتحقيق هذا الهدف، سيتعين علينا الاعتماد على الكفاءة البحثية في المجالات ذات الأولوية للدول العربية مثل: التشفير وتقنية سلسلة الكتل blockchain والذكاء الاصطناعي AI وإدارة الهوية الآمنة، وسوف يتعين علينا ضمان أن يكون تطوير القدرات والكفاءات الهامة مدرجا في مستوى التعليم الأساسي والتطبيقي. من أجل التخفيف عمليًا من المخاطر التكنولوجية، نتصور بشكل أساسي أنه يجب المحافظة على تحديث حلول تكنولوجيا المعلومات، وضمان تصميم الحلول التي تسمح بإحداث التغييرات بطريقة مرنة وإيجاد حلول بديلة إلى جانب الوقاية من التهديدات السيبرانية، ستكون مواكبة التكنولوجيات الجديدة والتقدّم في المجال مهمة في مكافحة الجرائم السيبرانية وأشكال التهديدات الأمنية الجديدة بما في ذلك التهديدات والمخاطر الهجينة hybrid threats المحتملة.

كما ستحدّد **الإستراتيجية العربية للأمن السيبراني** مقاربة منسجمة coherent لإدارة المخاطر ليتم إتباعها من قبل جميع الهيئات الحكومية ومشغلي البنى التحتية الحساسة الذين يتم تحديدهم محليًا. ويجب أن تهدف هذه المقاربة إلى الاعتماد على تقييم التهديدات السيبرانية وتطوير سجل وطني للمخاطر، يتم تخزينه وتبادله بشكل آمن، للسماح للحكومات بالإشراف على المخاطر والأساليب المتبعة لإدارتها. علاوة على ذلك، يجب أن تطوّر هذه المقاربة طريقة لتحديد الأولويات بناءً على احتساب احتمالية حدوث المخاطر ومدى وتأثيرها. وأيضا، يجب أن تحدد مسؤوليات الهيئات الرئيسية في كل قطاع فيما يتعلق بالتقييم وعتبة القابلية ومعالجة مخاطر الأمن السيبراني على المستوى الوطني.

على الصعيد الدولي، نحن مرتبطون أشد الارتباط بالتطورات العالمية ونحن جزء لا يتجزأ من المشهد العالمي لتكنولوجيا المعلومات والاتصالات – ومن أجل تطويع هذا التطور ليتماشى مع مصالح المنطقة واحتياجاتها، سيكون من الضروري المشاركة في الحوار على المستوى الدولي. كمنطقة عربية، نحن بالضرورة مندمجون مع القطاع الخاص وخدمات الشركات المصنعة الكبرى Google) و Apple و Microsoft وما إلى ذلك - (وقد تم توضيح التأثير المحتمل لهذه degenderizes خلال أزمة بطاقة الهوية في خريف عام 2017). للتغلب على مثل هذه المخاطر وتبعاتها، يتعين علينا تطوير مركز كفاءة قادر على تقييم أمن التكنولوجيات والخدمات ولديه نظرة عامة مركزية على المخاطر الرئيسية، ويقدم الاستشارة لمؤسسات القطاعين العام والخاص بشأن الأمور المتعلقة التكنولوجيا المستقبلية ويقع الاعتراف به دوليّا.

ويشمل التحدي الثالث تأمين البنية التحتية المعلوماتية، وجهود القوات المسلحة فى تأمين البنية التحتية الحرجة، وذلك من خلال التعاون مع الجهات المعنية لمجابهة التهديدات السيبرانية ضد الأماكن والأهداف الحيوية، لتجنب تداعياتها السلبية على المرافق والمنشآت الحيوية بالمنطقة العربية.

1.3.4التحدي الرابع: تأمين إدارة البيانات

من أجل إتخاذ التدابير اللازمة التي تشمل إدارة المخاطر، يجب أن تعمل الحكومة على تعزيز الجهود لتطوير وتنفيذ تدابير أمنية ملموسة في مجال الصناعة. سيتم تحقيق ذلك من خلال صياغة إرشادات خاصة بالصناعة بناءا على إطار عمل للتدابير الأمنية التي تغطي كلاً من الفضاء الإلكتروني والفضاء المادي. ستدعم الحكومة الوطنية المبادرات التي تقودها الصناعة والتي تهدف إلى تعزيز تبادل المعلومات وإعداد التقارير والإعلانات المناسبة داخل سلسلة التوريد، بحيث يمكن السيطرة على أي مخاطر تحدث من قبل كل صاحب مصلحة مع رؤية واسعة لسلسلة التوريد بأكملها، بما في ذلك الشركات الصغيرة والمتوسطة، المكاتب الخارجية وشركاء الأعمال. بالإضافة إلى ذلك، ستقوم الحكومة الوطنية ببناء آلية لتأمين موثوقية مكونات سلسلة التوريد بما في ذلك الأجهزة والبرامج والبيانات والخدمات. بالإضافة إلى ذلك، يجب أن تعمل الحكومة الوطنية على المضي قدمًا في بناء آلية للكشف والحماية من الهجمات التي تضعف صيانة وموثوقية إمكانية التتبع، وذلك بهدف الحفاظ على استمرار الموثوقية في هذه المكونات في سلسلة التوريد.

1.3.5التحدي الخامس: الإشراف على الفضاء السيبراني العربي

إنه لمن الأهمية بمكان للمنطقة العربية ضمان الاتصال الآمن والفعال وتبادل البيانات بين الأنظمة المتخصّصة لمختلف مجالات الإدارة والسلطات (بما في ذلك الاتصالات الهاتفية والاتصال بالإنترنت). للقيام بذلك، من المقرّر، ولأوّل مرّة تطوير رؤية شاملة - مفهوم اتصال إقليمي يحدّد الحاجة إلى التواصل في كل من المواقف العادية وأيضا في أوقات الأزمات. بناءً على ذلك، سيكون من الممكن تحديد احتياجات التطوير وتخطيط الأنشطة ووضع تقسيم المهام وكيفية تنظيمها بين الأطراف المختلفة. علاوة على ذلك، من المقرّر الاستمرار في توسيع وتطوير شبكة اتصالات البيانات الإقليمية والانتقال إلى المراسلات الإلكترونية المشفرة واتصالات البيانات لضمان الاتصال الآمن بين المؤسسات الحكومية.

خلال فترة الإستراتيجية، سيكون التركيز الرئيسي على ضمان استمرارية الخدمات الحيوية والوقاية من الحوادث ذات التأثير الكبير. خلال السنوات الأربع الماضية، شهدت المنطقة العربية تركيز عدد من مراكز المراقبة وتسوية للحوادث على الصعيد الوطني على مدار الساعة طوال أيام الأسبوع (CERT 24/7) وهناك أيضًا إطار عمل ضروري للوقاية من الحوادث السيبرانية والاستجابة لها فيما يتعلق بالخدمات الحيوية للقطاعين العام والخاص.

تعزّز **"الاستراتيجية العربية للأمن السيبراني"** ACSS تطوير إطار إقليمي لإدارة المخاطر الأكثر حدّة. وعليه، فإن مجال التدخّل هو إعداد تحليلات المخاطر وخطط الاستمرارية وجودتها المتقلبة. ويتمثل أحد التحديات التي سيتم تناولها خلال فترة الاستراتيجية الحالية في الوصول إلى مستوى جديد في إدارة المخاطر، والتطبيق العملي للأطر القانونية المعمول بها حاليا، والانتقال إلى حل قائم على القدرات/الكفاءات التي من شأنها التعامل مع الأزمات السيبرانية، وهي القدرات/الكفاءات المحددة من المؤسسات المختلفة، وبالتالي ضمان قدرة الاستجابة المثلى والاستخدام الأكثر فعالية لموارد المنطقة.

تشجع **الإستراتيجية العربية للأمن السيبراني** على إنشاء آليات لتقييم الأثر أو الخطورة لتقدير وتقييم حوادث الأمن السيبراني بناءً على تأثيرها على الأصول والخدمات والبنية التحتية الحرجة والأفراد. يهدف هذا النوع من التقييمات إلى فهم السياق الأوسع للحادث السيبراني، بما في ذلك آثاره المحتملة والفعلية على مختلف القطاعات و / أو المجموعات السكانية وتأثيراتها المتتالية. يجب إجراء مثل هذه التقييمات بالتشاور مع مجموعة واسعة من أصحاب المصلحة بطريقة منفتحة وشاملة وشفافة. يجب دمج التقييمات في الخطط الوطنية للتعافي من الكوارث والطوارئ، ويجب أن تُفيد النتائج في الاستجابة للحوادث الإلكترونية بشكل عام.

سوف تسلّط الإستراتيجية العربية للأمن السيبراني (ACSS)الضوء على الأطر التشريعية والتنظيمية الحالية أو اقتراح تطوير أطر تشـريعية وتنظيمية جديدة تحدد الحد الأدنى من المتطلّبات للأمن السـيبراني لمشـغلي المنشآت الحساسة.

يجب أن تتناول متطلّبات السـلامة والأمن مجموعة من أولويات إدارة المخاطر عالية المسـتوى بالإضـافة إلى ممارسـات الأمن السـيبراني الأكثر تحديدًا ودقّة، مثل تحديد المخاطر السـيبرانية وإنشـاء هياكل حوكمة إدارة المخاطر؛ حماية البيانات والأنظمة عبر بروتوكولات إدارة الوصـول والتدابير الأخرى؛ مراقبة البيئات الرقمية واكتشاف الانحرافات أو الأحداث المحتملة؛ والاستجابة للحوادث والتعافي منها.

عند تطوير هذه المتطلّبات، يجب مراعاة المعايير وأفضـل الممارسـات المعترف بها دوليًا لضـمان نتائج أمنية أفضـل وكفاءة أكبر. يجب وضـع المتطلّبات/الاحتياجات ذات الصـلة عبر القطاعات كنقطة انطلاق، مما يتيح مزيدًا من قابلية التشـغيل البيني وتناسـق/تناغم الممارسـات الخاصـة بالقطاع والامتثال المبسـط للوظائف بين القطاعات.

سـوف تسلّط الإسـتراتيجية العربية للأمن السـيبراني (ACSS) الضـوء أيضًا على أن المتطلّبات الأسـاسـية للأمن السـيبراني يجـب أن تركز على النتـائج لضـمـان مزيـد من المرونـة بمرور الوقـت حيـث أن مجـال المخـاطر والتكنولوجيا مسـتمر في التطور بسـرعة. إن توضـيح الأهداف التي ترمي المؤسـسـات إلى تحقيقها (على سـبيل المثال، "التحكم في الوصـول المنطقي إلى الموارد الهامة") بدلاً من كيفية تنفيذ المؤسـسـات للأمان (على سـبيل المثال، "اسـتخدام المصـادقة متعددة العوامل") يمكن أن يسـمح للحكومة والصـناعة على حد سـواء من بالاسـتفادة من التحسـينات الأمنية المسـتمرة. بالإضـافة إلى ذلك، يمكن اسـتكمال المقاربة القائمة على النتائج لتطوير هذه المتطلّبات، عن طريق التنفيذ من قبل قطاع معيّن / قطاع بعينه أو إرشادات "كيفية"، والتي توفر خيارات لتقديم المعلومات وإدماج ممارسات المؤسسة.

الفصل الثاني: الرؤية، الأهداف، المبادئ والتوجّهات:

يتمثل دور الإستراتيجية العربية للأمن السيبراني في إنشاء نموذج/ إطار تنظيمي قوي ومستقر وفعال للتعاون بين الدول العربية لتمكين تنفذ تدابير الأمن السيبراني القائمة على المخاطر لأصحاب المصلحة المتعددين من أجل حماية الفضاء السيبراني الإقليمي. وتعتمد الشراكة العابرة للحدود التي تم التركيز عليها في هذه الاستراتيجية على رؤية مشتركة تحدّد التوجّهات في تحقيق أهداف الأمن السيبراني وإيجاد مسار موحّد للحفاظ على بيئة تحتيّة رقمية آمنة ومرنة داخل الفضاء السيبراني العربي.

2.1 : رؤية الاستراتيجية العربية للأمن السيبراني

نحو مجتمع عربي آمن-متكامل ومندمج في الاقتصاد الرقمي العالمي ومكتفي ذاتيا في مجال الحلول والخبرات الداعمة للثقة الرقمية والحامية للفضاء السيبراني العربي.

- **مجتمع عربي آمن:** مجتمع عربي آمن من خلال توفير الشروط والمتطلبات الموضوعية لتحقيق الامن السيبراني وتعزيز شعور كافة افراد المجتمع بالأمان
- **متكامل:** شامل ومعتمد على تفاعل كل اصحاب المصلحة.
- **مندمج في الاقتصاد الرقمي العالمي:** من خلال صياغة تدابير السلامة التنظيمية والتقنية اللازمة ضد الأضرار المحتملة على ضوء المعايير وأفضل الممارسات الدولية المعتمدة والمبادئ التوجيهية الواضحة التي تمكن الشركات والفاعلين الاقتصاديين أن تعمل من خلالها بأمان في تطوير منتجات وخدمات رقمية جديدة ومبتكرة تكون جزءا من الاقتصاد الرقمي.
- **محقق للاكتفاء الذاتي في مجال الحلول/البرمجيات:** من خلال وضع الإستراتيجيات التحفيزية لمطوري الحلول/البرمجيات في المنطقة العربية من أجل انتاج وسائل وبرامج للسلامة المعلوماتية محلية الصنع.
- **الخبرات الداعمة للثقة الرقمية:** من خلال وضع البرامج التعليمية والتدريبية المؤهلة للكوادر والإطارات العربية في كل المجالات الداعمة للثقة الرقمية.

- **الحامية للفضاء السيبراني العربي:** الهدف النهائي الاستراتيجي هو حماية الفضاء السيبراني الإقليمي والوطني العربي

2.2 : الأهداف النوعية للإستراتيجية:

بالنظر الى ما تمت الإشارة اليه من تحديات جدية والمخاطر التي تعترض المنطقة العربية والتي تضاعفت نتيجة للأزمة الصحية العالمية "الاستثنائية" سنة 2020، تهدف هذه **الإستراتيجية** إلى:

- خلق آليات تشاركية للاستفادة من سوق الأمن السيبراني في المنطقة
- تطوير قدرات المتخصصين في الأمن السيبراني، وتشجيع المهنيين والطلبة على الانخراط في المجال وبناء القدرات وتطوير منظومة متكاملة في مجال التدريب في الأمن السيبراني
- زيادة وعي أفراد المجتمع بالأمن السيبراني والمخاطر المتعلّقة بالإنترنت، وتشجيع اتباع الممارسات الآمنة في التعامل مع التكنولوجيا الرقمية، وتشجيع المؤسسات على نشر الوعي السيبراني بفاعلية
- تنظيم مسابقات تدعم التميّز في مجال الأمن السيبراني خلال برامج مسابقات عربية، وتشجيع المؤسسات على إطلاق برامج حول الأمن السيبراني، وإلهام رواد الأعمال للابتكار في المجال، ودعم الأبحاث المبدعة والخلاّقة في المؤسسات الأكاديمية، وتنشيط تشجيع الطلبة على الانخراط في مجال الأمن السيبراني
- إنشاء آلية مشتركة لكشف عن حوادث الأمن السيبراني والإبلاغ عنها
- إنشاء منهجية موحدة لتقييم درجة خطورة الحوادث السيبرانية لتوفير الدعم المناسب لها
- بناء قدرات عربية على مستوى عالمي للاستجابة لكل أنواع الحوادث السيبرانية
- تصميم إطار قانوني وتنظيمي شامل للأمن السيبراني لمعالجة جميع أنواع الجرائم السيبرانية، ولحماية التقنيات الحالية والناشئة،
- وضع أنظمة داعمة لتمكين الشركات الصغيرة والمتوسطة وحمايتها من التهديدات السيبرانية.

2.3 : المبادئ التوجيهية

تم تقديم التفاصيل الخاصّة بالمبادئ التوجيهية لهذا الإطار التنظيمي في القسم التالي:

2.3.1 : سيادة القانون

تركز الاستراتيجية على تطبيق سيادة القانون على المستوى الوطني والإقليمي، وتشمل إجراءات وتدابير جوهرية لضمان الحفاظ على حقوق المواطنين في جميع الأوقات بموجب الأطر التنظيمية الوطنية والإقليمية.

2.3.2 : مقاربة أصحاب المصلحة المتعددين

انطلاقا من تركيبة مختلف أنظمة تكنولوجيا المعلومات والاتصالات المنتشرة في الفضاء السيبراني العربي على مستوى الملكية والتشغيل المشترك والمعقّد، وبما أنه لا يمكن للحكومات تحمل المسؤولية بصفة فردية وحصرية لحماية الفضاء السيبراني وحقوق المواطنين على شبكة الانترنت يتحتم على مالكي ومشغلي أنظمة تكنولوجيا المعلومات والاتصالات تحمّل مسؤولية حماية أنظمتهم والمعلومات الخاصّة بحرفائهم/عملائهم.

2.3.3 : المقاربة القائمة على المخاطر

يجب أن تكون التدابير الرامية إلى زيادة مستوى الحماية مرتكزة على تقييم المخاطر والتهديدات التي تواجه المنطقة، ومن هذا المنطلق تعزز الاستراتيجية العربية للأمن السيبراني التقييم المستمر لمخاطر الأمن السيبراني من قبل الأفراد والشركات وهيئات القطاع العام والحكومات ككل، وذلك بهدف تحسين فاعلية ونجاعة الإجراءات الاستباقية والتفاعلية.

2.4 : توجّهات الاستراتيجية العربية للأمن السيبراني

مقترحات لتعزيز الأمن السيبراني على المستوى الوطني

من خلال حصرنا لواقع وتحديات الأمن السيبراني بالدول العربية فإننا يمكن أن نقف على بعض المكاسب والإنجازات التي يمكن أن تمثّل المقومات التي سترتكز عليها الرؤية الاستراتيجية وتتمثل في ما يلي :

- توجهات العديد من الدول العربية نحو اعتماد إستراتيجية وطنية للأمن السيبراني
- توجهات العديد من الدول العربية نحو اعتماد تشريعات عامّة للأمن السيبراني
- أهمية المبادرات العربية في تقريب التشريعات الوطنية العربية من بعضها البعض وتطوير العمل المشترك في مجال الأمن السيبراني
- اعتماد أغلب الدول العربية على أفضل الممارسات التشريعية في العالم سواء في وضع الإستراتيجية أو في وضع التشريعات الوطنية للأمن السيبراني
- تثمين دور مبادرات المنظمات الدولية العالمية والعربية خصوصا/ بالتحديد في بلورة استراتيجيات وتشريعات وطنية ناجعة.

2.4.1: وضع إطار تعاون وعمل مشترك ضمن الاستراتيجيات الوطنية للأمن السيبراني:

في ظل تطوير أغلب الدول العربية لاستراتيجيات وطنية للأمن السيبراني، تهدف الاستراتيجية العربية إلى دعم العمل المشترك والمبادرات الجهوية قصد تحقيق الأهداف الاستراتيجية المطلوب تحقيقها. ويعد تطوير إطار عمل مشترك للتعامل مع الأمن السيبراني هو أولى خطوات العمل نحو تحقيق فضاء رقمي آمن على الصعيد العربي. ومما لا شك فيه أن مسار هذه الاستراتيجية يبدأ بعد أن تحدد كل دولة الرؤية والرسالة الخاصة بها فيما يتعلق بإدارة موضوع الأمن السيبراني وتأثير مخاطره عليها.

ومن أهم وأفضل المرجعيات العالمية في هذا الصدد هو النموذج الإرشادي الذي تم تطويره من قبل الاتحاد الدولي للاتصالات والمتعلق بخطوات صياغة وتطوير إستراتيجيات الأمن السيبراني.
(GUIDE TO DEVELOPING A NATIONAL CYBERSECURITY STRATEGY)
وبمجرد تحديد الرؤية والرسالة ينبغي البدء في إنجاز تحليل الفجوة ما بين الوضع القائم والوضع المرجو الوصول إليه، تمّ تطوير الاستراتيجية لتكون بمثابة خارطة الطريق للإتجاه نحو الوضع المنشود. ويجب أن

تنفذ استراتيجية الأمن السيبراني في إطار من الحوكمة المؤسسية/ المؤسساتية بما يضمن تقليل المخاطر وحسن استغلال الموارد، وتوافق المبادرات والمشروعات مع الأهداف لتقديم المخرجات المنتظرة. كما يجب وضع وتطوير معايير لقياس الأداء خلال كافة المراحل.

كما ينصح، وبشدة، إتباع أحد الأطر العالمية للأمن السيبراني، حيث تمثل هذه الأطر أفضل الممارسات العالمية لإدارة هذا الموضوع الهام. ومن أشهر هذه النماذج، نجد إطار NIST للأمن السيبراني (NIST Cybersecurity Framework) للأمن السيبراني والذي يعمل في إطار خمسة محاور متوازية من أجل إمتلاك القدرات الكاملة لتحقيق الأمن السيبراني وهي:

- تحديد الأصول الرقمية والمخاطر المرتبطة بها
- الحماية والتأمين
- اكتشاف الهجمات السيبرانية
- الاستجابة للحوادث السيبرانية
- التعافي من الحوادث السيبرانية

والجدير بالذكر أن الإطار المذكور هو إطار عام يمكن استخدامه في أي مكان ومن قبل أي قطاع من قطاعات الأعمال المختلفة. كما أنه لا يرتبط بتكنولوجيا محددة بل يتوافق ويتكامل مع عدد كبير جدا من أشهر المعايير والأطر العالمية المرتبطة بالأمن السيبراني. ويجب أن يرتبط تنفيذ هذا الإطار بوجود العديد من الآليات ومنها على سبيل الذكر لا الحصر ما يلي:

- آليات لتحديد الأصول الرقمية الحرجة للمؤسسة
- آليات لتقييم المخاطر
- آليات لدعم مبدأ التحسين والتطوير المستمر

وتدعم الاستراتيجية الاعتماد على آليات حديثة لقياس المخاطر السيبرانية والتي تعمل على الربط بين بيئة الأعمال من جهة والمخاطر السيبرانية التي يمكن أن تتعرض لها الأصول الإلكترونية من جهة أخرى، مثل مبادرة FAIR Institute وفقاً لنموذج Cyber Risk Quantitative Model

2.4.2: دعم البحث والتطوير:

من أهم العوامل والمحاور الداعمة لتحقيق نجاح ملموس في مجال امتلاك القدرات السيبرانية سواء في إطار الدفاع أو الهجوم السيبراني هو عامل البحث والتطوير، ويرتبط مستوى النجاح في تحقيق القدرات

المطلوبة بحجم الانفاق والدعم اللوجستي المتاح للقائمين على البحوث والتطوير في هذا المجال والذي تعددت فروعه وتخصصاته بشكل كبير جدا ومنها على سبيل المثال (الحوسبة السحابية - أنظمة الهواتف المحمولة – النظم والتطبيقات الافتراضية – الأنظمة المدمجة وتطبيقات أنترنت الأشياء).

ومن الواجب في هذا الصدد إلقاء الضوء على فرص التشارك والتعاون المطلوبة بين القطاع الحكومي والقطاع الخاص الذي يمكنه تعزيز استثمارات هذا المجال بما يؤدي إلى تحقيق أهداف عديدة لا تقتصر فقط على دعم البحوث والتطوير وإنما يمكن أيضا أن تنشئ فرص لتطوير حلول وتطبيقات أو سبل تدعم الأمن السيبراني وأيضا تثري سوق التكنولوجيا في البلدان العربية.

يجب على الاستراتيجية العربية للأمن السيبراني تحديد وتقييم بيئة التهديدات السيبرانية المتطورة والتأثيرات والعواقب المحتملة على البنى التحتية الحيوية والخدمات الأساسية. يجب أن تحدّد أولاً البنى التحتية والخدمات الحيوية المحلية للدولة - تلك الأنظمة المادية والسيبرانية/ الافتراضية والأصول التي تعتبر حيوية للأداء السليم للمجتمع والاقتصاد، والتي سيكون لعجزها أو تدميرها تأثير مدمر للأمن المادي أو الاقتصادي أو الصحة العامّة أو سلامة الدولة. يجب إجراء تقييم لطبيعة التهديدات السيبرانية لتحديد التهديدات والمخاطر السيبرانية التي تستهدف البنى التحتية والخدمات الحيوية، وكذلك الأفراد الذين يستخدمونها ويعتمدون عليها، وأيضا للمساعدة في ترتيب أولويات الموارد بغرض حمايتها. مثل هذا التقييم من شأنه أن يساعد أيضًا في مواءمة استراتيجيات إدارة المخاطر الإلكترونية مع خطة إدارة الأزمات في الدولة. يمكن أن يساعد أيضًا في تسخير القدرات اللازمة والأشخاص والتمويل والاستراتيجيات لتعزيز الوضع العام للأمن السيبراني في المنطقة.

2.4.3 : التدريب ورفع الوعي :

تعتمد أي منظومة ناجحة على ثلاثة ركائز أساسية: (الأفراد – الضوابط والسياسات والقوانين – التكنولوجيا). وفي مجال الأمن السيبراني تعد الموارد البشرية/ يعد العنصر البشري من أهم عناصر المنظومة وتكاد تكون الأهم على الإطلاق. فمهما كانت مقدرة المؤسسات والدول على امتلاك تقنيات فائقة التطوّر، سيظل الحصول على أفضل أداء ممكن من هذه التقنيات مرهون/ مرتبط بالقدرات/ الكفاءات القائمة على تشغيلها وإدارتها.

وهنا تكمن الأهمية الكبيرة لإعداد الكوادر وبناء القدرات البشرية. والجذير بالذكر أن العالم يشهد نقصا كبيرا في الكوادر المدربة والمؤهلة لتأمين آلاف التقنيات الموجودة في كل قطاعات الأعمال، مثل : التعليم

والصحة والخدمات الحكومية الإلكترونية والخدمات البنكية بأنواعها المختلفة وأنظمة التحكم الصناعي وشبكات إدارة البينة التحتية الحرجة والتي قد تعد الأخطر على الإطلاق، حيث أن العبث بإعدادات هذه الشبكات أو الاتصال غير المشروع بها قد يؤدي إلى شلل تام بالمؤسسات بل وبالدول أيضا.

وفي هذا الصـدد، يوجد نماذج وأطر عالمية شـهيرة يمكن الاعتماد عليها أو حتى اعتمادها كما هي بسـبب وجود رؤية لإعداد متخصصين في مجالات الأمن السيبراني المختلفة. ولعل أشهر هذه النماذج هو نموذج (NICE- National Initiative for Cybersecurity Education) والذي تم تطويره من قبل المعهد القومي الأمريكي للمعايير القياسـية والتكنولوجيا (NIST). ويحدد هذا الإطار عدد العاملين في مجال الأمن السيبراني ويضع لكل خطّة نوعا من التوصيف الوظيفي بالإضافة إلى القدرات والمهارات المطلوبة لشاغل الوظيفة. وهو ما يمكّن من العمل على إعداد برامج تدريبية متخصصة بغرض إعداد متخصصين فروع الأمن السيبراني المختلفة كوضع مسار واضح لتطوير قدرات العاملين في هذا المجال من المستويات الأولى إلى مسـتويات متقدمة. ولعل أفضـل النماذج العربية في هذا الإطار هو ما قامت به المملكة العربية السـعودية فيما أطلق عليه "الإطار السـعودي لكوادر الأمن السـيبراني (سـيوف) The "Saudi initiative for cybersecurity cadres (swords)

وإذا تطرّقنا إلى العامل/ العنصـر البشـري كأحد أهم العوامل الداعمة لنجاح منظومة الأمن السـيبراني، فإنّ ذلك لا يقتصر على متخصصي ومسؤولي الأمن السيبراني بل يمتد إلى كل فرد في المؤسسة، حيث أنه، ومن الوارد جدا أن يتم اسـتهداف أي مؤسـسـة بالكامل عن طريق أي موظف أو منتسـب لها، أو حتى أي فرد تعامل معها مثل: الموردين والعملاء والشـركاء وأي مؤسـسـة أخرى ترتبط بالهدف المراد اختراقه. ومن هنا تأتي التوعية بمخاطر الأمن السيبراني كعامل شديد الأهمية، حيث أننا دائما ما نتأكّد على أن الحلقة الأضعف في سلسلة أمن المعلومات هي العامل/العنصر البشري.

2.4.4 : تعزيز معايير الحماية والأمن :

يعد اعتماد معايير محددة للأمن السـيبراني كحد أدنى لضـوابط تأمين المنظومات التكنولوجية أمرا هاما. ولذا طورت العديد من دول العالم معايير وضـوابط قياسـية ملزمة لتحقيق حد أدنى من أهداف الأمن السـيبراني، والتي من الممكن تعزيزها ولكن لا يمكن النزول دونها. ومن أشـهر النماذج العالمية في هذا الصدد نموذج الولايات المتحدة الأمريكية.

- FIPS Federal Information Processing Standards
- CC Common Criteria
- NIST 53-800 r5 (Security and Privacy Controls for Information Systems

كما يوجد أيضـــا العديد من النماذج العالمية والتي تمثل معايير عامة لا ترتبط بدولة بعينها وإنما يمكن استخدامها كمرجعيات عامة، وهي تحظى بقبول كل المتخصصين في العالم:

- CIS Controls - Top Critical Controls
- ISO 27001 International Standard for Information Security

ومن الأمثلة/النماذج العربية المميزة في هذا السـياق: الإمارات العربية المتحدة والمملكة العربية السـعودية ودولة قطر، حيث يوجد في كل من هذه الدول ضـــوابط ملزمة لقطاعات الأعمال المختلفة بما يكفل تحقيق حد أدنى من الأمن الســيبراني على مســتوى الدولة بالكامل، كما يؤســس لتطوير ضــوابط أكثر تخصصا أو أكثر قوّة وفي كل قطاع من قطاعات الأعمال، وفق متطلبات التأمين الفعلية.

يجب أن تكون الإســتراتيجية العربية للأمن الســيبراني مصــحوبة بخطة تنفيذ توضــح بمزيد من التفصــيل كيفية تحقيق أهدافها الاســتراتيجية. تحدد خطط التنفيذ الفعالة الهيكل المســؤول عن كل مهمة وكل هدف، والموارد المطلوبة لتنفيذها عبر الزمن المحدد لها (المدى القريب، والمتوســط، والطويل)، والعمليات التي سيتم استخدامها، إلى جانب النتائج المتوقّعة منها.

2.4.5 : التعاون العربي المشترك والمبادرات المشتركة :

إن تبادل الخبرات والمعلومات التقنية المرتبطة بتحليل آليات الاختراق السـيبراني ومحاولة معرفة مصـدره وأهدافه يعد من الأمور الهامة والتي يمكن أن تكون إحدى فوائد ونتائج/ثمار التعاون العربي المشــترك. إذ أن الحصول على المعلومات وتوقيت الحصول عليها هو أمر بالغ الأهمية في اكتشاف الحوادث السيبرانية

أو توقّع حدوثها. وقد يمكّن أيضـا من منعها أو الحد من آثارها. وفكرة التعاون وتبادل المعلومات ليسـت جديدة، ولعل من أقوى وأهم الأمثلة في هذا الصـدد: نموذج حلف شـمال الأطلسـي NATO الذي أنشـأ مركز تميز للدفاع السـيبراني المشـترك من الدول الأعضـاء في الحلف. ويضـم هذا المركز في عضـويته متخصـصـين من 25 دولة مختلفة ويعمل على رصـد التهديدات السـيبرانية التي تتعرض لها أي دولة من دول الحلف، كما يقوم بمحاولات صـدّ هذه الهجمات بالتنسـيق مع كل الدول المعنية من أجل منعها أو التقليل من تأثيرها.

وحتى يكون هذا التعاون مثمر وفاعل فإنه يجب أن يغطي المحاور الثلاثة التالية:

- الأفراد
- السياسات والإجراءات والقوانين
- امتلاك التقنيات والتكنولوجيات المناسبة

كما أنه من الممكن مشـاركة بعض المعلومات التقنية كنتيجة لهذا التعاون مع المراكز البحثية ذات الصلة في الدول العربية بما يعزز قدرتها البحثية وتطوير أدواتها في التصدي للهجمات السيبرانية.

يجب أن تحدد الاسـتراتيجية العربية للأمن السـيبراني تخصـيص الموارد المخصـصـة والمناسـبة لتنفيذها وصيانتها ومراجعتها. ويوفر التمويل الكافي والمتسق والمستمر الأساس لوضع أمن سيبراني وطني فعال. يجب تحديد الموارد من حيث المال الميزانية المخصصة والأشخاص والمواد. كما أن التنفيذ الناجح أيضـا يتطلب إلزاما وقيادة سياسية مدعومة بشراكات موثوقة. ويمكن البناء على المبادرات الجهوية التي سبق اقتراحها وتعزيزها من بعض الأطراف على غرار المركز العربي الإقليمي للأمن السـيبراني للاتحاد الدولي للاتصـالات التي تستضيفه سلطنة عمان والذي تم انشاءه في عام **2013.**

لا ينبغي النظر إلى الأهداف والمهام في إطار هذه الاسـتراتيجية على أنها تتطلب تخصـيصـا للموارد لمرّة واحدة، حيث يجب مراجعة متطلّبات الموارد بصـفة دورية بناء على نسـبة التقدّم والعراقيل العرضـية في تنفيذ البرامج والمهام والأهداف المدرجة داخلها.

قد تنظر الحكومات أيضـا في إنشـاء ميزانية مركزية للأمن السـيبراني تدار بواسـطة آلية حوكمة مركزية للأمن السـيبراني. وسـواء تم تجميع مصـادر تمويل متباينة في إطار برنامج متماسـك ومتكامل أو إنشـاء

ميزانية بين مختلف أطراف الحكومة، يجب إدارة البرنامج الشامل ومتابعته من خلال وضع مراحل رئيسية لضمان التنفيذ الناجح للإستراتيجية العربية للأمن السيبراني.

2.4.6 : إنشاء وتطوير المراكز الوطنية للاستجابة للحوادث السيبرانية

تعتبر المراكز الوطنية للاستجابة للحوادث السيبرانية بمثابة خط الدفاع الأول أو وحدات الكشف المبكر عن الهجمات السيبرانية. وتلعب دورا هاما في محاولة تحديد مصادر هذه الهجمات وأهدافها ومحاولة تحليل أساليب عملها والثغرات المستهدفة بهذه الهجمات، وفي أقل التقديرات ينبغي أن يكون هناك على الأقل مركزا واحدا على مستوى الدولة ويفضل التنسيق بين هذا المركز والمراكز المشابهة والتي تعمل في نطاق محدود على مستوى مؤسسة بعينها أو إحدى الوزرات. كما ينصح بإنشاء مراكز متخصصة على مستوى قطاعات الأعمال المختلفة مثل: قطاع الصحة أو الاتصالات أو قطاع البنية التحتية الحرجة، ... حيث يوجد متطلبات نوعيّة تختلف من قطاع إلى آخر كما تختلف أولويات الهجمات السيبرانية ووسائلها وأهدافها من قطاع إلى آخر ومن مؤسسة إلى أخرى. وتوجد مراكز الاستجابة للحوادث السيبرانية بالعديد من الدول العربية ولكنها تتفاوت في مقدرتها وإمكانياتها كما أنها تكاد تفتقد لأليات التعاون العربي المشترك ولتبادل الخبرات والمعلومات.

وفي عدد من الدول لا يوجد مثل هذه المراكز وهو ما يتطلب بالضرورة وضع خطة عاجلة لدعم إنشاء المراكز الوطنية للاستجابة للحوادث السيبرانية بهذه الدول وكذلك تدريب العاملين بها.

وهناك العديد من المرجعيات الدولية التي يمكن الاستعانة بها في هذا الصدد وعلى رأسها إصدارات الاتحاد الدولي للاتصالات المتعلقة بهذه المراكز وأيضا المركز الأوروبي للأمن السيبراني (ENISA)

وكذلك المعهد القومي للمعايير القياسية والتكنولوجيا بالولايات المتحدة الأمريكية.

يجب أن تعكس الاستراتيجية العربية للأمن السيبراني فهما للتبعيات / الارتباط الذي تملكه الحكومات على القطاع الخاص وأصحاب المصلحة غير الحكوميين المحليين (والعكس بالعكس) في تحقيق نظام بيئي/ إيكولوجي أكثر أمنا وأمانا ومرونة (مبدأ الشمولية والاندماج). ولهذه الغاية يجب على الاستراتيجية توضيح كيفية إشراك الحكومات لأصحاب المصلحة المختلفين وتحديد أدوارهم ومسؤولياتهم.

على سبيل المثال، يجب أن تحدد الإستراتيجية شبكة من نقاط الاتصال الوطنية الرسمية للصناعات الحيوية الضرورية لتشغيل واستعادة الخدمات والبنى التحتية الحيوية والحرجة. يجب أن تتماشى الاستراتيجية العربية للأمن السيبراني مع الأولويات الوطنية الأخرى، مثل ضمان أن يكون النفاذ منخفض التكلفة ومتاحا وشاملا؛ تعزيز حماية البيانات والخصوصية مع تعزيز الابتكار؛ تعزيز قدرة البنى التحتية

على الصمود وتوفر الخدمات للكوارث وتغيير المناخ والأوبئة؛ استكشاف تكنولوجيات جديدة مثل الذكاء الاصطناعي و سلسلة الكتل والتحليل الكمي.

2.4.7 : تعزيز مناهج الأمن السيبراني الموجهة نحو سوق الشغل :

إلى حد بعيد، توجد فجوة كبيرة بين ما يدرسه طلاب الجامعات من التخصّصات التقنية أو في مجال أمن المعلومات، إن وجد كتخصص أكاديمي، وبين احتياجات سوق العمل الفعلية.
وسوف يكون التوجه نحو توفير تخصصات دراسية مرتبطة بعلوم الأمن السيبراني أحد الخطوات الهامة لتوفير كوادر مدربة لسد العجز الشديد بين احتياجات سوق الشغل/ العمل وعدد الأفراد المؤهلين بشكل مناسب لشغل هذه الوظائف. حيث يمكن توفير أعداد كبيرة مدربة بشكل جيد في فترة زمنية قصيرة وأيضا بتكلفة قليلة بالمقارنة مع تكاليف التدريب المتخصص أو الدورات المعتمدة عالميا والتي عادة ما يصل سعرها إلى بضعة آلاف من الدولارات للدورة الواحدة لكل متدرّب.
كما يمكن أيضا تطوير محتوى يقوم على إعداده والإشراف عليه نخبة من الأكاديميين والمهنيين من أجل إنتاج مناهج دراسية بتكاليف مناسبة لإعداد أجيال من المتخصصين في الأمن السيبراني للوفاء بمتطلبات سوق العمل/الشغل في المنطقة العربية من ناحية ومن ناحية أخرى لدعم جهود البحث العلمي في هذا المجال الهام. وباستثناء عدد محدود للغاية من الجامعات العربية فإن الغالبية العظمى منها تفتقد وجود تخصصات متعلقة بالأمن السيبراني وربما أيضا لبعض المواد الدراسية المتعلقة بهذا المجال.

2.4.8 : تحديث أطر حوكمة الأمن السيبراني :

إن من أكبر المشاكل والتحديات التي تواجه معظم الدول العربية هي عدم وجود تحديد لمفهوم الأمن السيبراني وكذلك تحديد أين تقع مسؤوليات تأمين المعلومات والنظم فقد تكون مسؤولية تكنولوجيا المعلومات هي مسؤولية شخص واحد داخل مؤسسة أو فريق عمل تابع لإدارة تكنولوجيا المعلومات، وفي حالات نادرة ما تكون إدارة الأمن السيبراني إدارة موجودة ولها تبعية مباشرة للإدارة العليا.

ويمثل هذا النموذج الأخير أفضل الممارسات العالمية في هذا الصدد. وحين يتعلق الأمر بوضع رؤية موحدة للدول العربية بخصوص الأمن السيبراني، فإنه من الضروري أن يكون هناك بكل الهيئات والمؤسسات التابعة للدولة إدارة خاصة بأمن المعلومات ولها مهام واضحة ومحددة بالإضافة إلى تشكيل هيكل إداري بهذه الإدارة بتوصيف وظيفي مناسب حتى يكون لكل مؤسسة إدارة تعمل على تأمين كل ما لديها من أجهزة

رقمية وشبكات. وتخضع هذه الإدارة والعاملين بها لتقييم الأداء من خلال مؤشرات أداء محددة وتكون في حالة تطوير وتحسين مستمر. ويجب أن تكون ت هذه الإدارة تابعة لأعلى سلطة داخل المؤسسة بما يدعم أدواتها التنفيذية لتفعيل سياسات وأدوات وضوابط الأمن السيبراني.

الفصل الثالث: خطّة عمل الاستراتيجية العربية للأمن السيبراني

البرامج المقترحة للإستراتيجية العربية للأمن السيبراني

بناء على التحليل الذي تم القيام به في الفصل الفارط، تم تحديد سبعة حزم عمل من أجل تنفيذ ناجح للإستراتيجية العربية للأمن السيبراني (الرسم البياني رقم 6) ....

تمكّن الإجراءات المحددة في حزم العمل هذه التنفيذ الفعال لرؤية الاستراتيجية العربية للأمن السيبراني مع مراعاة مرونة مكوّنات الفضاء السيبراني العربي، والسيادة الرقمية للدول الأعضاء فضلا عن استدامة الضوابط الأساسية المتعلقة بها.

الرسم البياني 6: حزم عمل *Work packages* الاستراتيجية العربية للأمن السيبراني

تتضمن حزم العمل المذكورة أعلاه مجموعة من الإجراءات مفصّلة في الجدول التالي.

حزمة العمل 1 /WP1 :تطوير إطار موحد لتقييم الأمن السيبراني	تقديم منهجية موحدة لتحديد وقياس مستويات النضج للأمن السيبراني
	تطوير هيكلية إطار الأمن السيبراني الإقليمي
	تقديم سياسة لتحديد النتيجة المستهدفة لكل وظيفة وفئة
	تصميم منهجية ترتيب scoring للأمن السيبراني
حزمة العمل 2: تعزيز التدريب ورفع الوعي في مجال الأمن السيبراني	إعداد مناهج للأمن السيبراني للمؤسسات
	إعداد مناهج للأمن السيبراني للجامعات
	تطوير مواد الدروس ونشر وتنفيذ الدورات التدريبية عبر الانترنت
	وضع سياسة توعية إقليمية للأمن السيبراني
	إنشاء إرشادات منهجية لتقديم دورات الأمن السيبراني عبر الانترنت
حزمة العمل 3: إنشـــاء وتطوير فريق إقليمي-عربي للاســـتجابة لحوادث الأمن الســـيبراني/ الحوادث السيبرانية CSIRT	إعداد مسح/ جرد للمجموعات/ الفرق الوطنية والقطاعية: CSIRT / CERT / CIRT
	إنشاء مخطط للتنسيق بين أصحاب المصلحة الذين تم تحديدهم من خلال الإجراء السابق
	تحديد خطط الاستجابة للحوادث الإقليمية
	تحديد احتياجات فريق CSIRT الاقليمي من حيث الموارد البشرية والمعدات/الأجهزة والبرمجيات HW/SW components وكذلك التمويل
	إنشاء CSIRT العربي

حزمة العمل 4: تعزيز المطابقة للمعايير الدولية	إعداد جرد/مسح لمعايير الأمن السيبراني المعتمدة في المنطقة
	تحديد التآزر والتركيبات البديلة بين المعايير المعتمدة
	تقييم الفجوات من حيث اعتماد المعايير ونضجها
	وضع خارطة طريق لاعتماد معيار الأمن السيبراني
	تصميم وتنفيذ آليات الاشراف على خارطة طريق تبني المعايير
حزمة العمل 5: تعزيز نضج الهياكل المؤسسية والإدارية	تحديد سياسات تقييم الأمن السيبراني للمؤسسات والإدارات
	تجميع نتائج التقييم وتحديد الفجوات
	وضع استراتيجية لتحسين نضج الأمن السيبراني بالمؤسسات والإدارات
	إجراء تقييم مستمر للأمن السيبراني لتنفيذ رؤية مستدامة
حزمة العمل 6: دعم البحث والتطوير في الأمن السيبراني	تحليل تأثير ظهور الحوسبة الكميّة quantum computing على سرية البيانات الحساسة في الفضاء السيبراني العربي.
	تعزيز تطوير حلول الثقة الصفرية zero-trust لمعالجة المشاكل الإقليمية
	مرافقة المبادرات البحثية التي تتناول حماية إدارة البيانات وحركة البيانات
	تنظيم مؤتمرات إقليمية للأمن السيبراني لخلق تآزر بين دوائر البحث العربية
	تنظيم هاكاثوناتHackathons الأمن السيبراني الإقليمية لتحديد وتسريع الشركات الناشئة المبتكرة في مجال الأمن السيبراني
حزمة العمل 7: تطوير إجراءات/ أطر قانونية موحدة	إجراء دراسة حول تشريعات الأمن السيبراني في المنطقة العربية
	تنظيم مؤتمرات لمناقشة تأثير ابتكارات الأمن السيبراني على الأطر التنظيمية
	تطوير تدابير تنظيمية للأمن السيبراني لتعزيز الاقتصاد الرقمي الإقليمي

3.1: حزمة العمل 1: تطوير إطار موحد لتقييم الأمن السيبراني:

من خلال التحليل الذي تم تقديمه في الفصل الثاني/2 تم التوصّل إلى أن الفجوة على مستوى النضج في مجال الأمن السيبراني هي موجودة بشكل ملحوظ.

ولذلك، فإن اعتماد إطار تقييم إقليمي هو من بين التدابير الهامّة التي من شأنها تقليل هذا التفاوت والحد من هذه الفجوة.

والغاية هي تطوير نسخة خاصّة من إطار الاستئناس بالمعايير الدولية وخاصة الأمن السيبراني (CSF) للمعهد الوطني للمعايير والتقنية NIST والتي تأخذ بعين الاعتبار المميّزات الخاصة بالمنطقة العربية. ولهذا من البديهي إنشاء فريق عمل تقني يسهر على إعداد رؤية مشتركة فيما يخص/ فيما يتعلق بالمجالات التالية:

- منهجية موحدة لتحديد وقياس مستويات النضج الخاصة بالأمن السيبراني
- هيكلية لإطار إقليمي للأمن السيبراني (المهام، الفئات/الأصناف، الفئات الفرعية/ الأصناف الفرعية)
- سياسة لتحديد النتيجة المستهدفة لكل وظيفة وفئة
- تصميم منهجية ترتيب scoring للأمن السيبراني

سيؤدي إطار العمل العربي الموحد للأمن السيبراني إلى مواءمة مؤسسية/التوافق المؤسسي للأهداف الخاصّة بتحمّل المخاطر، مما سيؤدي إلى تحسين كفاءة تكلفة البرامج الوطنية للأمن السيبراني. سيسمح هذا أيضًا بتواصل أفضل في/داخل المشهد الإقليمي للأمن السيبراني. ومن ثم، سيتم إنشاء مجموعة من الأدوات القابلة لإعادة الاستخدام في إطار الإستراتيجية العربية للأمن السيبراني لتسهيل التنفيذ الملموس لإطار عمل الأمن السيبراني العربي الموحد.

3.2: حزمة العمل 2: تعزيز التدريب ورفع الوعي في مجال الأمن السيبراني:

من أجل التعامل المجدي مع تطوّر الجوانب التقنية للأمن السيبراني، يجب على الدول أن تنذل المزيد من الجهود في برامج تدريبية متقدّمة في إطار مفتوح يدعم المبادرات التشاركية الهادفة إلى معالجة التحديات الإقليمية. وفي الواقع، فإن قلة وندرة الموارد البشرية المؤهّلة تعتبر من بين التحديات والعقبات الرئيسية أمام تنفيذ وتطبيق إستراتيجيات وسياسات الأمن السيبراني. وبالتالي، يجب أن تتمتع البرامج التدريبية بالخصائص التالية:

1- **التغطية الواسعة/الشاملة:** يجب أن تغطي برامج التوعية الخاصّة بالأمن السيبراني أكبر عدد ممكن من المواطنين بغض النظر عن وضعهم الاجتماعي أو الإداري.

2- **الاستمرارية:** تعتمد برامج التدريب بشكل كبير على القدرة على تنظيمها بشكل متواصل ومستمر وتكييفها مع التحديات المحدثة في مجال الأمن السيبراني. ولذلك، فإن المراجعة المستمرّة للمناهج التدريبية والشهائد المعترف بها للجهات التدريبية، سوف يتم النظر فيها في إطار هذه الاستراتيجية العربية للأمن السيبراني.

3- **التغطية الأساسية:** يجب أن تنشر برامج التدريب والتوعية الخاصّة بالأمن السيبراني المعرفة بخصوص الموضوعات الأساسية مثل: أمن كلمات السر/المرور PSW وتقنيات مكافحة التصيّد الإحتيالي anti-phishing techniques والتصيّد بالرمح spear phishing ، والهندسة الاجتماعية.

i. **أمن كلمات السر/المرورPSW :** يجب أن يتم توضيح أهمية كلمات السر/ المرور للمواطنين وتدريبهم على إنشاء كلمات سر/مرور قوّة ذات طابع قوي تتضمّن على الأقل حرف أو رمز فريد one unique character وتجنّب كتابة كلمات السر على الملاحظات اللاصقة أو مشاركتها مع الزملاء.

ii. **مكافحة هجمات التصيّد الاحتيالي:** من خلال رفع الوعي يمكن للتجارب المتعدّدة مساعدة المواطنين/ المستعملين على اكتشاف رسائل البريد الضارّة والإبلاغ عن الرسائل الخبيثة؛ وهذا من شأنه أن يقلّل من هجمات التصيّد الاحتيالي. يجب أن يكون المستخدم حذرا من رسائل البريد الالكتروني المتأتية من مصادر غير معروفة. إذ تستخدم رسائل البريد الإلكتروني في عمليّات التصيّد الاحتيالي للوصول إلى الأنظمة وإحداث اضطرابات. وتشتمل ممارسات الأمان والسلامة موضوعات مثل الروابط والمرفقات الضارة. ومع رفع الوعي بالأمن السيبراني، والدورات التدريبية المتواصلة يمكن للموظفين تطوير وتحسين فهمهم بشكل كبير لهذه الهجمات.

iii. **الهندسة الاجتماعية:** تزيد ممارسات التوعية بالأمن السيبراني من الوعي بالمخاطر من قبل كل فرد في المؤسسة، كالتلاعب بالموظفين من أجل الوصول إلى الأنظمة أو الكشف عن معلومات سريّة لفائدة مؤسسات/منظمات أخرى.

ويمكن أن يساعد التدريب للتوعية الأمنية أيضا في تحديد وإصلاح أية ثغرات ونقاط ضعف في الشبكات وأنظمة الكمبيوتر. وتساعد ممارسات التوعية الأمنية من إعطاء المؤسسات والموظفين أفضل فرصة لتجنّب هجمات الهندسة الاجتماعية.

4- **اختبارات ما بعد التدريب:** من الضروري أن يكون هناك أداة لقياس كفاءة مبادرات التدريب والتوعية التي سيتم تنظيمها في المنطقة العربية. على سبيل المثال، يعد إجراء تمارين التصيّد الاحتيالي أحد الممارسات المستعملة على نطاق واسع والتي تمكن من تقييم كمّي للمخاطر المرتبطة بنقص الوعي. ويجب إعطاء المستعملين الذي يتعرضون لمخاطر كبيرة بعد تمرين التصيد phishing تدريبا إضافيا متماشيا مع السياق من أجل معالجة الثغرات والفجوات التي تم تحديدها خلال الاختبار.

ويعد الاكتشـاف المبكّر للثغرات الأمنية المتعلقة بالتصـيد الاحتيالي بغاية الأهمية من أجل تنوّع السـيناريوهات الهجومية التي تعتمد على استغلال ناجح للتصيّد الاحتيالي.

5- **النشـروالتعميم:** تحتاج الحكومات والمؤسـسـات التي تأوي خدمات حسـاسـة في الفضـاء السـيبراني العربي لغرس ممارسـات الأمن والسـلامة. ومن المهم أن يفهم الموظفون أدوارهم ومهامهم في برامج ومبادرات الأمن السـيبراني التي يشاركون فيها.

وتنقسم المبادرات المقترحة في هذا المجال إلى صنفين:

- دورات تكوينية تهدف إلى الرفع من قدرة الأطراف الفاعلة على حماية الفضاء السيبراني العربي
- دورات توعوية تهدف إلى الحد من الثغرات الناجمة عن سوء استعمال الوسائل الرقمية

بالإضـافة إلى ذلك، غالبا ما تشـكل نتائج اختبارات وتدقيق وتمارين الأمن السـيبراني مادة خام قيّمة يمكن استخدامها لتعلّم الدروس وزيادة الوعي. ولهذا الغرض، فإن إنشاء تصميمات إقليمية للاتصال تعتبر من أهم الإجراءات في إطار الاسـتراتيجية العربية للأمن السـيبراني. ويتنزل تأطير الدورات التكوينية والتوعوية ضـمن الأولويات الاستراتيجية على الصعيد العربي من خلال النقاط التالية:

1. إجراء تحليل الفجوة لاحتياجات سوق العمل والمخرجات التعليمية
2. .موائمة مناهج التعليم لتلبية احتياجات سوق العمل
3. .تطوير نموذج وطني لمجموعة مهارات الأمن السيبراني لكل وظيفة في الأمن السيبراني
4. .إجراء تحليل الفجوة للعاملين في مجال الأمن السيبراني
5. .تنفيذ برامج تدريبية لسد فجوة مهارات الأمن السيبراني
6. .اعداد برامج توعية عن العمل الحر في الامن السيبراني
7. تنفيذ تمارين سيبرانية إقليمية

3.3: حزمة العمل 3: إنشـاء وتطوير فريق إقليمي-عربي للاسـتجابة لحوادث الأمن السـيبر اني/ الحوادث السيبر انية CSIRT:

من أجل تحسين قدرة وإمكانيات الدول العربية في التعامل مع حوادث الأمن السيبراني، تشجع الاستراتيجية العربية للأمن السيبراني على إنشاء فريق إقليمي-عربي للاستجابة لحوادث الأمن السيبراني Arab CSIRT والذي من شأنه إدارة حوادث الأمن السيبراني وتخفيفها بشكل فعال، وإجراء عمليّات تحليل الحوادث، وتوفير معلومات الحماية وخدمات التوعية الظرفية. وسيكون هذا الفريق إطارا للتعاون بين مختلف الفرق العربية الفاعلة في هذا المجال.

كما تشمل قدرات الفريق الوطني CSIRT في الكشف عن حوادث الأمن السيبراني والتعامل معها بشكل منهجي لبناء الثقة في الخدمات الرقمي في القطاع العمومي والقطاع الخاص في المنطقة.

فريق الاستجابة للحوادث السيبرانية CSIRTهو مجموعة من المتخصصين في تكنولوجيا المعلومات الذين يزودون المؤسسة بالخدمات والدعم المتعلّق بتقييم وإدارة ومنع/ التصدي للطوارئ الطوارئ المتعلّقة بالأمن السيبراني، إلى جانب تنسيق المجهودات الخاصة بالاستجابة للحوادث السيبرانية.

ويعتبر CSIRT هيئة منظمة لها مهمّة محددة وهيكلية وأدوار ومسؤوليات. ويستثني هذا أية نشاط خاص ad hoc أو غير رسمي للاستجابة للحوادث السيبرانية والذي لا يملك مؤيّدات محددة أو أدوار ومسؤوليات موثّقة.

1- إستلام تقرير الحوادث السيبرانية من أحد المكوّنات constituent : من أجل استلام تقرير من فريق CSIRT يجب على المتلقي لخدمات الاستجابة للحوادث أن يكون على علم بوجود هذا الفريق وأيضا المهام المنوطة بعهدة هذا الفريق وكيفية الوصول إلى خدماته، بالإضافة إلى مستويات الخدمة والجودة التي يتوقعها. وبالتالي يحتاج فريق CSIRT إلى تحديد مهمّته وخدماته والاعلان عنها لعملائه المستهدفين، ونشر إرشادات حول كيفية طلب خدمات الحوادث. ويشمل هذا نشر سياسة الاستجابة للحوادث، والعمليات، والإجراءات والنماذج والموارد اللازمة لإعلام وتمكين العملاء المستهدفين من تقديم تقارير الحوادث السيبرانية.

- تحليل تقرير الحادث للتحقق من صحّته وفهمه. بمجرد استلام تقرير الحادث، يقوم فريق CSIRT بتحليله من أجل التحقق من وقوع حادث أو أي نوع آخر من الأنشطة التي تقع ضمن مهامه. ثم يقوم الفريق بتحديد مدى فهمه للتقرير وللحادث وإذا ما كان هذا الفهم جيدا كفاية للشروع في تحديد إستراتيجية استجابة تتماشى مع الأهداف الخاصة باستعادة السيطرة/ التحكّم وأيضا تقليل الأضرار. ومن بين الأمور الهامة التي يجب أن تتوفر للقدرة على تحليل تقرير الحادث والاستجابة بكفاءة هو وجود موظفين قادرين على أداء مجموعة متنوعة من المهام. يجب أن يكون لأعضاء CSIRT خطط وسياسات مكتوبة توثق أدوارهم ومسؤولياتهم بكل دقّة.

2- تقديم دعم الاستجابة للحوادث: إعتمادا على هيكلية CSIRT والخدمات التي يقدّمها، يجب أن يوفر دعم الاستجابة للحوادث عن طريق التالي:

- تقديم خدمات الاستجابة للحوادث في الموقع للمستفيدين الرئيسيين
- خدمات الاستجابة للحوادث عبر الهاتف أو البريد الالكتروني، أو
- خدمات الاستجابة للحوادث المنسقة التي تجمع وتحدّد جهود فرق الاستجابة للحوادث المتعددة المستفيدين الرئيسيين

قد تستخدم المؤسسات واحدا أو أكثر من الأنواع الرئيسية لفرق الاستجابة للحوادث على غرار: CSIRTsو SOCs وCERTs . في بعض الأحيان يتم استخدام هذه المصطلحات بشكل مترادف، على الرغم من وجود ختلافات، وفقا لاستخدامات المؤسسة للمصطلح (المصطلحات).

والأكثر تميّزا بين الثلاثة هو مركز العمليات الأمنيّة/ مركز عمليات الأمن Security Operation Center (SOC) . هذه المنشأة المخصّصة تراقب وتدافع عن التكنولوجيا والأجهزة وتعمل كمركز تحكّم وقيادة في المنطقة. فهو يحمي الشبكات والخوادم والتطبيقات والأجهزة الطرفية endpoints. ومع ذلك فإن مسؤوليات مركز العمليات الأمنية تمتد إلى ما هو أبعد من مجرّد الاستجابة للحوادث.

غالبا ما يتم استخدام CSIRT, CERT وفريق الاستجابة لحوادث الكمبيوتر الأقل استخداما (CIRT) بالتبادل. بشكل عام، CSIRTs, CERTs and CIRTs تتعامل مع الاستجابة للحوادث، بالرغم من أن مهامهم المحددة قد تختلف من مؤسسة إلى أخرى. ويجب تحديد المصطلحات المستخدمة من قبل المؤسسة بشكل يتلاءم مع الأهداف و الهيكليّة واستخدام الموارد اللازمة للاستجابة للحوادث بشكل ملائم.

والجدير بالذكر هنا أن CERT هي علامة تجارية مسجلة لجامعة كارنيجي ميلون Carnegie Mellon University (CMU). ويجوز للمؤسسات/المنظمات استعمال علامة CERT بعد الحصول على الترخيص/ الرخصة. ومع ذلك، فإن بعض المنظمات/المؤسسات، على الأرجح غير مدركة أنها علامة تجارية – وتستخدمها لتعريف/ لتحديد فرق الاستجابة للحوادث الخاصة بها.

وتأخذ الاستراتيجية العربية للأمن السيبراني ACSS في الاعتبار آليات عمل مشترك لمبادرة **فريق إقليمي-عربي للاستجابة لحوادث الأمن السيبراني** regional CSIRT

- تجميع ونشر تنبيهات الأمن السيبراني (نقاط الضعف، المخاطر والحوادث، ...)، وتدابير التحايل لتجنب التهديدات، والمبادئ التوجيهية وأفضل الممارسات
- بناء قاعدة بيانات موحدة للمعلومات الخاصّة بالحوادث على الصعيد الإقليمي

- المساهمة في معالجة الحوادث التي تؤثر على الحكومات والبنى التحتية الحساسة/ الحيوية
- إدراج مبادرة CSIRT الإقليمي في الشبكات العالمية لـ CSIRT
- تنسيق الإجراءات التفاعليّة وإدارة الأزمات مع أصحاب المصلحة الرئيسيين المشاركين في الاستجابة للحوادث
- تنظيم تمارين الأمن السيبراني الإقليمية مع فرق CSIRT الوطنية والقطاعية
- إنشاء بنية تحتية تقنية لجمع وتحليل البيانات المتعلّقة بالحوادث السيبرانية
- نشر تقارير ودراسات حول التهديدات والمخاطر التي تهدد الأمن السيبراني في المنطقة العربية

3.4: حزمة العمل 4: تعزيز الامتثال للمعايير الدولية:

تشجع الاستراتيجية العربية للأمن السيبراني ACSS اعتماد آليات الامتثال العالميّة للأمن السيبراني التي تأخذ بعين الاعتبار خصائص المنطقة العربية من حيث الثقافة، البنى التحتية، والجاهزية.

وتهدف هذه الآليات إلى توفير إطار عمل موحد لحماية الفضاء السيبراني من مصادر الثغرات نقاط الضعف الأمنية التي قد توجد في المعدات والأجهزة ومكونات البرامج التي تُبنى عليها أنظمة المعلومات والاتصالات. سيؤدي إنشاء إطار امتثال عربي مشترك للأمن السيبراني العربي المشترك إلى تحسين نضج الخدمات المنتشرة في الفضاء الرقمي العربي إلى حد كبير وإنشاء مستوى واضح من الفهم لجميع أصحاب المصلحة المتعاملين في الفضاء السيبراني فيما يتعلق بتبني المنتجات وعمليات التصديق. وبالتالي، فإن الخصائص الأمنية للخدمات الرقمية المنفذة في المنطقة العربية سوف تتماشى مع المعايير الدولية وأفضل الممارسات.

3.5 : حزمة العمل 5: تعزيز نضج الهياكل المؤسسية والإدارية :

تشجع **الاستراتيجية العربية للأمن السيبراني** (ACSS) على تطوير القدرات العربية لتنفيذ إطار حوكمة فعال للأمن السيبراني. لا يمكن تحقيق ذلك دون تحسين نضج الهياكل المؤسساتية والإدارية الرئيسية، التي تشارك وتساهم بشكل كبير في التنفيذ العملي لاستراتيجيات الحكومة الإلكترونية وكذلك إنشاء البنية التحتية للاقتصاد الرقمي. يتم تأكيد هذه الحاجة من خلال حقيقة أن بعض المؤسسات الحكومية والإدارية تدير عمليات الأمن السيبراني الوطنية الرئيسية مثل تحديد الهوية الإلكترونية والتحقيق الرقمي والثقة الرقمية والتدقيق الأمني. تعد هذه المسارات في جوهرها متعددة التخصصات ويجب أن تشمل التدريب

والتعليم لمجموعة من أصحاب المصلحة المشاركين في مكافحة الجريمة الإلكترونية (مثل القضاة والمدعين العامين والمحامين ومسؤولي إنفاذ القانون والمتخصصين في الطب الشرعي والمحققين الماليين وغيرهم).

يجب أن تتلقى هاته الفئة من أصحاب المصلحة تدريباً متخصصاً وبناء لقدراتهم المؤسسية لتفسير وتطبيق ضوابط الأمن السيبراني المحلية لاكتشاف الجرائم السيبرانية وتحليلها والتحقيق فيها والتعامل معها بشكل فعال.

ومن أجل تعزيز مستوى جاهزية الأمن السيبراني لهذه الهياكل الرئيسية، وبالتالي تحسين مرونة الفضاء السيبراني ، يجب إجراء مثل هذا التدريب والتعليم بشكل مستمر ليغطي الجوانب الفنية والإدارية والتنظيمية للحوادث الأمنية.

وتوصي الاستراتيجية العربية للأمن السيبراني باستمرارية تحديث الإجراءات الداعمة الهادفة لتحسين جاهزية الأمن السيبراني لدى الهياكل الإدارية والمؤسسية لتظل متماشية مع التطوّر الذي تشهده التحديات والتهديدات. ومن هذا المنطلق، يجب أن تأخذ هذه الإجراءات في الاعتبار محتوى حزم العمل الأخرى، لا سيما فيما يتعلق ببناء القدرات وزيادة الوعي.

3.6: حزمة العمل 6: دعم البحث والتطوير في الأمن السيبراني:

يعد البحث والتطوير من بين الركائز الرئيسية/ الأساسية والتي من المتوقع أن تمكن من نشر الحلول السيادية في جميع أنحاء المنطقة العربية. يجب على الدول بذل الجهود لتوفير التدريبات المناسبة والمرافق وخطط التمويل وإدارة المشاريع لتعزيز البحث والتطوير في مجال الأمن السيبراني. وتدفع الاستراتيجية العمل المشترك قصد تحفيز المؤسسات والمنظمات لتطوير حلول عربية لمجابهة التحديات الإقليمية المتعلقة بالأمن السيبراني.

تعد إدارة مخاطر الأمن السيبراني أحد المجالات التي يجب بذل جهود هامّة فيها من حيث البحث والتطوير. خلال العقد الماضي، دخل الذكاء الاصطناعي وخوارزميات التعلم الآلي Machine Learning إلى البنى التحتية الحيوية والمؤسسات وأنظمة المعلومات.

وقد ساهم هذا بشكل أساسي في التغلب على مشكلات الأتمتة ولضبط المزيد من الوظائف الكلاسيكية مثل اكتشاف التسلل intrusion detection وموازنة الحمل load balancing وجدولة المهام. tasks scheduling

وبالإضافة إلى الأتمتة، فتحت البنى التحتية الحيوية للشبكات الخارجية التي سهّلت التحكم في الأنظمة والتشخيص والصيانة بفضل الوصول عن بُعد إلى البيانات المحلية وتحليلها. إلا أنه، مع انفتاحها على الشبكات الخارجية، أصبحت البنى التحتية الحيوية فريسة للقراصنة والاستخدام الخبيث. وهذا يعني أن

إضافة واجهات اتصالات جديدة والاعتماد على الذكاء الاصطناعي لأتمتة المهام خلقت تهديدات جديدة وأبرزت نقاط الضعف الموجودة.

في الواقع، هذه الخروقات ليســت فقط هدفًا لهجمات تقنيات المعلومات الكلاســيكية مثل تعطيل الخدمة (DoS)، ولكنها أصبحت أيضًا هدفًا لهجمات متطورة ومعقّدة جديدة مثل استخدام نماذج المغارمة التوليدية generative adversarial models لإفشال خوارزميات التعلم الآلي ، أو الاعتماد على برامج الفدية و طلب مبالغ طائلة مقابل الحفاظ على خصــوصــية البيانات المجمعة. ونظرًا لأن أمان البنى التحتية الحيوية أمر إلزامي لســلامة المســتخدمين، أصــبح من الضــروري تقييم مخاطرها والتخفيف من حدتها ابتداء من مرحلة تحديد مواصفات الأنظمة حتى تركيزها وأيضا وأثناء دورتها الحياتية. في الواقع، تعمل إدارة المخاطر على تحديد التهديدات ونقاط الضعف، والتنبؤ بتأثيرها على بنية النظام، والبيانات والأعمال ذات القيمة (على سبيل المثال، صورة العلامة التجارية وثقة العميل) ثم التخفيف منها.

ويشــمل تخفيف المخاطر اقتراح تدابير مضــادة للتهديدات الحرجة، وتحديد المخاطر المقبولة، وتقديم خطة للتعافي في حالة إدراك المخاطر. ويقصد بالمخاطر الأحداث الخارجية التي قد تؤدي إلى انحراف في سلوك النظام، أو الخروقات الأمنية ونقاط الضــعف التي تحتويها أصــول النظام. تتطلب طرق تقييم المخاطر تحديد الفرص الممكنة (أو احتمالات) للهجوم وآثاره (أو شدته).

ويشير تأثير الهجوم إلى الضرر المنجر عنه وأضراره المحتملة. في نفس الوقت، يتم احتساب احتمال الهجوم على أنه عكس إمكاناته، أي الصعوبة. في الواقع، كلما زادت صعوبة إدراك الهجوم، قل احتمال وقوعه. في الأقسام التالية، نقوم بمراجعة أهداف إدارة المخاطر ومكوناتها والمعايير الرئيسية لتقييم المخاطر وبعض تقنيات وصف الهجوم واحتساب المخاطر.

تهدف إدارة المخاطر إلى تحديد نقاط الضعف للنظام (أو أصوله) والتهديدات التي قد تستهدف هذا النظام. في الواقع، ترتبط التهديدات باســتغلال بعض نقاط الضــعف. هنا تشــير كلمة نظام إلى أي نوع من المنظمات أو الشركات أو البنى التحتية أو التقنيات/التكنولوجيات.

ترتبط أهداف إدارة المخاطر بأهداف النظام والتوجيهات القانونية. على ســبيل المثال، يمكن للشــركة تقييم المخاطر المرتبطة بأحد منتجاتها قبل تصــنيعها ومن ثم بعد إنتاجها. في هذه الحالة، ســتســمح إدارة المخاطر

للشـركة بتحديد التهديدات المتعلقة بهذا المنتج والتخفيف من المخاطر الضـارة. هذا، سـوف يعمل على تجنب المخاطر عند تقديم المنتج إلى السـوق وتمييزه عن المنتجات الأخرى. كما سـيعكس جدية الشـركة المصـنعة ويحسـن صـورة علامتها التجارية. في الواقع، مع عدم وجود إدارة للمخاطر، قد تخاطر بعض الشـركات بتقديم منتجات لا تحترم التوجيهات القانونية مما يمكن أن يؤدي بعد ذلك إلى خسـارة الاسـتثمار. ويسـتوجب تفعيل المشاريع المقترحة التطرق للنقاط التالية:

1- اعداد إطار عمل للابتكار في الامن السيبراني

2- انشاء / دعم انشاء مراكز ابتكار في الامن السيبراني تهدف الى:

- تعزيز ودعم ثقافة الابتكار وريادة الأعمال في الأمن السيبراني والتقنيات الحديثة
- التشجيع على البحث والابتكار والتدريب في مجال الأمن السيبراني
- المساهمة وتطوير حلول وطنية مجال الأمن السيبراني
- بناء حلقة وصل بين الجهات الحكومية والقطاع الخاص والمؤسسات الأكاديمية

3.7: حزمة العمل 7: تطوير إجراءات/ أطر قانونية موحدة:

تشـجع الاسـتراتيجية العربية للأمن السـيبراني ACSS تطوير الأطر القانونية المحلية للأمن السـيبراني وحماية البيانات، والتي تتعلّق بالتعامل مع الحوادث، وشـهادة منتجات الأمن السـيبراني، والتحقيق الرقمي، والثقة الرقمية، والإدارة الآمنة للبيانات. تشمل هذه الأطر الإجراءات ذات الصلة بالوقاية من حوادث الأمن السيبراني ومراقبتها والتعامل معها، وأية إجراءات أخرى يستوجب المؤسسات/الهيئات العامة أو الخاصّة القيام بها لتعزيز فضـاء رقمي وطني آمن وقادر على الصـمود. وتجدر الإشـارة إلى أنه بالإضـافة إلى الأدوات/الوسـائل القانونية الإقليمية التي تم تحديدها في هذه الاستراتيجية لمعالجة جوانب الأمن السيبراني، سيتم وضع/ تقديم أفضل الممارسات لضمان التكامل الفعال للأطر التنظيمية الوطنية على المستوى الإقليمي.

وسـوف تعتمد الاسـتراتيجية العربية للأمن السـيبراني على القوانين واللوائح الحالية التي تعالج تحديات الأمن السـيبراني ، إن وجدت ، وإنشـاء وتحديث وإصـلاح الأطر القانونية الحالية للأمن السـيبراني ، بما في ذلك على سـبيل الذكر لا الحصـر: قواعد أمن البيانات وإمكانية تطبيقها على أمن أنظمة المعلومات ؛ تحديد البنية التحتية الوطنية للمعلومات الحيوية/الحسـاسـة ؛ إنشـاء وكالات وطنية وقطاعية تتعامل مع جوانب الأمن السيبراني) على سبيل المثال ، وكالات الأمن السيبراني الوطنية ، وفرق الاستجابة للطوارئ على المستوى الوطني

والقطاعي / CERTs/CSIRT/CIRTالتصديق على مؤسسات وعمليات ومنتجات وسياسات الأمن السيبراني ؛ قواعد الأمن الوطني / للدولة المطبقة على أمن الفضاء السيبراني.

علاوة على ذلك، توفر الإجراءات المذكورة في الاستراتيجية إرشادات حول كيفية التعامل مع الأساليب التنظيمية الشائعة/ Common التي تتعلق بكل من الأمن السيبراني والجرائم السيبرانية مثل التبادل العابر للحدود لمعلومات الأمن السيبراني، والتحليل المشترك لبيانات الجرائم السيبرانية، فضلاً عن الاستجابة المشتركة لحوادث الأمن السيبراني.

سيشمل الإطار التنظيمي الإقليمي الذي تتناوله الاستراتيجية العربية للأمن السيبراني تعريفات مشتركة تتعلق بالتهديدات والجرائم السيبرانية، مما سيوفر قوى إجرائية كافية للتحقيق والملاحقة القضائية الفعالة، وكذلك الفصل في القضايا ذات الصلة على أساس الأدلة الرقمية المقبولة.

ويجب بذل جهود كبيرة لدمج/إدماج مخرجات الاستراتيجية العربية للأمن السيبراني في الأطر التنظيمية الوطنية الحالية للأمن السيبراني (على سبيل المثال، قانون العقوبات والقوانين المنظمة للبنوك والاتصالات والقطاعات الأخرى). من أجل وضع تشريعات واضحة وقابلة للتنفيذ بشأن الجرائم السيبرانية العابرة للحدود، يجب على البلدان محاولة مواءمة إطارها القانوني المحلية مع الإجراءات القانونية الدولية والإقليمية القائمة بهذا الصدد. وتوفر الاستراتيجية أيضًا إرشادات للجوانب التشغيلية للتحقيق في الجرائم السيبرانية والملاحقة القضائية، مثل إنشاء وحدات متخصصة، وقدرات التحليل الجنائي الرقمي المناسبة، وإجراءات التشغيل الموحدة، وخطط الإبلاغ عن الجرائم التي قد لا يتم وضعها على مستوى التشريع الأساسي ولكن يمكن تقديمها مع ذلك على أنها لوائح ثانوية أو إرشادات أو أفضل الممارسات. وتشجع الاستراتيجية العربية للأمن السيبراني أيضا على إنشاء عملية لرصد تنفيذ ومراجعة التشريعات وآليات الحوكمة، وتحديد الثغرات/الفجوات والسلطات المتداخلة، وتوضيح وتحديد أولويات المجالات التي تتطلب التحديث (على سبيل المثال، القوانين الحالية مثل قوانين الاتصالات القديمة).

والجدير بالذكر أن المساهمات تكمل بعضها البعض لتشكل مشهدًا شاملاً لنماذج الأمان والثقة المطبقة في إطار الثورة الصناعية الرابعة (الصناعة 4.0). ويوضح هذا تناول جوانب مختلفة متعلقة بتطبيق تقنية سلسلة الكتل blockchain لنشر سياسات الأمان والثقة في المنصات الصناعية المنتشرة التي تدعم إنترنت الأشياء.

الفصل الرابع : خاتمة

يجب أن يسير الأمن السيبراني جنبًا إلى جنب مع سياسات وخطط واستراتيجيات التحول الرقمي. مع التطور السريع لمشهد التهديدات السيبرانية، يجب أن يكون الأمن السيبراني أولويّة مدعومة على جميع مستويات الحوكمة. تحدد هذه الوثيقة ركائز الاستراتيجية العربية للأمن السيبراني، والتي تشمل مجموعة من الإجراءات التنسيقية التي تسمح بالتنفيذ المتكرر/المتواصل للأطر الاستراتيجية الوطنية بالإضافة إلى خلق قيمة جماعية تعتمد على أصول الفضاء السيبراني العربي.

إن تنسيق مبادرات الأمن السيبراني ومشاركة المعلومات الأساسية من شأنه أن يعزز بشكل كبير الأمن والسلامة والمرونة والثقة داخل الفضاء السيبراني العربي. تعد حزم العمل والإجراءات المقترحة مفيدة للدول الأعضاء

لتعزيز فهم مشـترك لتحديات الأمن السـيبراني الإقليمية وللمسـاعدة في التنفيذ الفعال للضـوابط والإجراءات التعـاونيـة. سـيمكن هـذا المنطقـة العربيـة من تبوّأ مكانـة تتمكن من خلالهـا من جني فوائـد التحول الرقمي ، والابتكار المعتمد على أصحاب المصلحة المتعددين والاقتصاد الافتراضي.

فريق الخبراء

أ. محمد حمدي، جامعة قرطاج، تونس	رئيس الفريق
د. منى الهواوره، جامعة ديكن، أستراليا	خبيرة في الأمن السيبراني
د. علي إسماعيل عوض، جامعة الإمارات العربية المتحدة	خبير في الأمن السيبراني
د. أيمن بودقيقة، هيئة الطاقة الذرية، فرنسا	خبير في تحليل المخاطر السبرانية